Administering Avaya IP Office with Web Manager

Release 12.1
Issue 53
March 2025

© 2024-2025, Avaya LLC
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

“**Hosted Service**” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Part 1: Introduction 32
- **Chapter 1: Purpose** 33
  - New in IP Office Release 12.0 33
  - New in IP Office Release 12.1 34
  - New in IP Office Release 12.1 SP1 36
- **Chapter 2: IP Office Web Manager** 37
  - Supported Web Browsers 37
  - IP Office Types 37
- **Chapter 3: Logging in to web manager** 39
  - Logging in to Web Manager 39
  - Logging in without a certificate 40
  - Logging out of Web Manager 41
  - Web Manager Service Users 41
  - Changing your password 42
- **Chapter 4: The Web Manager User Interface** 43
  - The Menu Bar and Solution Display 43
  - Menu Bar Options 45
  - Solution Button Menus 46
    - Actions Menu (Linux-based server) 46
    - Actions Menu (IP500 V2) 47
    - Configure Button Menu 47
    - Solution Settings Button Menus 48
    - The "Hamburger" Server Menu 48
  - User Preferences 49
  - Record Consolidation 51
  - Offline Mode 52
- **Chapter 5: Displaying and Managing Configuration Records** 56
  - Types of Configuration Records 56
  - Displaying Configuration Records 59
  - Filtering the list 60
  - Searching the list 60
  - Sorting the list 60
  - Adding a New Record 61
  - Quick Edit 61
  - Editing an Existing Entry 62
  - Editing Multiple User Records 62
  - Deleting a Record 63
  - Deleting Multiple Records 63
- **Chapter 6: The Setup Wizard/Initial Configuration** 64

Setup Wizard: Panels Summary 65
Setup Wizard: System Panel (Initial Configuration Utility) 66
Setup Wizard: VoIP 70
Setup Wizard: Voicemail 74
Setup Wizard: Subscription 76
Setup Wizard: Licensing 77
Setup Wizard: User 77
Setup Wizard: Groups 77
Setup Wizard: Lines 78
Setup Wizard: Incoming Call Routes 78
Setup Wizard: Outgoing Call Routes 79
Chapter 7: Using User and Extension Templates 81
Saving a user or extension as a template 81
Adding a new template 82
Adding users or extensions using a template 82
Deleting a template 83
Editing a template 83
Downloading a template 83
Uploading a template 84
Renaming a template 84
Part 2: The Solution Menu 85
Solution 85
Chapter 8: The "Solution Settings" Menu 86
View Scheduled Jobs 86
Remote Server 87
Remote server settings 87
Proxy 88
User Synchronization Using LDAP 89
Connect to Directory Service 90
Synchronize User Fields 92
View Jobs 95
Manage User Provisioning Rules 95
User Synchronization using MS Teams 96
Connect to Directory Service 97
Synchronize User Fields 98
View Jobs 101
Manage User Provisioning Rules 101
Application Server 102
Chapter 9: The "Actions" Button Menu 104
Backup 105
Restore 105
Transfer ISO 106
Upgrade 106

Synchronize Service User and System Password..... 107
Synchronize Single Sign-On Configuration..... 107
Synchronize APNS configuration..... 108
Synchronize APNP System-ID..... 108
Download Configuration..... 108
Remote Operations Management..... 109
Chapter 10: The "Actions" Button Menu (IP500 V2)..... 110
Backup..... 111
Restore..... 111
Upgrade..... 112
Download Configuration..... 112
Upload Configuration..... 113
Backup Status..... 113
Restore Status..... 113
On-boarding..... 113
Initial Configuration..... 114
Service Commands (Standalone IP500 V2)..... 114
Reboot..... 115
System Shutdown (IP500 V2)..... 116
Erase Security Settings (IP500 V2)..... 116
Service Status..... 117
Erase Configuration..... 117
Memory Card Start..... 117
Memory Card Stop..... 118
Copy to Optional SD..... 118
Chapter 11: The "Configure" Button Menu..... 119
Add System to Solution..... 119
Remove System from Solution..... 121
Convert to Select Licensed System..... 121
Resiliency Administration..... 121
Set All Nodes to Subscription..... 121
Set All Nodes License Source..... 122
Link Expansions..... 122
Chapter 12: The "Hamburger" Server Menu..... 124
Dashboard..... 125
Platform View..... 125
Backup..... 125
Restore..... 126
On-boarding..... 127
Launch SSA..... 127
Service Commands..... 128
Restart IP Office Service..... 128
Erase Configuration..... 129

Erase Security Settings..... 129
Initial Configuration..... 129
Download Configuration..... 130
View Upgrade Report..... 130
Chapter 13: The Platform View menus..... 131
System..... 132
Logs..... 134
Debug Logs..... 135
Syslog Event Viewer..... 135
Download..... 135
Updates..... 136
Settings..... 137
General Settings..... 137
System Settings..... 145
AppCenter..... 154
Part 3: The Call Management Menu..... 156
The Call Management Menus..... 156
Chapter 14: Users..... 157
User Actions..... 158
Import Users..... 158
Export users..... 158
User Template Management..... 159
Create From Template..... 159
Provision Users..... 159
Users..... 160
Voicemail..... 168
Button Programming..... 174
Telephony 174
Telephony Call Settings..... 175
Supervisor Settings..... 178
Multiline Options..... 181
Telephony Call Log..... 183
Telephony TUI..... 184
Short Codes..... 185
Forwarding..... 186
Mobility..... 190
Group Membership..... 194
Voice Recording..... 194
Do Not Disturb..... 196
Announcements..... 197
Personal Directory..... 199
SIP 200
Menu Programming..... 201

Menu Programming — T3 Telephony ... 202
Menu Programming — Hunt Group ... 202
Menu Programming — 4400/6400 ... 203
Dial In ... 204
Source Numbers ... 204
User Portal ... 205
Chapter 15: Extension ... 209
Extension Template Management ... 209
Create From Template ... 210
Provision Extensions ... 210
Add Extension ... 211
Extension Common Fields ... 211
Analog ... 214
H323 Extension VoIP ... 217
SIP Extension VOIP ... 220
T38 Fax ... 225
IP DECT Extension ... 227
Chapter 16: Groups ... 229
Add Groups ... 230
Group settings ... 230
Queuing ... 234
Overflow ... 237
Fallback ... 239
Voicemail ... 242
Voice Recording ... 248
Announcements ... 249
SIP ... 252
Chapter 17: Conferences ... 254
Chapter 18: Auto Attendant (EVM) ... 257
Auto Attendant settings (EVM) ... 258
Auto Attendant (EVM) ... 259
Actions (EVM) ... 260
Chapter 19: Auto Attendants (Voicemail Pro) ... 263
Auto Attendants ... 263
Action ... 267
Part 4: The System Settings Menu ... 270
System Settings ... 270
Chapter 20: Account Code ... 272
Account Code ... 273
Voicemail Recording ... 273
Chapter 21: Alternate Route Selection ... 275
Add Alternate Route ... 275

Chapter 22: Authorization Code 280
Add Authorization Code 280
Chapter 23: Firewall Profile 281
Add Firewall Profile 281
Chapter 24: Incoming Call Route 283
Add Incoming Call Route 283
Incoming Call Route General Settings 286
Incoming Call Route Voice Recording 289
Incoming Call Route Destinations 291
Incoming Call Route MSN Configuration 293
Chapter 25: IP Route 294
Add IP Route 294
Chapter 26: Licenses 296
License 296
Remote Server 299
Chapter 27: Line 303
Add Trunk Line 303
ACO Line 305
ACO Line | ACO 305
ACO Line | VoIP 307
ACO Line | T38 FAX 309
Analog Line 311
Line Settings 311
Line Options 313
BRI Line 319
Line Settings 320
Channels 324
H.323 Line 324
H.323 Line VoIP 325
H.323 Line Short Codes 327
H.323 Line VoIP Settings 328
IP DECT 331
IP DECT Line 331
Gateway 331
VoIP 333
IP Office Line 335
IP Office Line 336
IP Office Line Short Codes 341
IP Office Line VoIP Settings 341
T38 Fax 344
Legacy SIP DECT Line 345
SIP DECT Base 346

SIP DECT VoIP ... 347
MS Teams Line ... 348
MS Teams ... 348
VoIP ... 351
Engineering ... 355
PRI Trunks ... 356
E1 Line ... 357
E1 PRI Line ... 357
E1 Short Codes ... 363
E1 PRI Channels ... 363
E1 R2 Line ... 365
E1-R2 Options ... 365
E1-R2 Channels ... 367
E1–R2 MFC Group ... 369
E1-R2 Advanced ... 369
T1 Line ... 371
US T1 Line ... 371
T1 Channels ... 373
SIP Line ... 376
SIP Line ... 377
SIP Line I Transport ... 381
Call Details ... 384
SIP Line VoIP ... 391
T.38 Fax ... 395
SIP Line Credentials ... 397
SIP Line Advanced ... 398
SIP Line Engineering ... 404
T1 PRI Line ... 405
T1 ISDN ... 406
T1 ISDN Channels ... 409
T1 ISDN TNS ... 411
T1 ISDN Special ... 412
Call By Call (US PRI) ... 412
SM Line ... 414
SM Line Session Manager ... 414
SM Line VoIP ... 417
SM Line T38 Fax ... 421
Chapter 28: Locations ... 423
Location ... 423
Address ... 426
Chapter 29: RAS ... 429
Add RAS ... 429
Chapter 30: Services ... 432

Normal, WAN, or Internet Service 433
SSL VPN Service 441
Remote Support Services 444
Chapter 31: Short Codes 445
Add Short Code 445
Chapter 32: Subscription 447
Chapter 33: System Directory 449
Add Directory Entry 449
Chapter 34: System 451
System 451
Voicemail 461
System Events 469
SNMP Settings 469
Add SNMP Trap 471
SMTP 476
DNS 477
SMDR 478
LAN1 479
Settings 480
Settings (IPv6) 483
VoIP 487
Network Topology 495
LAN2 501
VoIP 501
VoIP 501
VoIP Security 503
Access Control Lists 506
Directory Services 506
LDAP 506
HTTP 510
Telephony 512
Telephony 512
Park and Page 521
Tones and Music 522
Ring Tones 526
SM 526
MS Teams 527
Call Log 528
TUI 529
Contact Center 532
Avaya Cloud Services 532
Avaya Push Notification Services 535
Remote Operations 536

Chapter 35: Time Profiles 537
Add Time Profile 537
Chapter 36: Tunnel 540
L2TP Tunnel 540
L2PT Tunnel 541
L2TP 542
L2TP PPP 542
IP Security Tunnel 543
IPSec Main 543
Tunnel | IKE Policies (IPSec) 544
IPSec Policies 545
Chapter 37: User Rights 546
Add User Right 546
User 547
Short Codes 547
Button Programming 548
Telephony 548
Call Settings 549
Supervisor Settings 550
Multi-line Options 551
Call Log 551
User Rights Membership 552
Voicemail 553
Forwarding 554
Chapter 38: WAN Port 556
Add WAN Port — Sync PPP 556
Add WAN Port — Sync Frame Relay 557
Part 5: The Security Menu 560
Chapter 39: Security Administration 561
Service Users, Roles, and Rights Groups 561
Default Service Users and Rights Groups 563
Default Rights Groups 564
Access Control 566
Encryption 567
Message Authentication 568
Certificates 569
Implementing Security 569
SRTP 571
Chapter 40: Security Settings 573
General 573
System 577
System Details 577

Unsecured Interfaces ... 579
Services ... 581
Rights Groups ... 583
Group Details ... 583
Configuration ... 584
Security Administrator ... 585
System Status ... 586
Telephony APIs ... 586
Web Services ... 586
External ... 588
HTTP ... 589
Service Users ... 589
Certificates ... 590
Part 6: The Applications Menu ... 600
Applications menu options ... 600
Chapter 41: File Manager ... 601
Chapter 42: IP Office Manager ... 602
Chapter 43: one-X Portal ... 604
Chapter 44: Voicemail Pro - System Preferences ... 605
General ... 605
Email ... 607
Gmail Integration ... 610
Housekeeping ... 611
SNMP Alarm ... 612
Outcalling ... 613
Voicemail Recording ... 614
Syslog ... 615
Alarms ... 615
User Group ... 617
Backup Config ... 617
Chapter 45: Voicemail Pro - Call Flow Management ... 618
Chapter 46: WebRTC Configuration ... 619
System Settings ... 619
SIP Server Settings ... 620
Media Gateway Settings ... 621
Chapter 47: Web License Manager ... 624
Chapter 48: Media Manager ... 625
Media Manager Configuration Settings ... 625
Connectors ... 627
Alarms ... 628
Recordings ... 628
Migration ... 630

Audit Trail..... 631
Chapter 49: Centralized Media Manager Audit Trail..... 633
Chapter 50: Centralized Media Manager Recordings..... 635
Part 7: Backup..... 637
Chapter 51: Backup and Restore..... 638
Backup and restore policy..... 639
Backup and restore protocols..... 640
Enabling HTTP backup support..... 640
Disk space required for backups..... 641
Checking the backup server's backup quota..... 642
Backup data sets..... 642
Creating a remote server connection..... 644
Backing up a server/servers..... 644
Restoring from the backup server..... 645
Restoring a failed server..... 646
Part 8: VMPro Auto Attendants..... 648
Chapter 52: Voicemail Pro Auto-Attendants..... 649
Google TTS Prompt Language..... 650
Text-to-Speech (TTS) Prompts..... 650
Enabling Google Speech and the Default Voice..... 651
Auto-Attendant Fallback Options..... 652
Auto-Attendant Callflow..... 652
Auto-Attendant Consent Example..... 653
Chapter 53: Managing Auto-Attendants (Voicemail Pro)..... 655
Enabling Google Speech and the Default Voice..... 655
Displaying the list of Auto-Attendants..... 656
Adding a new Auto-Attendant..... 656
Editing an Auto-Attendant..... 656
Deleting an Auto–Attendant..... 657
Deleting multiple Auto–Attendants..... 657
Chapter 54: Voicemail Pro Auto-Attendant Settings..... 659
Auto-Attendant..... 659
Actions..... 663
Chapter 55: Voicemail Pro Auto-Attendant Actions..... 666
Dial By Conference..... 666
Dial By Name..... 667
Dial By Number..... 669
Leave Message..... 670
Supervised Transfer..... 671
Park & Page..... 672
Replay Menu..... 674
Speak By Name..... 675

Speak By Number 676
Unsupervised Transfer 677
Transfer to Auto Attendant 678
Chapter 56: Recording Auto-Attendant Prompts (Voicemail Pro) 679
Recording Auto-Attendant Prompts Using Short Codes 679
Using Pre-Recorded Prompt Files 680
Recording Auto-Attendant Prompts Using Text-to-Speech 681
Recording User Name Prompts 681
Chapter 57: Routing Calls to a Voicemail Pro Auto-Attendant 683
Routing External Calls to an Auto-Attendant 683
Routing Internal Calls to an Auto-Attendant 683
Part 9: Conferencing 685
Chapter 58: Conferencing 686
Conference Types 686
Conference Participants 687
User Conference Controls 687
Conference Capacities 688
Conference ID Numbers 689
Conference Notes 689
Conference Phones 690
Context Sensitive Conferencing 691
Chapter 59: Ad-Hoc Conferencing 694
Dropping External Party Only Conferences 694
Adding Callers to an Ad-Hoc Conference 694
Chapter 60: Personal Meet-Me Conferences 696
Setting a User's Personal Conference PIN 696
Routing Internal Callers to a Meet-Me Conference 697
Routing External Callers to a Meet Me Conference 697
Personal Meet-Me Conference Callflow 698
Chapter 61: System Conferences 700
Adding a System Conference 700
Editing a System Conference 701
Deleting a System Conference 701
System Conference Settings 702
Routing External Calls to a System Conference 704
System Conference Callflows 705
Part 10: Centralized Media Manager 707
Chapter 62: Centralized Media Manager 708
Select local or centralized Media Manager 709
Setting How Long Recordings are Kept 709
Configuring User Access to the Recording Library 710
Changing the Recording Source in the User Portal 711

Chapter 63: Viewing Recordings 712
Applying a Recording Filter 712
Playing Recordings 713
Downloading Recordings 714
Deleting Recordings 715
Archiving Recordings to the External Storage 715
Chapter 64: Displaying the Recording Audit Trail 717
Exporting the Audit Trail 717
Chapter 65: Archiving Recordings to External Storage 719
Configuring Connection to the Google Storage Bucket 720
Archiving Recordings to the External Storage 720
Google Administrator Access to the External Storage 721
Allowing Access to the External Storage by Other Users 723
The Archive Listing Page 724
Part 11: Configuring Systems 725
Chapter 66: Subscriptions 726
Ordering Subscriptions 726
Trial Mode 727
User Subscriptions 727
Application Subscriptions 728
Customer Operations Manager (COM) 729
Subscription Connection Operation 730
Subscription Network Requirements 731
Subscription Mode Ports 732
Migrating Existing IP Office Systems to Subscription Mode 733
Chapter 67: General System Configuration 734
Centralized System Directory 734
Advice of Charge 738
Using Locations 739
Caller Display 739
Parking Calls 740
Automatic Intercom Calls 741
Wide Band Audio Support 742
Media Connection Preservation 743
Configuring IP Routes 744
Creating a Virtual WAN Port 745
Chapter 68: On-boarding 747
Configuring an SSL VPN using an on-boarding file 747
Chapter 69: Fax Support 749
Server Edition T38 Fax Support 750
Chapter 70: Paging 752
Paging Capacity 752

Phone to Phone Paging 753
Paging to an External Paging Device 753
Mixed Paging 754
Chapter 71: System Events 756
Configuring Alarm Destinations 757
Chapter 72: Certificate Management 758
Certificate Overview 758
Windows Certificate Store 760
Certificate Support 763
Certificate File Naming and Format 763
Identity Certificate 764
Trusted Certificate Store 766
Signing Certificate 767
Certificate File Import 769
Chapter 73: Configuration for Emergency Calls 772
Emergency Call Indication 773
System Alarm Output 774
Chapter 74: Ring Tones 775
Chapter 75: Music On Hold 777
System Source 779
Alternate Source 779
Chapter 76: System Date and Time 783
System Date and Time Options 783
Applying Daylight Saving 784
Checking Automatic Time and Date Operation 785
Manually Changing the System Date and Time 786
Chapter 77: Configuring Time Profiles 787
Overriding a Time Profile 788
Chapter 78: Applying Licenses 790
PLDS licensing 790
Web License Manager (WebLM) 791
Server Edition Centralized Licensing 792
Distributing Server Edition Licenses 792
Nodal license distribution 794
Centralized license distribution 795
Procedures for Applying Licensing 797
Obtaining the Host ID of the WebLM Server 798
Installing a License File on the WebLM Server 798
Configuring the Server Edition License Source 799
Uploading a PLDS License File to IP Office 799
Configuring Server Edition Nodal Licensing 800
Configuring Server Edition Centralized Licensing 800

Configuring the License Server in an Enterprise Branch Deployment 802
Converting from Nodal to Centralized Licensing 803
Migrating Licenses to PLDS 804
Chapter 79: Working with Templates 806
Saving Template files 806
Creating a Template in Manager 807
Creating an Analog Trunk Template in Manager 807
Creating a New Analog Trunk from a Template in Manager 808
Chapter 80: Configuring ARS 809
Example ARS Operation 810
ARS Operation 811
ARS Short Codes 813
Simple Alternate Line Example 814
Simple Call Barring 815
User Priority Escalation 815
Time Based Routing 817
Account Code Restriction 818
Tiered ARS Forms 818
Planning ARS 820
Chapter 81: Call Barring 821
Applying Call Barring 821
Overriding call barring 822
Chapter 81: Configuring authorization codes 823
Entering an Authorization Code 824
Chapter 81: Preventing Toll Bypass 825
Configuring unknown locations 826
Chapter 81: Configuring Call Admission Control 827
Manager location tab 827
Assigning a network entity to a location 828
System actions at maximum call threshold 828
Example 829
Chapter 82: Configure User Settings 831
User Management Overview 831
Configuring Gmail Integration 833
Call Intrusion 834
Call Tagging 837
Call Waiting 837
Call Barring 838
Centralized Call Log 839
Centralized Personal Directory 839
Account Code Configuration 840
Setting a User to Forced Account Code 841

Malicious Call Tracing (MCID)..... 842
Twinning..... 842
Private Calls..... 845
System Phone Features..... 846
The 'No User' User..... 847
Suppressing the NoCallerId alarm..... 848
Chapter 83: Avaya cloud authorization..... 849
Apple push notification services..... 849
Enabling Apple push notifications..... 850
Chapter 84: Managing Users with LDAP..... 852
Performing LDAP Synchronization..... 852
Creating a User Provisioning Rule for LDAP Synchronization..... 853
Chapter 85: Message Waiting Indication..... 855
Message Waiting Indication for Analog Phones..... 855
Message Waiting Indication for Analog Trunks..... 856
Chapter 86: Configuring User Rights..... 858
Adding User Rights..... 860
Creating a User Right Based on an Existing User..... 860
Associating User Rights to a User..... 861
Copy User Rights Settings over a User's Settings..... 861
Chapter 87: DND, Follow Me and Forwarding..... 862
Do Not Disturb (DND)..... 863
Follow Me..... 865
Forward Unconditional..... 867
Forward on Busy..... 869
Forward on No Answer..... 871
Determining a User's Busy Status..... 873
Chaining..... 874
Chapter 88: Hot Desking..... 876
Hot Desking Operation..... 877
Logging Out..... 877
Hot Desking Controls..... 878
Hot Desking in an IP Office Network..... 878
Call Center Agents..... 879
Hot Desking Examples..... 879
Scenario 1: Occasional Hot Desking..... 880
Scenario 2: Regular Hot Desking..... 880
Scenario 3: Full Hot Desking..... 880
Scenario 4: Call Center Hot Desking..... 881
Automatic Log Out..... 881
Chapter 89: Group Operation..... 883
Group Types..... 886

Call Presentation 887
Group Member Availability 889
Example Hunt Group 891
CBC/CCC Agents and Hunt Groups 892
Coverage Groups 893
Chapter 90: Mobile Call Control 894
Mobile Direct Access (MDA) 897
Mobile Callback 899
Chapter 91: Transferring calls 900
Transferring call notes 900
Transferring call notes 901
Off-Switch Transfer Restrictions 902
Context Sensitive Transfer 903
Dial Tone Transfer 904
Handsfree Announced Transfers 906
One Touch Transferring 908
Centrex Transfer 909
Chapter 92: Simultaneous mode 911
Simultaneous Mode Devices 911
Simultaneous Mode Notes 911
Moving Calls Between Simultaneous Devices 912
Chapter 93: User Source Numbers 913
Individual User Source Numbers 913
NoUser Source Numbers 915
Part 12: SIP Trunks 923
Editing Configuration Settings 923
Chapter 94: SIP Trunk Overview 924
Configuring a SIP Trunk 924
SIP Line Requirements 925
Chapter 95: SIP Headers and URIs 929
SIP URI Formats 929
Standard SIP Headers 930
Setting the SIP URI Host 930
Setting the SIP URI Content 931
Selecting the SIP Header Format Used 933
Chapter 96: Outgoing SIP Call Routing 934
SIP Outgoing Call Routing 934
Anonymous SIP Calls 935
SIP ARS Response Codes 936
Typical outgoing call scenarios 938
Chapter 97: Incoming SIP Call Routing 941
SIP Short Codes 941

SIP Incoming Call Routing 942
SIP Prefix Operation 944
Media path connection 944
SIP Caller Name and Number Display 945
Typical incoming call scenarios 946
Chapter 98: SIP messaging 950
Codec selection 950
SIP DTMF Transmission 951
Fax over SIP 952
SIP Call Hold Scenarios 952
SIP Call Transfers (Refer) 954
Ringback Tone 955
Hold Reminders 956
Chapter 99: SIP Line Appearances 957
SIP Line Appearance Incoming Call Routing 957
SIP Line Appearance Outgoing Call Routing 957
SIP Line Appearance User Button Programming 958
Chapter 100: SIP Calling Number Verification (STIR/SHAKEN) 959
The STIR/SHAKEN SIP Protocols 960
Obtaining a call's number verification result 961
Setting the system's number verification default behavior 961
Enabling calling number verification on a SIP line 962
SIP Calling Number Verification (STIR/SHAKEN) 963
Changing the rejected call responses 965
Changing the authentication header used 965
Customizing the call handling behavior 966
Call Records 966
Chapter 101: IP Office SIP trunk specifications 968
SIP RFCs 968
Transport protocols 970
Request methods 970
Response methods 971
Headers 971
Part 13: Short Codes 972
Chapter 102: Short Code Overview 973
Short Code Characters 975
User Dialing 980
Application Dialing 982
Secondary Dial Tone 982
? Short Codes 984
Short Code Matching Examples 984
Default System Short Code List 987

Chapter 103: Short Code Features 993
Auto Attendant 996
Auto Intercom Deny Off 997
Auto Intercom Deny On 997
Break Out 998
Barred 998
Busy On Held 999
Call Intrude 1000
Call Listen 1000
Call Park 1002
Call Park and Page 1002
Call Pickup Any 1003
Call Pickup Extn 1003
Call Pickup Group 1004
Call Pickup Line 1005
Call Pickup Members 1005
Call Pickup User 1006
Call Queue 1006
Call Record 1007
Call Steal 1008
Call Waiting On 1009
Call Waiting Off 1009
Call Waiting Suspend 1010
Cancel All Forwarding 1010
Cancel Ring Back When Free 1011
Change Login Code 1012
Clear After Call Work 1012
Clear Call 1013
Clear CW 1013
Clear Hunt Group Night Service 1014
Clear Hunt Group Out Of Service 1015
Clear Quota 1015
Coaching Intrusion 1016
Conference Add 1016
Conference Meet Me 1017
CW 1018
Dial 1019
Dial 3K1 1020
Dial 56K 1020
Dial 64K 1021
Dial CW 1021
Dial Direct 1022
Dial Direct Hot Line 1022

Dial Emergency..... 1023
Dial Extn..... 1023
Dial Fax..... 1024
Dial Inclusion..... 1024
Dial Paging..... 1025
Dial Physical Extension by Number..... 1026
Dial Physical Extension By ID..... 1026
Dial Speech..... 1027
Dial V110..... 1027
Dial V120..... 1028
Dial Video..... 1028
Disable ARS Form..... 1028
Disable Internal Forwards..... 1029
Disable Internal Forward Unconditional..... 1029
Disable Internal Forward Busy or No Answer..... 1030
Display Msg..... 1030
Do Not Disturb Exception Add..... 1031
Do Not Disturb Exception Delete..... 1032
Do Not Disturb On..... 1033
Do Not Disturb Off..... 1033
Enable ARS Form..... 1034
Enable Internal Forwards..... 1034
Enable Internal Forward Unconditional..... 1035
Enable Internal Forward Busy or No Answer..... 1035
Extn Login..... 1035
Extn Logout..... 1037
Flash Hook..... 1037
FNE Service..... 1038
Follow Me Here..... 1038
Follow Me Here Cancel..... 1039
Follow Me To..... 1039
Forward Hunt Group Calls On..... 1040
Forward Hunt Group Calls Off..... 1041
Forward Number..... 1041
Forward On Busy Number..... 1042
Forward On Busy On..... 1043
Forward On Busy Off..... 1043
Forward On No Answer On..... 1044
Forward On No Answer Off..... 1044
Forward Unconditional On..... 1045
Forward Unconditional Off..... 1045
Group Listen Off..... 1046
Group Listen On..... 1046

Headset Toggle..... 1047
Hold Call..... 1047
Hold CW..... 1048
Hold Music..... 1049
Hunt Group Disable..... 1049
Hunt Group Enable..... 1050
Last Number Redial..... 1050
MCID Activate..... 1051
Mobile Twinned Call Pickup..... 1051
Off Hook Station..... 1052
Outgoing Call Bar Off..... 1052
Outgoing Call Bar On..... 1053
Private Call Off..... 1054
Private Call On..... 1054
Priority Call..... 1055
Record Message..... 1055
Relay On..... 1056
Relay Off..... 1057
Relay Pulse..... 1057
Resume Call..... 1058
Retrieve Call..... 1059
Ring Back When Free..... 1059
Secondary Dial Tone..... 1060
Set Absent Text..... 1060
Set Account Code..... 1062
Set Authorization Code..... 1062
Set Fallback Twinning Off..... 1063
Set Fallback Twinning On..... 1063
Set Hunt Group Night Service..... 1063
Set Hunt Group Out Of Service..... 1064
Set Inside Call Seq..... 1065
Set Mobile Twinning Number..... 1066
Set Mobile Twinning On..... 1066
Set Mobile Twinning Off..... 1066
Set No Answer Time..... 1067
Set Outside Call Seq..... 1067
Set Ringback Seq..... 1068
Set Time Profile..... 1069
Set Wrap Up Time..... 1070
Speed Dial..... 1071
Shutdown Embedded Voicemail..... 1071
Stamp Log..... 1072
Startup Embedded Voicemail..... 1072

Suspend Call ... 1073
Suspend CW ... 1073
Start After Call Work ... 1074
Toggle Calls ... 1074
Unpark Call ... 1075
Voicemail Collect ... 1075
Voicemail Node ... 1077
Voicemail On ... 1077
Voicemail Off ... 1078
Voicemail Ringback On ... 1078
Voicemail Ringback Off ... 1079
Whisper Page ... 1080
Part 14: Button Programming ... 1081
Chapter 104: Button Programming Overview ... 1082
Programming Buttons with IP Office Web Manager ... 1083
Interactive Button Menus ... 1083
Label Templates ... 1084
Chapter 105: Button Programming Actions ... 1085
Button Programming Actions Summary ... 1085
911-View ... 1093
Abbreviated Dial ... 1093
Abbreviated Dial Pause ... 1094
Abbreviated Dial Program ... 1094
Abbreviated Dial Stop ... 1095
Absent Message ... 1095
Account Code Entry ... 1095
ACD Agent Statistics ... 1096
ACD Stroke Count ... 1096
Acquire Call ... 1097
AD Special Functions ... 1097
AD Special Function Mark ... 1097
AD Special Function Wait ... 1098
AD Suppress ... 1098
After Call Work ... 1099
Appearance ... 1100
Automatic Callback ... 1101
Auto-Intercom Deny ... 1102
Automatic Intercom ... 1103
Break Out ... 1103
Bridged Appearance ... 1104
Busy ... 1105
Busy On Held ... 1105
Call Forwarding All ... 1105

Call Intrude..... 1106
Call Listen..... 1107
Call Log..... 1108
Call Park..... 1108
Call Park and Page..... 1110
Call Park To Other Extension..... 1110
Call Pickup..... 1111
Call Pickup Any..... 1112
Call Pickup Group..... 1112
Call Pickup Members..... 1113
Call Queue..... 1113
Call Record..... 1114
Call Screening..... 1114
Call Steal..... 1117
Call Waiting Off..... 1117
Call Waiting On..... 1118
Call Waiting Suspend..... 1118
Cancel All Forwarding..... 1119
Cancel Leave Word Calling..... 1119
Cancel Ring Back When Free..... 1120
Channel Monitor..... 1120
Clear Call..... 1121
Clear CW..... 1121
Clear Hunt Group Night Service..... 1122
Clear Hunt Group Out Of Service..... 1122
Clear Quota..... 1123
Coaching Intrusion..... 1123
Conference..... 1124
Conference Add..... 1125
Conference Meet Me..... 1125
Consult..... 1127
Coverage Appearance..... 1128
Dial..... 1128
Dial 3K1..... 1129
Dial 56K..... 1129
Dial 64K..... 1130
Dial CW..... 1130
Dial Direct..... 1131
Dial Emergency..... 1132
Dial Inclusion..... 1132
Dial Intercom..... 1133
Dial Paging..... 1134
Dial Physical Extn by Number..... 1134

Dial Physical Number by ID..... 1135
Dial Speech..... 1135
Dial V110..... 1136
Dial V120..... 1136
Dial Video..... 1137
Directed Call Pickup..... 1137
Directory..... 1138
Display Msg..... 1138
Do Not Disturb Exception Add..... 1139
Do Not Disturb Exception Delete..... 1140
Do Not Disturb Off..... 1140
Do Not Disturb On..... 1141
Drop..... 1141
Emergency View..... 1142
Extn Login..... 1143
Extn Logout..... 1144
Flash Hook..... 1144
Follow Me Here..... 1145
Follow Me Here Cancel..... 1146
Follow Me To..... 1146
Forward Hunt Group Calls Off..... 1147
Forward Hunt Group Calls On..... 1147
Forward Number..... 1148
Forward On Busy Number..... 1149
Forward On Busy Off..... 1150
Forward On Busy On..... 1150
Forward On No Answer Off..... 1151
Forward On No Answer On..... 1151
Forward Unconditional Off..... 1152
Forward Unconditional On..... 1153
Group..... 1153
Group Listen On..... 1154
Group Paging..... 1155
Headset Toggle..... 1156
Hold Call..... 1156
Hold CW..... 1157
Hold Music..... 1157
Hunt Group Enable..... 1158
Hunt Group Disable..... 1158
Inspect..... 1159
Internal Auto-Answer..... 1159
Last Number Redial..... 1160
Leave Word Calling..... 1160

Line Appearance..... 1161
MADN Call Appearance..... 1162
Manual Exclude..... 1163
MCID Activate..... 1163
Monitor Analog Trunk MWI..... 1164
Off Hook Station..... 1164
Pause Recording..... 1165
Priority Call..... 1166
Priority Calling..... 1166
Private Call..... 1167
Relay Off..... 1167
Relay On..... 1168
Relay Pulse..... 1168
Resume Call..... 1169
Request Coaching Intrusion..... 1170
Retrieve Call..... 1171
Ring Back When Free..... 1171
Ringer Off..... 1172
Self-Administer..... 1172
Send All Calls..... 1174
Set Absent Text..... 1174
Set Account Code..... 1175
Set Hunt Group Night Service..... 1176
Set Hunt Group Out Of Service..... 1177
Set Inside Call Seq..... 1178
Set Night Service Destination..... 1178
Set No Answer Time..... 1179
Set Out of Service Destination..... 1179
Set Outside Call Seq..... 1180
Set Ringback Seq..... 1180
Set Wrap Up Time..... 1181
Speed Dial..... 1181
Stamp Log..... 1182
Stored Number View..... 1183
Suspend Call..... 1183
Suspend CW..... 1184
Swap CLID Name/Number..... 1184
Time of Day..... 1184
Time Profile..... 1185
Timer..... 1187
Transfer..... 1187
Toggle Calls..... 1188
Twinning..... 1188

Unpark Call ... 1189
User ... 1190
Visual Voice ... 1191
Voicemail Collect ... 1193
Voicemail Off ... 1194
Voicemail On ... 1194
Voicemail Ringback Off ... 1195
Voicemail Ringback On ... 1196
Whisper Page ... 1196
Part 15: Call Appearance Buttons ... 1198
Appearance Buttons ... 1198
Chapter 106: Call Appearance Buttons ... 1200
Call Appearance Example 1 ... 1201
Call Appearance Example 2 ... 1201
How are Call Appearance Buttons Treated? ... 1202
Call Appearance Button Indication ... 1203
Chapter 107: Bridged Appearance Buttons ... 1205
Bridged Appearance Example 1 ... 1206
Bridged Appearance Example 2 ... 1206
Bridged Appearance Example 3 ... 1207
How are Bridged Appearances Treated? ... 1208
Bridged Appearance Button Indication ... 1209
Chapter 108: Call Coverage Buttons ... 1210
Call Coverage Example 1 ... 1210
Call Coverage Example 2 ... 1211
How is Call Coverage Treated? ... 1212
Call Coverage Button Indication ... 1213
Chapter 109: Line Appearance Buttons ... 1215
Line Appearance Example 1 ... 1216
Line Appearance Example 2 ... 1216
How are Line Appearances Treated? ... 1217
Line Appearance Button Indication ... 1218
Chapter 110: Appearance Button Features ... 1220
Selected Button Indication ... 1220
Idle Line Preference ... 1221
Ringing Line Preference ... 1223
Answer Pre-Select ... 1225
Auto Hold ... 1226
Ring Delay ... 1227
Delayed Ring Preference ... 1228
Collapsing Appearances ... 1230
Joining Calls ... 1231

Multiple Alerting Appearance Buttons..... 1233
Twinning..... 1234
Busy on Held..... 1234
Reserving a Call Appearance Button..... 1235
Logging Off and Hot Desking..... 1235
Applications..... 1236
Chapter 111: Programming Appearance Buttons..... 1237
Appearance Function System Settings..... 1239
Appearance Function User Settings..... 1239
Programming Line Appearance ID Numbers..... 1241
Automatic Renumbering..... 1241
Manual Renumbering..... 1241
Outgoing Line Programming..... 1242
Part 16: SMDR Call Records..... 1244
Chapter 112: Appendix: SMDR Call Records..... 1245
Enabling SMDR..... 1245
SMDR Record Buffering..... 1246
Checking SMDR Generation..... 1246
SMDR Record Output..... 1246
SMDR Record Format..... 1247
Call Times in SMDR..... 1247
SMDR Fields..... 1248
Chapter 113: SMDR Examples..... 1253
SMDR Example: Lost Incoming Call..... 1254
SMDR Example: Transfer..... 1254
SMDR Example: Call Answered by Voicemail..... 1255
SMDR Example: Call Transferred to Voicemail..... 1255
SMDR Example: Internal Call..... 1255
SMDR Example: External Call..... 1255
SMDR Example: Outgoing Call..... 1256
SMDR Example: Voicemail Call..... 1256
SMDR Example: Parked Call..... 1256
SMDR Example: Incoming Call with Account Code..... 1257
SMDR Example: Conference Using Conference Add Short Code..... 1257
SMDR Example: Conference Using Conference Button..... 1258
SMDR Example: Adding a Party to a Conference..... 1258
SMDR Example: Busy/Number Unavailable Tone..... 1259
SMDR Example: Call Pickup..... 1259
SMDR Example: Internal Twinning..... 1259
SMDR Example: Park and Unpark..... 1260
SMDR Example: Distributed Hunt Group Call..... 1260
SMDR Example: Voicemail Supervised Transfer..... 1260
SMDR Example: Outgoing External Call..... 1261

SMDR Example: Rerouted External Call..... 1261
SMDR Example: External Forward Unconditional..... 1261
SMDR Example: Call Transferred Manually..... 1262
SMDR Example: Mobile Twinned Call Answered Internally..... 1262
SMDR Example: Mobile Twinned Call Answered at the Mobile Twin..... 1263
SMDR Example: Mobile Twinned Call Picked Up Using the Twinning Button..... 1263
SMDR Example: External Conference Party..... 1264
SMDR Example: Call Routed by Incoming Call Route..... 1264
SMDR Example: Two Outgoing External Calls Transferred Together..... 1264
SMDR Example: Authorization code..... 1265
SMDR Example: Internal Network Call..... 1265
SMDR Example: Caller Consent Request..... 1265
Part 17: Further Help..... 1267
Chapter 114: Additional Help and Documentation..... 1268
Additional Manuals and User Guides..... 1268
Getting Help..... 1268
Finding an Avaya Business Partner..... 1269
Additional IP Office resources..... 1269
Training..... 1270

Part 1: Introduction

Chapter 1: Purpose

This document contains descriptions of the configuration fields and the configuration procedures for administering Avaya IP Office Platform using the IP Office Web Manager application. This document principally covers the IP Office Release 12.0.

Intended audience

The primary audience for the Administering Avaya IP Office using IP Office Web Manager is the customer system administrators, implementation engineers and support and services personnel.

Related links

New in IP Office Release 12.0 on page 33
New in IP Office Release 12.1 on page 34
New in IP Office Release 12.1 SP1 on page 36

New in IP Office Release 12.0

The following changes apply for IP Office R12.0:

- **Change of Linux Operating System**

  The version of Linux used by Linux-based IP Office servers has changed from CentOS to Rocky Linux.

  - The new Linux is supported on 64-bit servers only. For Unified Communications Module support see the notes below.
  - For existing Linux-based IP Office systems upgrading to IP Office R12.0, you must upgrade using the processes in Upgrading Linux-based IP Office Systems to R12.0.

- **UCM support in IP Office R12.0 and higher**

  The Unified Communications Module (UCM) cannot support the 64-bit Linux used for IP Office R12.0 and higher. Therefore, you cannot upgraded a UCM to run R12.0.x software. However, Avaya supports UCM modules running R11.1.3.2 software in IP Office R12.0 and higher systems with the following caveats:

  - If the existing Unified Communications Module is running pre-R11.1 software, you must upgrade it to R11.1.3.2 using the processes in the "Upgrading Linux-based IP Office Systems to R11.1" manual.
  - The IP Office system will output a UCM version mismatch alarm each time the IP Office is restarted. You can ignore this alarm.

  - There will be no future updates to the IP Office software components provided on the UCM modules.
  - There will be no any future updates for the CentOS operating system and no security CVE patches for UCM modules.
- **Display of Web Management Version**

  For Linux-based IP Office systems, the **Control Unit** details shown in IP Office Manager now include details for the web management service.
- **End of Support**

  The following are no longer supported:
  - **Web Collaboration**

Related links

Purpose on page 33

New in IP Office Release 12.1

The following changes apply for IP Office R12.1:

IPv6 support

For IP Office R12.1, IP Office systems can support IPv6 features in addition to the existing IPv4 features.

- IP Office supports IPv6 on Linux-based IP Office systems only.
- Use of IPv6 does not require any additional license or subscription.
- IPv4 remains always enabled. The IP Office does not support an IPv6 only mode.

The IPv6 features are:

- **IP Addressing**

  Avaya supports IPv6 on IP Office LAN1. Avaya also supports IPv6 on LAN2 but only when IPv6 is enabled on LAN1 also.
- **DHCPv6 Support**

  You can configure the IP Office to support DHCPv6. It can function as a DHCPv6 server or client on each IP Office LAN.
- **Stateless Address Auto Configuration (SLAAC)**

  You can configure the IP Office to use SLAAC to assign its IPv6 address on LAN1 and/or LAN2. You can also configure the IP Office to respond as an IPv6 router for other devices that are using SLAAC.
- **IPv6 Routing Support**

  You can configure the IP Office with static routes for IPv6 traffic.

- **Avaya Workplace IPv6 Support**

  You can use IPv6 for Avaya Workplace Client extension connection. That includes connection as local and remote extensions.

  - Avaya Workplace Client support for IPv6 with IP Office R12.1 requires Avaya Workplace Client R3.37 and higher.
  - The IP Office licensing and configuration requirements for remote extensions are the same for IPv6 as for IPv4. The IP Office treats any extension using an IPv6 global unicast address not issued by IP Office DHCP as a remote extension.
    - The IP Office must have an FQDN that resolves to both the IPv4 and IPv6 addresses of the IP Office.
    - You must configure the one-X Portal host domain settings (**Configuration** > **Host Domain Name**) with the FQDN of the IP Office server running the one-X Portal service.
  - Avaya Cloud Services do not support IPv6. Therefore, any Avaya Workplace Client using IPv6 cannot use features provided by Avaya Cloud Services. For example:
    - No client registration using email or SSO login.
    - No instant messaging if the IP Office uses Avaya Cloud Services as its messaging server.

- **J100 Phone IPv6 Support**

  You can use IPv6 for J100 Series phone extension connection (except J129). That includes connection as local and remote extensions.

  - IP Office support for IPv6 with J100 phones requires the phones to use J100 R4.1.6.0 or higher firmware.
  - For IPv6, IP Office supports the J100 Series phones (except J129) in dual-stack mode with the signaling address set to IPv6 and the media IP preference set to IPv6 over IPv4 (64). That is the default configuration set in the auto-generated `46xxsettings.txt` file. For Avaya does not support the use of any other combination of signaling and media address mode as that can cause unexpected call failures.
  - The IP Office licensing and configuration requirements for remote extensions are the same for IPv6 as for IPv4. The IP Office treats any extension using an IPv6 global unicast address not issued by IP Office DHCP as a remote extension.
  - The IP Office must have an FQDN that resolves to both the IPv4 and IPv6 addresses of the IP Office.

- **Certificates**

  The IP Office will include its IPv6 addresses when regenerating IP Office signed certificates.

  - If using the IP Office self-signed certificates, you must regenerate the self-signed IP Office certificates after enabling IPv6 support.

All other IP Office connections and features use IPv4 as in previous IP Office releases.

Support for KVM virtual servers

For IP Office R12.1, Avaya supports the deployment of IP Office virtual machines on the Avaya Solutions Platform 130 Appliance R6 platforms (ASP 130 R6). Avaya supplies the ASP 130 R6

with Red Hat Enterprise Linux 8.10 pre-installed and configured to support KVM based virtual machines.

J100 USB Headset support

The J100 R4.1.6 firmware installed by default with IP Office R12.1 includes support for USB HID headsets on J100 Series phones that have USB ports (J159 and J189).

Related links

Purpose on page 33

New in IP Office Release 12.1 SP1

The following changes apply for IP Office R12.1 SP1.

Avaya Wireless DECT

- **Support for Avaya Wireless DECT R5**

  IP Office supports the R5 release of Avaya Wireless DECT as well as the existing R4 release.

  - To reflect this, the IP Office documentation now uses the term Avaya Wireless DECT rather than DECT R4.
  - The R5 firmware is not include in the IP Office R12.1 admin suite installer. You can download the firmware from the Avaya support website.

- **Support for 1500 DECT extensions with Avaya Wireless DECT R5**

  With Avaya Wireless DECT R5, the maximum DECT extension capacity on a Linux-based IP Office primary or secondary server has increased from 750 to 1500.

  - The total extension capacity, DECT and non-DECT, must still remain within the extension capacity of the IP Office system and the whole IP Office solution.

Capacity

- **TLS Extension Capacity**

  The restriction that TLS extensions count as two extensions for IP Office capacity planning does not apply to the Avaya ASP 110 DELL R660 SRVR A2 IPO server.

Related links

Purpose on page 33

Chapter 2: IP Office Web Manager

IP Office Web Manager is a browser based management tool designed to simplify the installation and maintenance process by providing an intuitive and user-friendly management tool that runs on most standard browsers. Web Manager eliminates the need to have Windows PC as it can run on any device that supports standard browsers.

Related links

Supported Web Browsers on page 37
IP Office Types on page 37

Supported Web Browsers

IP Office Web Manager is supported with the latest versions of the following browsers:

- **Windows:** Chrome, Edge, and Firefox.
- **macOS:** Chrome and Safari.

Related links

IP Office Web Manager on page 37

IP Office Types

IP Office is supported on a variety of platforms and running in a number of modes. This affects how web manager is accessed and the menus available within web manager.

Platform	IP Office Mode	Description
IP500 V2	Basic Edition	This mode has its own separate web manager application that is not covered by this version of web manager.
	Essential Edition	These are referred to as 'Standard Mode'. Standard mode systems can be standalone or multiple systems can be linked in a Small Community Network (SCN).

Table continues…

Platform	IP Office Mode	Description
	Preferred Edition	The base license is an Essential Edition license. Additional features are enabled with a Preferred Edition license. Each IP500 V2 is managed separately through its own copy of web manager.
	Server Edition (Expansion Server)	In this mode, the IP500 V2 is part of the Server Edition network below and is managed through the web manager menus of the Server Edition primary server.
Server PC Virtual Server	Server Edition	A Server Edition network can consist of multiple servers, starting with a primary server to which a secondary and expansion servers are then added. All the servers are managed through the web manager provided by the primary server.
	Application Server	This standalone server can run the IP Office one-X Portal and Voicemail Pro services. It can be used in two ways: • With an IP500 V2 running in Preferred Edition mode, it can provide both services. • With a Server Edition, it can replace the one-X Portal service normally provided on the Server Edition primary server.
UCM	Preferred Edition	This server on a card can be installed inside an IP500 V2 running in Preferred Edition mode (see above). It can then provide that system with one-X Portal and Voicemail Pro services. Web manager is used to access and manage those services and the shell mode (see below) settings of the UCM.

Shell Server Mode

Web manager is chiefly used to configure the IP Office service which provide telephony features such as users, extensions and lines.

The IP Office Application Server or UCM module do not provide telephony features. However, those servers still host a version of IP Office service that provides some options, mainly related to security and IP routing settings, necessary to connect with the full IP Office service on other servers. This minimal IP Office service is referred to as a "shell server" mode.

Related links

IP Office Web Manager on page 37

Chapter 3: Logging in to web manager

This section details how to connect to a system using web manager.

Related links

Logging in to Web Manager on page 39
Logging in without a certificate on page 40
Logging out of Web Manager on page 41
Web Manager Service Users on page 41
Changing your password on page 42

Logging in to Web Manager

Use this procedure to log in to web manager via the default web links page provided by the IP Office system.

Before you begin

- You must have an service user ID and password with administration rights. The password for the default `Administrator` account is set during the server's ignition (installation).
- You must know the IP address of the IP Office system.
  - **Server Edition:** Use the address of the primary server. Access via the address of the secondary or expansion server is only supported during server deployment.
  - **UCM module:** Use the address of the IP Office system hosting the module.
  - Use the LAN1 IP address where possible. Some features are not supported when using the LAN2 IP address:
    - Opening a client application, for example IP Office Manager, from web manager.
    - Opening the **Platform View** page from web manager.

Procedure

1. In a web browser, enter the IP address of the IP Office system in the format `http://<ip_address>`.
2. Click on the required link for web manager: Click on:
   - **IP Office:** For the IP Office web manager, click **IP Office Web Manager**.

- **UCM Module:** For the web manager on the UCM module being hosted by the IP Office, click **IP Office Web Manager on UCM**.

3. On the login page, enter a user name and password.
4. (Optional) If you want or need to edit the configuration offline, select the **Offline Mode** checkbox. See Offline Mode on page 52.
5. Click **Login**.
   - Entering an invalid user name or password can cause further access to be blocked. The default is to block access for a minute following 3 failed attempts within 10 minutes. The options for this are set through the system's security settings.
   - You may be prompted to change your password. This is configured through the settings of service user account used.
   - IP Office allows five concurrent sessions using one administrator account. If exceeded, Web Manager displays `Limit of concurrent sessions per user exceeded`. Note that the following are also considered as sessions:
     - If the IP Office Manager application is connected using **SE Central Access**.
     - If the same administrator account has been used to log in any third-party application developed using the IP Office Management SDK.

Result

After logging in:

- Details of the last login using the same service user account are displayed.
- If configured, a security warning may be displayed.
- By default you will be automatically logged out after a period of inactivity set in the web manager preferences. See User Preferences on page 49.

Related links

Logging in to web manager on page 39

Logging in without a certificate

Importing a common certificate into the browser's trusted store provides additional security. If you do not install a certificate, you receive a message that the site is not trusted when logging in to web manager.

When that occurs, you can still continue with the logging in using the process below. This is not recommended for normal operation but is sometimes necessary with accessing a newly installed system.

Procedure

1. In a web browser, enter the IP address of the system in the format `http://<ip_address>/index.html`.

2. Click on **IP Office Web Manager**.
3. A page opens with the statement “This connection is untrusted”. Click **I understand the risks**.
4. Click **Add Exception**.
5. Select **Permanently store this exception**
6. Click **Confirm Security Exception**.
7. Continue to the log in procedure.

Next steps

- See Logging in to Web Manager on page 39.

Related links

Logging in to web manager on page 39

Logging out of Web Manager

Use this procedure to log out of Web Manager.

Procedure

1. In the upper right corner of the Web Manager interface, click **Logout**.
2. You receive a prompt to confirm the log out. Click **OK**.
3. You are logged out of the current session and returned to the login screen.

Related links

Logging in to web manager on page 39

Web Manager Service Users

The IP Office service user account used to login to web manager, determines what actions can be performed. By default the `Administrator` account has full access. However, that can be changed and other service users can be created with different levels of access.

Each service user is configured as a member of various **Rights Groups**. Those group define what the service user can do within web manager (and other interfaces that access the IP Office system). Configuration of service users and rights groups is done through the server's security configuration which is accessible as part of web manager (if your service user account is a member of a rights group with security configuration permission).

Related links

Logging in to web manager on page 39

Changing your password

Use the following process to change your own password.

Procedure

1. Click the icon in the top right corner of the screen.
2. Click **Preferences**.
3. Click the pencil icon next to the **Password** field.
4. Enter your new password into the **Password** and **Confirm Password** fields.
5. Enter your existing password in the **Old Password** field.
6. Click **Update**.

Related links

Logging in to web manager on page 39

Chapter 4: The Web Manager User Interface

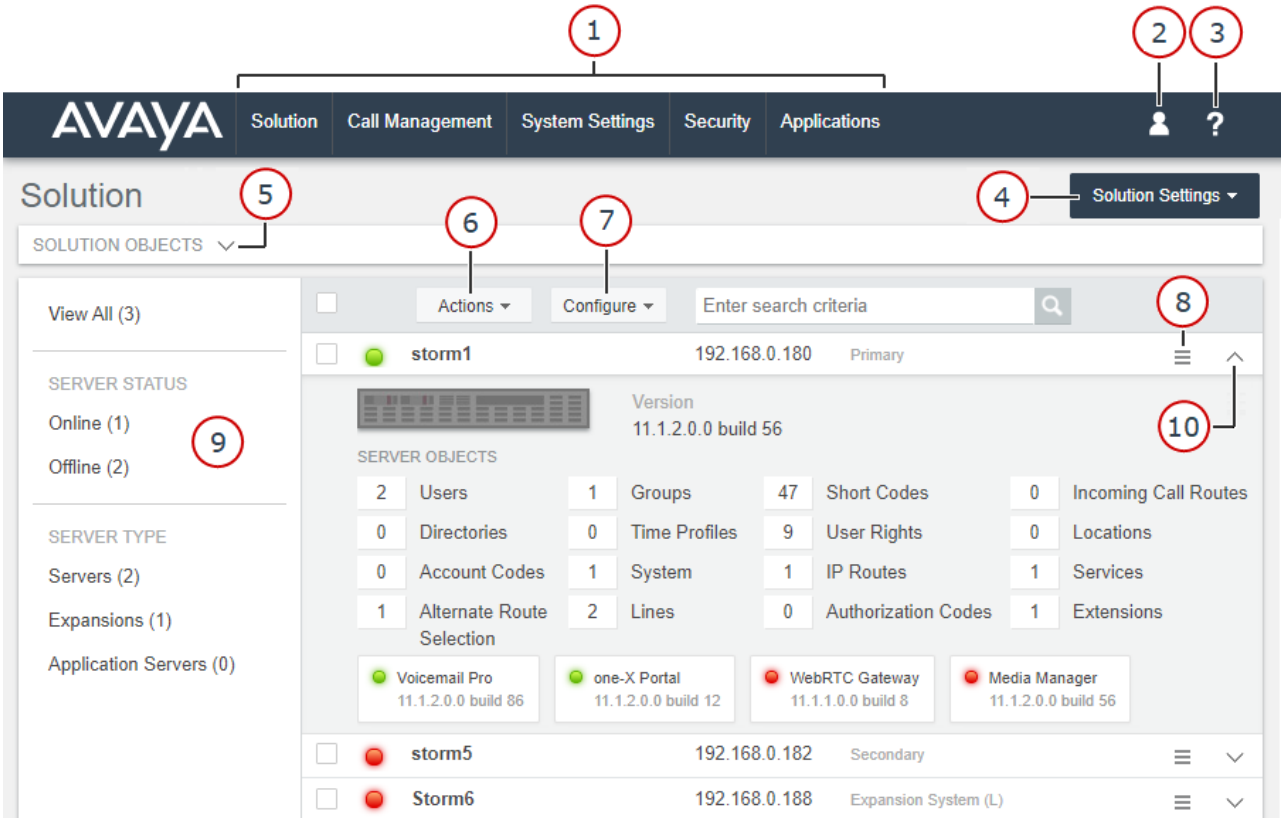
This section provides a summary of the web manager menus and buttons.

Related links

The Menu Bar and Solution Display on page 43
Menu Bar Options on page 45
Solution Button Menus on page 46
User Preferences on page 49
Record Consolidation on page 51
Offline Mode on page 52

The Menu Bar and Solution Display

The screenshot below shows an example IP Office Server Edition network, as seen by accessing the web manager of the primary server. The web manager view differs for other types of IP Office server, but largely contains the same controls.



Item	Description
1. Menu Bar	Use these options to navigate to various sub-menus. The menus vary depending on the type of IP Office system(s) being managed. See Menu Bar Options on page 45.
2. User Preferences	The icon is used to access to access the following options: • **User Preferences** - See User Preferences on page 49. • **Logout** - See Logging out of Web Manager on page 41.
3. Help	The help menu contains: • **Documentation** - Access online help for web manager: Administering Avaya IP Office™ Platform with Web Manager • **Knowledgebase** - Access the IP Office Knowledgebase web site. • **Avaya Support** - Access the Avaya Support web site. • **About** - Display the web manager version details.
4. Solution Settings	Provides options to support web manager operation. Not shown for IP500 V2 web manager. See Solution Button Menus on page 46.

Table continues…

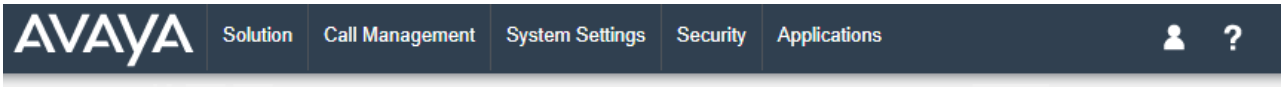
Item	Description
5. Solution Objects	Only shown for IP Office Server Edition. Click to a summary of the number of key configuration items. Clicking on any (**Users**, **Groups**, **Short Codes**, **Directories**, **Time Profiles**, **Locations**, **Account Codes** and **User Rights**), displays a list of those items that can be used to add, edit or delete entries.
6. Actions	Provides a range of configuration actions to be performed on the server or in a network, selected servers. See Solution Button Menus on page 46.
7. Configure	Only shown for IP Office Server Edition. Provides options to add, remove and link the multiple servers in the Server Edition network. See Solution Button Menus on page 46.
8. Server Settings	The icon is used to access a range of server specific options. See Solution Button Menus on page 46. This option is not shown for IP500 V2 web manager. Instead use **Actions** > **Service Commands**.
9. Filter Panel	Filter panels are shown on various screens in web manager. They can be used to show only matching entries.
10. Server Details	Use the icons to show additional details of the server such as its software version, the key services it is running and their versions. Not shown for IP500 V2 web manager.

Related links

The Web Manager User Interface on page 43

Menu Bar Options

The menu bar provides access to the options listed below.



The availability of the **Call Management** and **System Settings** options depend on the type of IP Office system being managed. Similarly, the commands provided by each menu also vary.

Menu	Description
Solution	Display the solution menu. See The Menu Bar and Solution Display on page 43. For IP500 V2 systems, this is the server dashboard.
Call Management	This drop-down menu is available in the menu bar of systems running the full IP Office server to support telephony. It is not shown on IP Office Application servers and UCM modules. For a summary of the options, see Types of Configuration Records on page 56.

Table continues…

Menu	Description
System Settings	This drop-down menu is available in the menu bar of systems running the full IP Office server to support telephony. It is not shown on IP Office Application servers. For a summary of the options, see Types of Configuration Records on page 56.
Security	Access the security settings for the server or servers.
Applications	Access additional menus and services.

Related links

The Web Manager User Interface on page 43

Solution Button Menus

The availability of the **Actions**, **Configure**, **Solution Settings** and ☰ button menus on the **Solution** menu depends on the type of IP Office system being managed. Similarly, the commands provided by each also vary.

The tables in the following sections summarize the options provided by each.

Related links

The Web Manager User Interface on page 43
Actions Menu (Linux-based server) on page 46
Actions Menu (IP500 V2) on page 47
Configure Button Menu on page 47
Solution Settings Button Menus on page 48
The "Hamburger" Server Menu on page 48

Actions Menu (Linux-based server)

Solution > **Actions**

Note that the actions vary depending on the type of server and the number of servers selected. For standalone IP500 V2 servers, see The "Actions" Button Menu (IP500 V2) on page 110.

Setting	Server Edition	Application Server	UCM
Backup	Yes	Yes	Yes
Restore	Yes	Yes	Yes
Transfer ISO	Yes	Yes	Yes
Upgrade	Yes	Yes	Yes
Synchronize Service User and System Password	Yes	–	–
Synchronize Single Sign-On configuration	Yes	–	–
Synchronize APNS configuration	Yes	–	–

Table continues…

Setting	Server Edition	Application Server	UCM
Synchronize APNP System-ID	Yes	–	–
Download Configuration	Yes	–	–
Remote Operations Management	Yes		

Related links

Solution Button Menus on page 46

Actions Menu (IP500 V2)

Solution > **Actions**

This table lists the actions available when managing a standalone IP500 V2 server. For other types of server, see The "Actions" Button Menu on page 104.

Command		IP500 V2
Backup		Yes[1]
Restore		Yes[1]
Upgrade		Yes[1]
Upload Configuration		Yes
Download Configuration		Yes
Backup Status		Yes
Restore Status		Yes
On-boarding		Yes
Initial Configuration		Yes
Service Commands	**Reboot**	Yes
	System Shutdown	Yes
	Erase Security Settings	Yes
	Service Status	Yes
	Erase Configuration	Yes
	Memory Card Start	Yes
	Memory Card Stop	Yes
	Copy to Optional SD	Yes

1. No longer supported by current web browsers.

Related links

Solution Button Menus on page 46

Configure Button Menu

Solution > **Configure**

Web manager on IP Office Server edition is used to manage multiple servers in the network. The **Configure** button provides options for adding, removing and editing the servers in the network.

Setting	Server Edition	IP500 V2	Application Server	UCM
Add System to Solution	Yes	–	–	–
Remove System from Solution	Yes	–	–	–
Convert to Select Licensed System	Yes	–	–	–
Resiliency Administration	Yes	–	–	–
Set All Nodes License Source	Yes	–	–	–
Set All Nodes to Subscription	Yes	–	–	–
Link Expansions	Yes	–	–	–

Related links

Solution Button Menus on page 46

Solution Settings Button Menus

Solution > **Solution Settings**

This menu is used to access the configuration of optional services that can then be used to support the server or servers being managed.

Setting	Server Edition	IP500 V2	Application Server	UCM
View Scheduled Jobs	Yes	–	Yes	Yes
Remote Server	Yes	–	Yes	Yes
Proxy	Yes	–	Yes	Yes
User Synchronization Using LDAP	Yes	–	–	Yes
User Synchronization using Microsoft Teams	Yes	-	-	Yes
Application Server	Yes	–	–	–

Related links

Solution Button Menus on page 46

The "Hamburger" Server Menu

Solution > ☰

The **Solution** page shows details of the server (or servers in a network). The ☰ icon next to each, accesses a menu of commands that can be applied to that server.

Command		Server Edition	IP500 V2	Application Server	UCM
Dashboard		Yes	–	–	–
Platform View		Yes	–	Yes	Yes
Backup		Yes	Yes[1]	Yes	Yes
Restore		Yes	Yes[1]	Yes	Yes
On-boarding		Yes	Yes[1]	Yes	Yes
Launch SSA		Yes	–	Yes	Yes
Service Commands	**Restart IP Office Service**	Yes	–	Yes	Yes
	Erase Configuration	Yes	Yes[1]	Yes	Yes
	Erase Security Settings	Yes	Yes[1]	Yes	Yes
Initial Configuration		Yes	Yes[1]	Yes	Yes
Download Configuration		Yes	Yes[1]	Yes	–
View Upgrade Report		Yes	–	Yes	Yes

1. For standalone IP500 V2 systems, these commands are available through the server's **Actions** menu. See The "Actions" Button Menu (IP500 V2) on page 110.

Related links

Solution Button Menus on page 46

User Preferences

This menu displays settings relating to the operation of web manager. The settings available vary depend on the type of IP Office system.

Navigation: > **Preferences**

Setting	Description	Server Edition	IP500 V2	Apps Server	UCM
CHANGE LOGIN PASSWORD					
Password	Change the password of the currently logged in user. This requires entry of the Old Password plus entering the new the new Password and Confirm Password	✓	✓	✓	✓
USER PREFERENCES					
Accessibility	Enables accessibility features.	✓	✓	–	–
APPLICATION PREFERENCES					

Table continues…

Setting	Description	Server Edition	IP500 V2	Apps Server	UCM
Inactivity Timeout	Default = 10 minutes. The time in minutes after which web manager automatically returns to the login screen if it detects no activity. The minimum time is 10 minutes.	✓	–	✓	✓
Web Manager Logging Level	Default = DEBUG (INFO on UCM) The level of logging information written to the Web Manager log file. The options are in increasing levels of detail are **INFO**, **DEBUG** and **ERROR**.	✓	–	✓	✓
Set current user for configuration synchronization	Sets the current logged in user for all the background configuration synchronization tasks.	✓	–	–	–
Server User / System Password Synchronization	Default = Yes. When enabled, the service user password and the system password are synchronized.	✓	–	–	–
Use Proxy	Default = No. Enables communication with expansion systems using the Primary Server's proxy. Only enable for expansion systems: • in a cloud deployment • behind a NAT router	✓	–	–	–
IP Address	If **Use Proxy** is enabled and an IP address is specified, then the IP address is used during the upgrade of expansion systems.	✓	–	–	–
IP Office IP Address	The IP address of the primary IP Office server to which the application server is providing services.	–	–	✓	–
Consolidate Objects	Default = No. When enabled, global objects are formed. Global objects are common across all systems in the Server Edition solution. See Record Consolidation on page 51.	✓	–	–	–

Table continues…

Setting	Description	Server Edition	IP500 V2	Apps Server	UCM
Minimum Protocol Version	Default = TLS 1.2 This updates the supported TLS version of the Solution Management Application (SMA) server and does not affect the TLS version of the IP Office system. SMA uses port 7070 for integrating management API SDK client applications through TLS connections. The TLS servers allow connections that meet the specified minimum requirement of the selected protocol version and connections from a lower TLS version fail. The available options are TLS 1.0 and TLS 1.2.	✓	–	✓	✓
LOGIN PREFERENCES					
Show Security Warning	If enabled, display a warning dialog whenever a user logs in to web manager.	–	✓	–	–
Warning title	The title for the warning dialog.	–	✓	–	–
Warning text	The text for the warning dialog.	–	✓	–	–

Related links

The Web Manager User Interface on page 43

Record Consolidation

By default, to maintain the configurations of the systems in a Server Edition solution in synch, certain types of configuration records are consolidated. That is, they are replicated in the individual configuration of each system in the network. Consolidation is applied to:

- **Short Codes** - System short codes only.
- **Time Profiles**
- **Account Codes**
- **User Rights**
- **Locations** - Even when consolidated, the **Emergency ARS** and **Fallback System** settings for each location are configured individually on each system.

Consolidate Network Operation

Use of consolidated settings is controlled by the > **Preferences** > **Consolidate Objects** setting.

Setting	Description
Enabled	• Entry and administration of consolidated records is performed only at the solution level. • Those records are then automatically replicated in the configurations of all the systems in the solution but, except for locations, are still only visible and editable at the solution level. • When the configurations are loaded or when this setting is changed to become selected, if any inconsistency between records are found, a **Consolidation Report** is displayed. This report allows selection of whether to update the system to match the primary or to update the primary to match the system.
Disabled	• Entry and administration of consolidated records can be performed at both the solution and individual system levels. • Records entered and edited at the solution level are still automatically replicated in the configurations of all the systems in the solution. Each record displays a label on the record indicating that it is a record that is shared across the solution. • If a shared record is edited at the individual system level, that copy of the record is no longer shared with the other systems. It will not be updated by any changes to the solution level version of the same record. • No consolidation checking for inconsistencies is done when the configurations are loaded.

Related links

The Web Manager User Interface on page 43

Offline Mode

By default, Web Manager operates in real time and configuration changes are applied to the IP Office system immediately. However, some settings can only be changed in offline mode. Web manager will indicate when that is the case.

In this mode, you can make multiple changes to the configuration and then apply them using the **Save to IP Office** action. Depending on the settings changed, this may cause a reboot of the IP Office service and ends all calls currently in progress.

Navigation: > **Offline Mode**

Using Offline Mode

To select offline mode, click > **Offline Mode**. Once in **Offline Mode**:

- The > **Offline Mode** changes to **Save to IP Office**.
- The **Save to IP Office** option is also available above the menu bar.

Saving Setting in Offline Mode

After clicking **Save to IP Office**, web manager displays a save dialog with the following settings. Configure the menu as required and click **OK**.

Setting	Description
IP Office	Select the system to which settings should be saved. In a Server Edition network, more than one server may be shown.
Change Mode	Select the method of saving: • **Merge** - This method is automatically selected if none of the configuration changes made require a system reboot. If this method is used for a configuration that includes changes that do require a reboot, those changes are not applied until the system is manually rebooted. • **Immediate** - This method saves the new configuration changes and then restarts the system. Any current calls and services in progress are ended. This method is automatically selected if any of the changes made so far require a reboot before they are applied to the system. • **Free** - This method allows the **Incoming Call Barring** and **Outgoing Call Barring** options to be used. The system reboots when the criteria for the selected options are matched. • **Timed (HH:MM)** - This method reboots the system at the selected time. It can also be used with the call barring options to only reboot after the set time when the selected options are matched.
Reboot Time	Set the time for the reboot if **Timed (HH:MM)** is the selected save method.
Incoming Call Bar	This option can be used with the **Free** and **Timed** reboot methods. When selected, the system bars any further incoming calls. However, it allows existing calls to continue until they are ended.
Outgoing Call Bar	**Outgoing Call Barring** - This option can be used with the **Free** and **Timed** reboot methods. When selected, the system bars any further outgoing calls. However, it allows existing calls to continue until they are ended. **Warning:** • This option also bars the making of emergency calls. Therefore, it should be used with caution.

Settings that can only be edited in Offline Mode

The following table lists the configuration settings which can only be edited in **Offline Mode**.

Settings	Offline Only	Exceptions
Call Management > **Extensions** > **Edit Extension**		
Common	All	
H323	All	
SIP VoIP	All	
SIP T38 Fax	All	
IP DECT	Some	Can be edited online except **Reserve License**.
System Settings		
Licenses > **Remote Server**	Some	Only **Reserved Licenses** can be edited online.

Table continues…

Settings	Offline Only	Exceptions
System Settings > **System**		
System	Some	Can be edited online except **Locale** and **Favor RIP Routes over Static Routes**.
Voicemail	Some	Can be edited online except **Voicemail Type** and **Voicemail IP Address**.
System Events	All	
SMTP	All	
DNS	All	
LAN > **Settings**	All	
LAN > **VoIP**	All	
LAN > **Network Topology**	All	
LAN > **DHCP Pools**	All	
VoIP	All	
VoIP Security	All	
WAN Port	All	
System Settings > **System** > **Telephony**		
Telephony	Some	Can be edited online except **Companding LAW** and **Media Connection Preservation**.
Tones and Music	All	
SM	All	
System Settings > **Line**		
Legacy SIP DECT Line > **SIP DECT Base**	All	
Legacy SIP DECT Line > **SIP DECT VoIP**	All	
Analog Line > **Line Settings**	Some	Can be edited on line except **Network Type** setting.
Analog Line > **Line Options**	All	

Table continues…

Settings	Offline Only	Exceptions
BRI Line > Line Settings	Some	The following settings must be edited offline. • **Line Sub Type** • **Network Type** • **TEI** • **Add 'Not-end-to-end ISDN' Information Element** • **Progress Replacement** • **Clock Quality** • **Force Number Plan to ISDN** Decreasing the **Number of Channels** setting requires a “merge with service disruption”. When the configuration file is sent to the system, active calls on the deleted channels are cleared.
E1 PRI Line	All	
E1 PRI Channels	All	
E1–R2 Options	All	
E1-R2 MFC Group	All	
E1-R2 Advanced	All	
US T1 Line	All	
T1 Channels	All	
T1 ISDN	All	
T1 ISDN Channels	All	
T1 ISDN TNS	All	
T1 ISDN Special	All	
T1 ISDN Call By Call	All	

Related links

The Web Manager User Interface on page 43

Chapter 5: Displaying and Managing Configuration Records

The system configuration consists of collections of different types of records. For example user records, group records, etc. The menu bar across the top of the browser window is the main route for accessing the lists of particular records types.

From the lists, which you can sort and filter, you can add, edit and delete records.

Related links

Types of Configuration Records on page 56
Displaying Configuration Records on page 59
Filtering the list on page 60
Searching the list on page 60
Sorting the list on page 60
Adding a New Record on page 61
Quick Edit on page 61
Editing an Existing Entry on page 62
Editing Multiple User Records on page 62
Deleting a Record on page 63
Deleting Multiple Records on page 63

Types of Configuration Records

The following different types of configuration records can be selected from the menu bar options.

Call Management

This drop-down menu is available in the menu bar of systems running the IP Office service to support telephony. It is not shown on IP Office Application servers and Unified Communications Module.

Sub-Menu	Description
Auto Attendants	Auto-attendants are services that the system can provide to answer calls and prompt the caller for which service they require or who they want to talk to. Auto attendants can be used as the destination for incoming call routes.
Conferences	In addition to ad-hoc and personal conference features, systems support system meet-me conferences.
Extensions	Each physical phone (desk phone) registered with the system requires a matching extension record in the system configuration.
Groups	Groups are collections of multiple users. Each group has an extension number and can be used as the destination for calls.
Users	Users are the individual users who make and answer calls. They can do this via physical phones or softphone applications.

System Settings

This drop-down menu is available in the menu bar of systems running the IP Office service to support telephony. It is not shown on IP Office Application servers and Unified Communications Module.

Menu/Sub-Menu	Description
Account Code	Account codes can be used to track calls. Users can either voluntarily enter an account code during a call, or for certain numbers, be forced to enter a valid account code in order to make a call.
Alternate Route Selection	Alternate Route Selection (ARS) records are used to control the routing of outgoing calls. Short codes within the ARS record are matched against the number to dial to see which line to uses or whether it is barred and to change the number actually dialed from the system if necessary.
Authorization Code	Each authorization code is associated with a particular user. That code allows the user to temporarily override the settings of another users phone and make a call from it using their own settings.
Firewall Profile	Configure firewall profiles which can then be applied to IP connections.
Incoming Call Route	Incoming call routes records are used to control the routing of incoming calls. Various aspects of the incoming call (for example the line it is on and the caller ID) are compared for matches to the available ICR records. The destination settings in the ICR record that is the best match are then used to route the call.
IP Route	This menu is used to configure static IP routes to control the routing of matching IP addresses and address ranges.
Licenses	This menu is used to configure the license source settings on non-subscription systems.
Line	Lines are used for external calls, both incoming and outgoing.
Locations	Location records can be used to identify where particular extensions are physically located and to apply settings that need to differ from that location.
RAS	A Remote Access Server (RAS) is a piece of computer hardware which sits on a corporate LAN and into which employees dial on the public switched telephone network to get access to their email and to software and data on the corporate LAN.

Table continues…

Menu/Sub-Menu	Description
Services	Services are used to configure the settings required when a user or device on the LAN needs to connect to a another network. Services can be used when making data connections via trunk or WAN interfaces. Once a service is created, it can be used as the destination for an IP Route record.
Short Codes	Dialing by users on the system can be compared to short codes. When a match occurs, the matching short code sets what should happen. This may be the triggering of some feature, changing a system setting, or changing the dialed number.
Subscription	On subscription mode systems, display the subscriptions obtained and the settings used.
System Directory	The system directory contains records for external contacts, that is their names and numbers. These can be displayed on phones in order to make outgoing calls. They can also be used to match a name to the number on incoming calls.
System	This menu gives access to a set of sub-menus for settings that control system-wide behavior.
Time Profiles	Time profiles contains time, date and weekly schedule settings. Using those each time profile is currently either ‘true’ or ‘false’. That value is used to change the behavior of other types of record that can be linked to the time profile such as incoming call routes.
Tunnel	These menus can be used to create L2TP and IPSec tunnels to other servers and services. Supported on IP Office IP500 V2 systems only.
User Rights	User rights can be used to override some of the individual settings of some users. Changes to the user rights are then automatically applied to all those users rather than having to individually edit each user.
WAN Port	Use these menus to configure physical and virtual WAN ports.

Security/Security Settings

The **Security** menu allows you access to the overall security settings of the system.

Menu/Sub-Menu	Description
General	General settings such as the password rules for service users and for general system users.
System	General system settings for ports.
Services	The ports on which the system’s services listen for access and the security used for that access.
Rights Groups	Rights groups define what the different security service users that are members of the group can do.
Certificates	This menu lists the security certificates stored by the system and allows processes such as adding and changing certificates.
Service Users	Service users are the accounts used by administrators and services to connect to the system. The service user's permissions are defined by the **Rights Groups** to which they belong.

Related links

Displaying and Managing Configuration Records on page 56

Displaying Configuration Records

There are two types of configuration record:

- For some records there is only one record for the server. Selecting the option from the menu bar displays the settings of that record:
  - For servers in a Server Edition network, for **System** and **Security** settings, each server has its own configuration record. A list of servers is displayed from which you can select which server's configuration record you want to access.
- For other records, such as users and group, there can be multiple records of that type. You can add or delete records. Selecting the appropriate option from the menu bar displays a list of all the existing records.

Procedure

1. From the menu bar, select the type of configuration record that you want to manage.
   - If there is only one configuration record of that type, its settings are displayed.
   - For Server Edition, if a list of servers is displayed, selected the server whose configuration record you want to view.
   - For other record types, a list of all the existing records is displayed.
2. When a list of configuration records is displayed, use the following methods to manage those records:
   - **Sort:** See Sorting the list on page 60.
   - **Search:** See Searching the list on page 60.
   - **Filter:** See Filtering the list on page 60.
   - **Add:** See Adding a New Record on page 61.
   - **Edit:** There are several ways in which you can edit the entries shown in a list of configuration entries.
     - **Quick Edit:** For extensions, users and groups, you can edit the displayed details of a record directly in the list. See Quick Edit on page 61.
     - **Full Edit:** See Editing an Existing Entry on page 62.
     - **Edit Multiple:** For users, you can select and edit multiple entries. See Editing Multiple User Records on page 62.
   - **Delete:** See Deleting a Record on page 63.
3. To stop displaying the list, click **Solution**.

Related links

Displaying and Managing Configuration Records on page 56

Filtering the list

You can use the checkboxes on the right to what records you want to display. If no check boxes are selected, the list defaults to displaying all records.

Procedure

1. Use the checkboxes to filter the list of matching records.
   a. Click on the checkbox or its label to select or deselect it.
   b. To remove all the currently selected check boxes in a particular category, click on the **X** icon.
   c. To deselect all check boxes, click on **Show All**.
2. When using the actions above, after a short pause the list is updated to only show records that match the selected checkboxes or all records if no checkboxes are selected.

Related links

Displaying and Managing Configuration Records on page 56

Searching the list

You can filter the list by performing a search for entries that match a keyword you enter. The search box at the top of the list indicates the column names to which the search is applied.

You can use a search in conjunction with the filtering checkbox options.

Procedure

1. In the search box at the top of the list, enter your search term.
2. Click on the icon.
3. The list of entries is filtered to show only matching entries.
4. To clear the search, either manually remove your search terms or click on **Show All**.

Related links

Displaying and Managing Configuration Records on page 56

Sorting the list

The list of configuration records can be sorted.

Procedure

1. Click on the column header. The list is sorted using that column and an icon is shown next to the column header.
2. To reverse the direction of the sorting, click on the same column header again.

Related links

Displaying and Managing Configuration Records on page 56

Adding a New Record

Use this process to add a new configuration record to the existing list of records.

- New users, extensions and SIP trunks created using templates. Refer to the configuration settings for those records for details. See Using User and Extension Templates on page 81.

Procedure

1. Click the **+ Add** button.
   - In some cases, you are prompted to select a sub-type. For example, if adding an extension, you may be prompted to select either **SIP** or **H.323**.
   - If the system is part of a network of servers, you may also be prompted for which server should host the new configuration record.
2. Use the form to enter the details as required.
3. When you have configured the record as required, click **Create**.
   - When creating a user record, the system will prompt you whether it should also create a matching extension record.

Related links

Displaying and Managing Configuration Records on page 56

Quick Edit

Each list of configuration entries displays keys settings. For extensions, users and groups, those key settings can be edited directly in the list rather than having to access the full set of settings for each record.

Procedure

1. Click on the existing details displayed for the record that you want to edit.
2. The existing details change to a set of editable fields. Change these details are required.
3. When completed, click **Save**.

Related links

Displaying and Managing Configuration Records on page 56

Editing an Existing Entry

Use the following process to edit an entry in the currently displayed list.

Procedure

1. Click the pencil icon next to the entry.
2. Change the settings as required.
3. When completed, click **Update**.

Related links

Displaying and Managing Configuration Records on page 56

Editing Multiple User Records

The list of user entries can be used to edit multiple users at the same time. You can select which settings to edit and apply to all the users.

Procedure

1. Click **Call Management** > **Users** and sort/filter the list as required.
2. Click the checkbox next to each of the users you want to edit.
3. Click **Edit Multiple**.
4. For each setting that you want to change for all the selected users:
   a. Click the checkbox next to the setting.
   b. Change the setting to the required value for all the selected users.
   c. Repeat this process for any other setting that you want to change for all the selected users.
5. When completed, click **Update**.

Related links

Displaying and Managing Configuration Records on page 56

Deleting a Record

Use the following process to delete a record from the list.

- Before deleting an entry, check that it is not being used as the destination for any other functions such as an auto-attendant action or incoming call route.
- For IP500 V2 servers, configuration records that match physical ports in the system (extension and line ports) cannot be deleted. If removed, the record is automatically recreated with default settings when the system is next restarted.

Procedure

1. Click on the trash can icon next to the entry to delete.
2. Click **Yes** to confirm the deletion.

Related links

Displaying and Managing Configuration Records on page 56

Deleting Multiple Records

Use the following process to delete several records from the list.

- Before deleting an entry, check that it is not being used as the destination for any other functions such as an auto-attendant action or incoming call route.
- For IP500 V2 servers, configuration records that match physical ports in the system (extension and line ports) cannot be deleted. If removed, the record is automatically recreated with default settings when the system is next restarted.

Procedure

1. Select the checkbox next to the records to be deleted.
2. Click the **Delete** button at the top of the lists.
3. Click **Yes** to confirm the deletion.

Related links

Displaying and Managing Configuration Records on page 56

Chapter 6: The Setup Wizard/Initial Configuration

IP Office Web Manager displays the setup wizard when it connects to a new IP Office server for the first time (except IP Office Application Server and Unified Communications Module). The setup wizard consists of a number of panels, each of which you can use to configure a different area of the IP Office server configuration.

- Click on a panel to access its settings.
  - On a new IP Office system, you can only access the panels is sequence, starting with the **System** panel.
  - After you have configured the settings in a panel, the panel displays a summary of those settings and you can access the next panel.
  - After you have configured the settings within a panel, you can return to it at any time.
- Some of the panels alter settings that require an IP Office system reboot. Therefore, on a new server the setup wizard run in offline mode. When completed, clicking **Save to IP Office** applies the settings and restarts the IP Office.
- The **System** panel is also call the **Initial Configuration Utility** (ICU).
  - On system's that have already completed initial configuration, you can return to this menu using ☰ > **Initial Configuration** (IP500 V2: **Actions** > **Initial Configuration** for IP500 V2).
- On standalone IP500 V2 systems, IP Office Web Manager displayed the panels as the system's **Solution** display and as the dashboard (**Solution** > **Server Menu** > **Dashboard**).

Related links

Setup Wizard: Panels Summary on page 65
Setup Wizard: System Panel (Initial Configuration Utility) on page 66
Setup Wizard: VoIP on page 70
Setup Wizard: Voicemail on page 74
Setup Wizard: Subscription on page 76
Setup Wizard: Licensing on page 77
Setup Wizard: User on page 77
Setup Wizard: Groups on page 77
Setup Wizard: Lines on page 78
Setup Wizard: Incoming Call Routes on page 78
Setup Wizard: Outgoing Call Routes on page 79

Setup Wizard: Panels Summary

The following tables provide a brief summary of the role of each panel. It also indicates their availability which may depend on other settings or the type of IP Office server.

Panel	Description
System	Configure general system settings such as IP Office mode, locale and IP addresses.
VoIP	Configure the system's settings for H.323 and SIP telephony.
Voicemail	Configure the system's use of voicemail to handle unanswered and missed calls.
Licensing	Configure the system PLDS license settings and upload a license file. This panel is not shown on IP Office subscription systems.
Subscription	Display details of the system subscription settings and subscriptions. This panel is only shown on IP Office subscription systems.
Users	Configure the system users.
Groups	Configure groups of users. Each group has its own extension number which allows it to be used as the destination for calls.
Lines	Configure external telephone lines.
Incoming Call Routes	Configure the destination for incoming external calls based on the lines being used and the incoming telephone number.
Outgoing Call Routes	Configure the settings applied to outgoing external calls by default and for particular users if required.

Panel	Server Edition		IP500 V2
	Primary Secondary	Expansion	
System	✓	✓	✓
VoIP	✓	×	✓
Voicemail	✓	×	✓
Licensing	✓	×	✓
Subscription	✓	×	✓
Users	✓	×	✓
Groups	✓	×	✓
Trunks	✓	×	✓
Incoming Call Routing	✓	×	✓
Outgoing Call Routing	✓	×	✓

Related links

The Setup Wizard/Initial Configuration on page 64

Setup Wizard: System Panel (Initial Configuration Utility)

This is the only mandatory panel in the setup wizard. This menu is also called the **Initial Configuration** utility.

On IP Office systems that have already completed initial configuration, you can return to this menu using ☰ > **Initial Configuration** (IP500 V2: **Actions** > **Initial Configuration**).

Common Settings

Option	Description
System Mode	Sets the operating mode of the server. The options available depend on the type of server platform. For further details, refer to the appropriate IP Office deployment manual. • For Linux-based servers: - **Server Edition** - **Server Edition - Select** - **Server Edition - Subscription** • For an IP500 V2 server: - **IP Office Standard Edition** - **IP Office Subscription** - **IP Office ACO ATA Gateway** - **Server Edition Expansion** - **Server Edition Expansion - Subscription** • For an existing IP Office being reconfigured, the choice of system modes is restricted. For example, you cannot change a subscription mode system to non-subscription mode. In order display the full set of options, you must default the IP Office system configuration .
System Name	A name to identify this system. This is typically used to identify the configuration by the location or customer's company name. Some features require the system to have a name. • This field is case sensitive and within any network of systems must be unique. • Do not use <, >, |, \0, :, *, ?, . or /.
Retain Configuration Data	This option is shown for existing servers where the initial configuration menu is being rerun. • If cleared, the existing configuration of the IP Office system is defaulted. • If enabled, the existing configuration is retained. However, some elements of that configuration may be invalid or ignored. It is your responsibility to ensure that the final configuration is valid.

Table continues…

Option	Description
Locale	This setting sets default telephony and language settings based on the selection. It also sets various external line settings and so must be set correctly to ensure correct operation of the system. See Avaya IP Office Locale Settings. For individual users, the system settings can be overridden through their own locale setting (**User** > **User** > **Locale**).
Default Extension Password	Default = Existing default extension password The field provides you with option to view and edit the existing default extension password. The default extension password is set up during IP Office installation either by the administrator or is randomly generated by the system. The system generated random password is of 10 digits. Use the Eye icon to see the existing default password. The password must be between 9 to 13 digits.
Hosted Deployment	This option is only used on non-subscription Server Edition system. If enabled, it indicates that the system is a hosted deployment.
Services Device ID	This setting is shown for Server Edition servers only. The ID is displayed on the **Solution** view, **System Inventory** and on the **System** > **System** tab in the configuration. • The value can be changed using the **Device ID** field on the **System** > **System Events** configuration tab.

Subscription System Details

These details are only shown for subscription mode systems. They are used by the system to obtain its subscriptions. They details required are supplied when the system if registered for subscription.

Name	Description
System ID	This is a fixed value against which the system's subscriptions are issued and validated. • For an IP500 V2 system, this ID is based on the System SD card installed in the system.
Customer ID	The customer ID specified when the system was registered for subscriptions.
License Server Address	The address of the server which provides the system with its subscriptions.

LAN Configuration Settings

Name	Description
Public LAN Interface	Select which of the server's LAN interfaces is connected to the customer network routed to the external internet. Additional IP Route details are added to the system configuration based on this choice.
Gateway	The address of the default gateway on the customer network to which non-LAN traffic should be routed. After initial configuration, a default IP route is created, using this address and the selected **Public LAN Interface** setting.

Table continues…

Name	Description
DNS Server	The address used on the customer network for resolution of DNS queries. This is either the customer's DNS server or the DNS address provided by their internet service provider.
LAN1 CONFIGURATION/LAN2 CONFIGURATION Separate sets of LAN configuration details are shown for LAN1 and LAN2.	
IP Address	The base IP address for the LAN. The defaults are 192.168.42.1 for LAN1 and 192.168.43.1 for LAN2. If the server is acting as the DHCP server for the LAN, this is the starting address for the DHCP address range.
IP Subnet Mask	Default = 255.255.255.0. This is the IP subnet mask used with the IP address.
DHCP Mode	Select whether the server performs DHCP for the LAN. • **Server** - When this option is selected, the system will act as a DHCP Server on this LAN, allocating address to other devices on the network and to PPP Dial in users. - Devices on requesting an address are allocated addresses from the bottom of the available address range upwards. - Dial In users are allocated addresses from the top of the available range downwards. - If the control unit is acting as a DHCP server on LAN1 and LAN2, Dial in users are allocated their address from the LAN1 pool of addresses first. • **Disabled** - When this option is selected, the system will not use DHCP to get or issue IP addresses. • **Dial In** - When this option is selected, the system will allocate DHCP addresses to PPP Dial In users only. On systems using DHCP pools, only addresses from a pool on the same subnet as the system's own LAN address will be used. • **Client** - When this option is selected, the system request its IP Address and IP Mask from another DHCP server on the LAN.
Enable NAT	Default = Off. Shown for IP500 V2 systems only. This setting controls whether NAT should be used for IP traffic from LAN1 to LAN2.

Solution Settings

These settings are shown for Linux-based systems. The options vary depending on the server's role in the network (primary, secondary or expansion).

Name	Description
Server Edition Primary Server	For secondary and expansion servers, specify the address of the primary server.
Server Edition Secondary Server	For primary and expansion servers, specify the address of the secondary server.

Table continues…

Name	Description
WebSocket Password	For each of the addresses set above, a bi-directional WebSocket connection is created. A matching password must be set at each end of the line.
DNS Server	This is the IP address of a DNS Server. If this field is left blank, the system uses its own address as the DNS server for DHCP client and forwards DNS requests to the service provider when **Request DNS** is selected in the service being used (**Service** > **IP**).

Time Settings

These settings are shown for non-subscription IP500 V2 servers only. They are only shown in the IP Office Web Manager initial configuration menu.

Name	Description
Time Setting Configuration Source	An accurate time source and settings are vital to many functions, including any services that use certificates. Avaya recommend that you use SNTP and a reliable source such as `time.google.com`. • **None** Set the system date and time manually using a phone with **System Phone Rights** (**User** > **User**). • **SNTP** Use a list of SNTP servers to obtain the UTC time. The IP Office tries the addresses in the list one at a time in order until there is a response. The system makes a request to the specified addresses following a reboot and every hour afterwards. • **Voicemail Pro/Manager** *(Obsolete)* The Windows-based Voicemail Pro service and the IP Office Manager program can act as RFC868 Time servers for the IP Office system. Use of other RFC868 server sources is not supported. They provide both the UTC time value and the local time as set on the PC. The system makes a request to the specified address following a reboot and every 8 hours afterwards.
The following setting is available when the **Time Setting Configuration Source** is set to **SNTP**.	
Time Server Address	Default = Blank A list of SNTP servers the used to obtain the UTC time. • The records in the list are used one at a time until there is a response. The system makes a request to the specified addresses following a reboot and every hour afterwards.

Centralized Management

The following settings are used for IP Office systems being deployed as branch systems in a network managed using System Manager. Refer to the Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager manual.

Name	Description
Under Centralized Management	When selected, the additional fields below are shown.
SMGR Address	Enter the IP address of the System Manager server managing the branch network.
Redundant SMGR Address	Enter the IP address of the secondary System Manager server managing the network.
SMGR Community	The shared community name for servers within the branch network.
SNMP Device ID	The unique SNMP ID for the IP Office server within the network.
Trap Community	The public name for sending SNMP trap alarms.
SCEP Domain Certificate Name	The domain name for SCEP (Simple Certificate Enrollment Protocol) operation in the branch network.
Certificate Enrollment (SCEP) Password	The password for requesting certificates from the network's SCEP server.

Related links

The Setup Wizard/Initial Configuration on page 64

Setup Wizard: VoIP

You can use this panel to configure the H323 Gatekeeper and SIP Registrar support provided on each of the system's LAN interfaces.

LANS

Field	Description
Select LAN	Use this control to switch between configuring LAN1 or LAN2.

H.323 Gatekeeper

These settings relate to the H.323 extension support provided by the system on the currently selected LAN.

Field	Description
H.323 Gatekeeper Enable	Default = Off If enabled, the system will support H.323 trunk and extension connections on the LAN.

Table continues…

Field	Description
H.323 Signaling over TLS	Default = Disabled. For hosted deployments, default = Preferred. When enabled, TLS is used to secure the registration and call signaling communication between IP Office and endpoints that support TLS. The H.323 phones that support TLS are 9608, 9611, 9621, and 9641 running firmware version 6.6 or higher. When enabled, certificate information is configured in the `46xxSettings.txt` file on IP Office and automatically downloaded to the phone. When IP Office receives a request from the phone for an identity certificate, IP Office searches its trusted certificate store and finds the root CA that issued its identity certificate. IP Office then provides the root CA as an auto-generated certificate file named `Root-CA-xxxxxxxx.pem`. For information on IP Office certificates, see **Security** > **Certificates**. The options are: • **Disabled**: TLS is not used. • **Preferred**: Use TLS when connecting to a phone that supports TLS. • **Enforced**: TLS must be used. If the phone does not support TLS, the connection is rejected. When set to **Enforced**, the **Remote Call Signaling Port** setting is disabled. If TLS security is enabled (**Enforced** or **Preferred**), it is recommended that you enable a matching level of media security on **System Settings** > **System** > **VoIP Security**.
H.323 Remote Extn Enable	Default = Off The system can be configured to support remote H.323 extensions in the case where NAT is used in the connection path. This could be the case where the IP Office is located behind a corporate NAT/Firewall router and/or the H.323 phone is located behind residential NAT enable router. Currently, only 9600 Series phones are supported as H.323 remote extensions.
Remote Call Signaling Port	Default = 1720 The call signaling port used for remote H.323 extensions.
Auto-create Extension	Default = Off If enabled, the system will automatically create a extension entry in its configuration in respond to successful registration by an H.323 IP phone. • This setting is automatically disabled 24-hours after being enabled.
Password	Default = Blank If set, sets the password for extension registration using auto-creation. If left blank, the system Default Extension Password setting is used.

Table continues…

Field	Description
Auto-create User	Default = Off If enabled, the automatic creation of an H.323 extension entry in the system configuration also causes the automatic creation of a matching user entry for the extension.

SIP Trunks

Field	Description
SIP Trunks Enable	Default = On. This settings enables support of SIP trunks. It also requires entry of **SIP Trunk Channels** licenses. Enabling **SIP Trunks Enable** allows configuration of the **RTP Port number Range (NAT)** settings.

SIP Registrar

These setting relate to the support of SIP extensions on the selected LAN.

Field	Description
SIP Registrar Enable	Default = Off Used to set the system parameters for the system acting as a SIP Registrar to which SIP endpoint devices can register. Separate SIP registrars can be configured on LAN1 and LAN2. Registration of a SIP endpoint requires an available **IP Endpoints** license. SIP endpoints are also still subject to the extension capacity limits of the system.
Auto-create Extn/User	Default = Off. The field to set up auto creation of extensions for SIP phones registering themselves with the SIP registrar. If selected, the system prompts you to enter and confirm the password is used for subsequent auto creation of extensions. • This setting is not supported on systems configured to use WebLM server licensing. • For security, any auto-create settings set to On are automatically set to Off after 24 hours.

Table continues…

Field	Description
SIP Remote Extn Enable	Default = Off. The system can be configured to support remote SIP extensions in the case where NAT is used in the connection path. This could be the case where the IP Office is located behind a corporate NAT/Firewall router and/or the SIP phone is located behind residential NAT enable router. • This option cannot be enabled on both LAN1 and LAN2. • The use of this option and the interaction and configuration of external third party elements is beyond the scope this help file. In the case where the public IP address of the corporate router is unknown, the LAN's Network Topology settings should be used to configure a STUN Server. Enabling **SIP Remote Extn Enable** allows configuration of: • the **Remote UDP Port**, **Remote TCP Port**, **Remote TLS Port** settings • the **Port Number Range (NAT)** settings
SIP Domain Name	Default = Blank This value is used by SIP endpoints for registration with the IP Office system. SIP endpoints register with IP Office using their SIP address that consists of their phone number and IP Office SIP domain. Since IP Office does not allow calls from unauthorized entities, the SIP domain does not need to be resolvable. However, the SIP domain should be associated with FQDN (Fully Qualified Domain Name) for security purposes. The entry should match the domain suffix part of the SIP Registrar FQDN below, for example, `example.com`. If the field is left blank, registration uses the LAN 1, LAN2, or public IP address. **Note:** For Avaya SIP telephones supported for resilience, the **SIP Domain Name** must be common to all systems providing resilience.
SIP Registrar FQDN	Default = Blank The fully-qualified domain name to which the SIP endpoint send their registration requests. For example, `sbc.example.com`. • This FQDN is also used for **Avaya Cloud Services** and **Avaya Push Notification Services** The customer DNS must resolve this FQDN to an IP address that routes to the IP Office. That is: • For local extensions, the IP address of the IP Office LAN. • For remote extensions, the external IPv4 address of the Avaya SBC or customer firewall that routes to the IP Office.

Related links

[The Setup Wizard/Initial Configuration](#) on page 64

Setup Wizard: Voicemail

Voicemail

Name	Description
Voicemail Type	Sets the type of voicemail service used by the system. The options supported depend on the type of IP Office system. • **Server Edition Systems** These systems are supported by **Voicemail Pro** running on the primary server. All other servers in the Server Edition network should be set to **Centralized Voicemail**. • **Standalone IP500 V2 Systems** These can support a range of options: - **Voicemail Pro** - Use the Voicemail Pro service provided by an IP Office Application server. - **Centralized Voicemail** - In an SCN network of IP500 V2 systems, only the Voicemail Pro server associated with one IP500 V2 system holds the messages and recording (the centralized voicemail server). All other systems should be set to **Centralized Voicemail** or **Distributed Voicemail**. - **Embedded Voicemail** - Use the voicemail service provided internally by the system itself. This uses the system's System SD card to store messages and prompts. - **Group Voicemail** - Used with some 3rd-party voicemail services. - **Distributed Voicemail** - In an SCN network of IP500 V2 systems, only the Voicemail Pro server associated with one IP500 V2 system holds the messages and recording (the centralized voicemail server). However, the other IP500 V2 systems can be associated with their own Voicemail Pro server which handles that systems calls. - **Analog Trunk MWI** - Use voicemail provided by the analog trunk provider. - **Voicemail Pro on UC Module** - Use the Voicemail Pro service provided by a UCM module installed in the IP500 V2 control unit. • Only select this option is the module is already installed and fully configured. Otherwise, select **Voicemail Pro**. The settings are automatically changed during the configuration of the UCM module.
Voicemail IP Address	Default = Primary Server IP Address The IP address of the server hosting the voicemail service for the IP Office system.

Hold Music

This section is used to define the source for the system's default music on hold source. Once the system is installed, additional music on hold sources can be configured for specific groups and incoming call routes

- You must ensure that any MOH source you use complies with copyright, performing rights and other local and national legal requirements.

Name	Description
System Source	Select the source the system should use its default music on hold. The options available depend on the type of system. • **WAV File** - Use a WAV file called `HoldMusic.wav`. The file can be uploaded using the controls below. Note that on Linux systems, the file name is case sensitive. • **External** - IP500 V2 systems only. Use the audio source connected to the back of the control unit. • **Tone** - Use of a repeated double tone generated by the system. This tone is also automatically used if, for any of the .WAV file options the has not yet been successfully uploaded. • **WAV (Restart)**: Identical to **WAV File** above except that for each new listener, the file plays from the beginning. Not supported on IP500 V2 systems.
Select a File **Upload**	If use of a wav file is selected, use these fields to select and upload the file to the system. The file should be in the following format: • PCM • 8kHz 16-bit • Mono • Maximum length: - IP500 V2 = 90 seconds. - Linux-based Server = 600 seconds.

Auto Attendants

These settings are shown for an IP500 V2 systems with the **Voicemail Type** set to **Embedded Voicemail**. It allows configuration of auto-attendant services. These can then be used as the destination for external calls in incoming call routes.

Name	Description
Name	Range = Up to 12 characters This field sets the name for the auto-attendant service. This can be used to route calls to the auto-attendant.

Table continues…

Name	Description
Maximum Inactivity	Default = 8 seconds; Range = 1 to 20 seconds. This field sets how long, after playing the prompts, the auto-attendant waits for a valid key press. If exceeded, the call is transferred to the Fallback Extension if set, otherwise the call is disconnected.
AA Number	This number is assigned by the system and cannot be changed. It is used in conjunction with short codes to access the auto attendant service or to record auto attendant greetings.
Direct Dial-By-Number	Default = Off. This setting affects the operation of any key presses in the auto attendant menu set to use the **Dial By Number** action. If selected, the key press for the action is included in any following digits dialed by the caller for system extension matching. For example, if 2 is set in the actions to **Dial by Number**, a caller can dial 201 for extension 201. If not selected, the key press for the action is not included in any following digits dialed by the caller for system extension matching. For example, if 2 is set in the actions to **Dial by Number**, a caller must dial 2 and then 201 for extension 201.
Dial by Name Match Order	Default = First Name/Last Name. Determines the name order used for the Embedded Voicemail Dial by Name function.
Enable Local Recording	Default = On. When off, use of short codes to record auto-attendant prompts is blocked. The short codes can still be used to playback the greetings.

Related links

The Setup Wizard/Initial Configuration on page 64

Setup Wizard: Subscription

This panel is only shown for subscription mode systems. It display details of the system's subscription settings and the subscriptions obtained.

The panel is only shown on systems that have completed their initial configuration. The settings cannot be edited. For systems going through initial configuration, the subscription settings are set through the **System** panel.

Name	Description
System ID	This is a fixed value against which the system's subscriptions are issued and validated. • For an IP500 V2 system, this ID is based on the System SD card installed in the system.

Table continues…

Name	Description
Customer ID	The customer ID specified when the system was registered for subscriptions.
License Server Address	The address of the server which provides the system with its subscriptions.

Available Subscriptions

These fields indicate the subscriptions provided to the system. For user subscriptions, the number of subscriptions are shown. For feature subscriptions, true indicates that the system has obtained that subscription.

Related links

The Setup Wizard/Initial Configuration on page 64

Setup Wizard: Licensing

This panel is shown for non-subscription systems. It allows configuration of where the system should obtain its licenses.

Related links

The Setup Wizard/Initial Configuration on page 64

Setup Wizard: User

This panel lists the users configured on the system. It allows you to add, delete or edit entries.

For IP500 V2 control units, user and extension records are automatically created for each physical extension port detected at system start.

Related links

The Setup Wizard/Initial Configuration on page 64

Setup Wizard: Groups

This panel lists the groups configured on the system. It allows you to add, delete or edit entries.

Each group has its own extension number and settings for how calls directed to that number should be presented to the users added to the group.

Related links

The Setup Wizard/Initial Configuration on page 64

Setup Wizard: Lines

This panel lists the lines configured on the system. It allows you to add, delete or edit entries.

For IP500 V2 control units, line records are automatically created for each physical line detected at system start.

Related links

The Setup Wizard/Initial Configuration on page 64

Setup Wizard: Incoming Call Routes

You can use this panel to configure where incoming external calls should be routed.

Working Hours Time Profile

These settings are used to define a default time profile for the customer's normal hours of business. This profile is then used to alter the routing of incoming calls inside and outside those times.

Once the system has been configured, additional time profiles can be added if required.

Setting	Description
Start Time	The time when normal working hours begin.
End Time	The time when normal working hours end.
Days	The days of the week when the working hours apply.

Incoming Call Routes

You can create and edit incoming call routes for the lines setup in the previous setup wizard panel. A route is required for each of the incoming line group IDs used for the lines in the system configuration.

Setting	Description
Incoming Line Group ID	Each of the lines in the system is configured with an Incoming Line Group ID. The same ID can be used for on several line. The incoming call route with the same ID is then used to route calls on those lines.
Trunk Identifier	This is a unique name added by the system for the set of trunks
Incoming Number	If required, in addition to matching the **Incoming Line Group ID** you can also match the incoming number received to route the calls for that number to different destinations. This option is not supported on all trunks. For example it is not supported with analog trunks.

Table continues…

Setting	Description
Working Hours Destination	The destination for calls that match the incoming call route during the times defined by the working hours time profile. The destination number can be selected from the drop-down list. This lists: • All existing users, groups and auto-attendants. • **Voicemail** for caller access to voicemail to collect messages. For destinations not listed in the drop-down list, the destination number can be entered manually.
Out of Office Hours Destination	The destination for calls that match the incoming call route outside the times defined by the working hours time profile.

Related links

The Setup Wizard/Initial Configuration on page 64

Setup Wizard: Outgoing Call Routes

This panel is only shown for systems where the **Locale** is set to **United States (US English)** or **Canada (Canadian French)**.

Telephony Settings

Setting	Description
Directory Overrides Barring	Default = On. When enabled, the **Outgoing Call Bar** setting on any user is not applied to the dialing of numbers that are in the system directory. This does not affect other methods of call barring.
Bar outgoing calls for Out of Office hours	Default = Off. When enabled, outgoing external calls are barred during times outside the default working hours time profile settings.

Line Selection for Outgoing Calls

Setting	Description
Select Line for Outgoing Calls	This field selects the default outgoing line group ID that should be used for all outgoing calls. That outgoing group ID can be assigned to multiple lines. Outgoing calls will then use any available line that has the same outgoing group ID
Outgoing Group ID	These fields show a summary of the existing outgoing group IDs configured and the lines using those settings. To edit the outgoing line groups use the **Lines** panel.
Line Information	

Assign Users to Outgoing Route

By default the dialing of external numbers is processed through alternate route selection (ARS) entries in the configuration. These contain setting that control what numbers are allowed, add or remove prefixes, etc.

The default ARS entry is called **Main**. However, the number of additional outgoing call routes exist (**Unrestricted**, **International**, **National** and **Long Distance**). The menu below allows you to select which of these ARS entries should be used by each user.

Setting	Description
Name	The user name.
Outgoing Route	The ARS entry that should be applied to the users outgoing calls. Click on the current setting to select a different ARS entry.

Related links

The Setup Wizard/Initial Configuration on page 64

Chapter 7: Using User and Extension Templates

You can use templates (XML files) to help speed up the creation of users/extensions with similar settings. The templates that you create and use are stored on the system.

- A range of other configuration records can also be created using templates. However, that is done using the IP Office Manager application rather than web manager.

Related links

Saving a user or extension as a template on page 81
Adding a new template on page 82
Adding users or extensions using a template on page 82
Deleting a template on page 83
Editing a template on page 83
Downloading a template on page 83
Uploading a template on page 84
Renaming a template on page 84

Saving a user or extension as a template

You can save the settings of an existing user or extension as a template.

Procedure

1. From the list of users or extensions, click on the icon next to the entry you want to save as a template.
2. Click on **Save As Template**.
3. Enter a name for the template file. The file extension ***.xml*** is added automatically.
4. Click **OK**.
5. If you made any changes to the user or extension before saving them as a template, click **Update**. Otherwise, click **Cancel**.

Related links

Using User and Extension Templates on page 81

Adding a new template

In addition to creating a template from an existing user or extension (see Saving a user or extension as a template on page 81), you can directly create a new template.

Procedure

1. Display the list of existing users or extensions.
2. Click **Actions** and then **Template Management**.
3. Click **+ Add**.
4. Enter a name for the template and click **OK**.
5. Edit the settings as required for future entries that will be created using the template.
6. Click **Create**.

Related links

Using User and Extension Templates on page 81

Adding users or extensions using a template

You can use a template to create a new users or extensions.

Procedure

1. In the user or extension list, click **Actions** and then **Create From Template**.
2. In **Enter number of records**, enter the number of new entries to create.
3. In **Enter starting extension**, enter the extension number for the first new entry. The other new entries will be added sequentially from that number.
4. Use the **Select Template** drop-down to select the template file to use.
5. Click **Preview**. The new entries are listed
   - You can click on an entry in the preview list to edit the key settings that are not part of the template.
   - If necessary, click on the icon to delete a new entry from the preview list.
   - You can delete multiple entries by selecting their check boxes and then clicking **Delete Selected Records**.
6. Click **Create**.

Related links

Using User and Extension Templates on page 81

Deleting a template

Procedure

1. Display the list of existing users or extensions.
2. Click **Actions** and then **Template Management**.
3. Click on the trash can icon next to the entry to delete.
4. Click **Yes** to confirm the deletion.

Related links

Using User and Extension Templates on page 81

Editing a template

You can edit an existing template. Note that editing a template does not affect any entries that were previously created using that template.

Procedure

1. Display the list of existing users or extensions.
2. Click **Actions** and then **Template Management**.
3. Click the icon to the right of the template.
4. Change the template settings as required. The categories shown on the left access different sets of settings.
5. When completed, click **Update**.

Related links

Using User and Extension Templates on page 81

Downloading a template

You can download a template to your PC as an XML file.

Procedure

1. Display the list of existing users or extensions.
2. Click **Actions** and then **Template Management**.
3. Click the icon to the right of the template.
4. The file is saved to your browser's download location.

Related links

Using User and Extension Templates on page 81

Uploading a template

You can upload an XML file to the system for use as a template.

Procedure

1. Display the list of existing users or extensions.
2. Click **Actions** and then **Template Management**.
3. Click on the **Select a File** field to browse for the template file on your PC.
4. Click **Upload**.

Related links

Using User and Extension Templates on page 81

Renaming a template

You can change the name of a template in order to make its use/purpose obvious.

Procedure

1. Display the list of existing users or extensions.
2. Click **Actions** and then **Template Management**.
3. Click the icon to the right of the template.
4. Enter the new name for the template.
5. Click **OK**.

Related links

Using User and Extension Templates on page 81

Part 2: The Solution Menu

Solution

This view shows a summary of the server and the main services it is providing. If accessing a primary server, the view includes details of all the servers in the network.

- For IP500 V2 systems, this view is replaced by the same menus used by the initial setup wizard. See The Setup Wizard/Initial Configuration on page 64.

Server type	Description
Primary Server	A single server providing IP Office, Voicemail Pro, one-X® Portal for IP Office and various other services.
Secondary Server	You can optionally add a secondary server to increase the capacity and provide resilience for the services on the primary.
Expansion Server	A Server Edition network can include expansion systems. These provide support for local phones and trunks in other physical locations. The expansion can be another Linux-based server, in which case it supports just IP extensions and trunks. It can also be an IP500 V2 system to add support for non-IP trunks and extensions.
Application Server	The IP Office Application Server is Linux-based server that supports the s. The Application Server supports the Voicemail Pro and one-X Portal for IP Office applications. • Within a Server Edition network, it can be used to provide one-X Portal for IP Office support for the primary or secondary server, reducing the processing load on that server. • It can be used to support a standalone IP500 V2 system, providing Voicemail Pro and one-X Portal for IP Office services for that system.
Unified Communication Module (UCM)	The UCM is an embedded server installed into an IP500 V2 system to provide Voicemail Pro and one-X Portal for IP Office services for that system.

Chapter 8: The "Solution Settings" Menu

Solution > **Solution Settings**

This menu is used to access the configuration of optional services that can then be used to support the server or servers being managed.

Setting	Server Edition	IP500 V2	Application Server	UCM
View Scheduled Jobs	Yes	–	Yes	Yes
Remote Server	Yes	–	Yes	Yes
Proxy	Yes	–	Yes	Yes
User Synchronization Using LDAP	Yes	–	–	Yes
User Synchronization using Microsoft Teams	Yes	-	-	Yes
Application Server	Yes	–	–	–

Related links

View Scheduled Jobs on page 86
Remote Server on page 87
Proxy on page 88
User Synchronization Using LDAP on page 89
User Synchronization using MS Teams on page 96
Application Server on page 102

View Scheduled Jobs

Navigation: Solution > **Solution Settings** > **View Scheduled Jobs**

This command displays a list of existing scheduled jobs. Existing jobs cannot be edited but they can be selected and deleted if required.

Field	Description
Name	IP address of the server on which the job is scheduled.
Operation	The type of Operation.

Table continues…

Field	Description
Recurring	When **Yes** is selected, the action will reoccur based on the value in the **Frequency** field. When **No** is selected, the action will occur only once.
Frequency	Schedule actions to reoccur **Daily**, **Weekly**, or **Monthly**.
Day	The day on which the action occurs. Presentation depends on the **Frequency** setting. • When **Frequency** is set to **Daily**, the field is disabled. • When **Frequency** is set to **Weekly**, the range is the days of the week from Monday to Sunday. • When **Frequency** is set to **Monthly**, the range is 1 to 28.
Status	

Related links

The "Solution Settings" Menu on page 86

Remote Server

Navigation: **Solution** > **Solution Settings** > **Remote Server**

This menu displays a list of existing remote server entries. Configuring a remote server may be required to

- download an ISO file from a remote server
- perform backup and restore actions on a remote server

Click **Add/Edit Remote Server** to create a new remote server.

Related links

The "Solution Settings" Menu on page 86
Remote server settings on page 87

Remote server settings

Navigation: Solution > **Solution Settings** > **Remote Server** > **Add/Edit Remote Server**

Field	Description
Storage Type	This field is only displayed on virtual servers deployed in a Google cloud environment. The options are: • **Google Storage**: Select this option you are using a Google Storage server inside the Google cloud. Note: Google storage can only be accessed by server's hosted in the cloud. It cannot be used as a backup destination by non—cloud—based servers in the same network. • **Custom Storage**: Select this option if you are not using a Google Storage server.
Server Name	A meaningful name for the remote server. Remote server names can be selected from other windows.
Protocol	Protocol supported by the remote server. The options are: **http**, **https**, **ftp**, **sftp**, **scp**. • For backup and restore, you can use HTTP, HTTPS, SFTP and SCP to connect to a remote IP Office Linux server. • HTTP and HTTPS can only be used to connect to an IP Office server. HTTP/HTTPS backup to a non-IP Office server is not supported.
Remote Server	IP address or Domain name of remote server.
Port	Port of remote server.
Remote Path	Default path on the remote server.
User Name	If required, the user name for logging in to the remote server.

Related links

Remote Server on page 87

Proxy

Solution > **Solution Settings** > **Proxy**

Selecting **Proxy** from the **Solution Settings** list displays current proxy detail entries. Click the icons beside a record to edit or delete.

Click **Add New Proxy** to create a new proxy.

Configuring proxy details may be required to

- download an ISO file from a remote server
- perform backup and restore actions on a remote server

Field	Description
Proxy Name	A meaningful name for the proxy. Proxy names can be selected from other windows.

Table continues…

Field	Description
Proxy Server	IP address or Domain name of proxy server.
Proxy Port	Port used for the proxy server.
User Name	If required, the user name for logging in to the proxy server.
Password	If required, the password for logging in to the proxy server.

Related links

The "Solution Settings" Menu on page 86

User Synchronization Using LDAP

Navigation: **Solution** > **Solution Settings** > **User Synchronization Using LDAP**

These menus are provided by the Collaboration service running on Linux-based IP Office servers. For IP500 V2/V2A server, the Collaboration service is provided by an IP Office Application Server or UCM Module. The Collaboration service supported LDAP v3/ LDAPS.

The IP Office system can use LDAP user synchronization to:

- Create new user (and extension) records, update existing user records and delete user records.
- Obtain directory information.
- Perform a combination of the above actions.

This is done by mapping LDAP fields onto IP Office user configuration fields. In addition to this field mapping, for new user creation, a ‘user provisioning rule’ (UPR) is used to define the extension type and extension template.

The information that can be managed through LDAP synchronization is:

IP Office User Field	New	Update	Delete
User Identification	Yes	No	Yes
Name	Yes	Yes	Yes
Full Name	Yes	Yes	Yes
Email	Yes	Yes	Yes
Extensions	Yes	Yes	Yes
Login Code	Yes	No	No
Voicemail Code	Yes	No	No
Mobile Twinning Number	Yes	Yes	Yes
Group Membership	Yes	Yes	Yes

Table continues…

User Provisioning Rule	Yes	No	No

- Mapping the **User Identification** and **Name** fields is mandatory for all operations. All the other fields are optional.
- Even if mapped, for each particular synchronization operation above, only those field labeled as '**YES**' are used.
- When creating a new user, if both the **Extensions** and **User Provisioning Rule** have been mapped, the extension number setting in the UPR takes priority.
- An LDAP field can be mapped to several IP Office fields. For example, the same LDAP field can be mapped to the user **Name** and **Full Name** fields.
- The LDAP data is not validated during synchronization. When the IP Office configuration is opened in a manual configuration tool, those fields may be flagged as errors until manually corrected. To stop this, the LDAP data should be corrected and resynchronized.

Related links

The "Solution Settings" Menu on page 86
Connect to Directory Service on page 90
Synchronize User Fields on page 92
View Jobs on page 95
Manage User Provisioning Rules on page 95

Connect to Directory Service

Navigation: **Solution** > **Solution Settings** > **User Synchronization Using LDAP** > **Connect to Directory Service**

Use this page to define the connection to the LDAP server and to define the parameters for searching the LDAP directory. All fields are mandatory.

Additional Configuration Information

For additional configuration information, see Managing Users with LDAP on page 852.

Configuration Settings

Field	Description
Application	Default = **User Synchronization** Select the application type to route to the LDAP server directory details or user details for synchronization. The following types are available: • **Directory Services** • **User Synchronization** • **User Synchronization & Directory Services** **Note:** Selecting the **Directory Services** or the **User Synchronization & Directory Services** option allows you to add **Number Attributes** and **Name Attribute**.

Table continues…

Field	Description
Host	Default = Blank. Enter the host name or IP address of the LDAP server.
Port	Default = Blank. Enter the listening port on the LDAP server. The standard ports used by the LDAP directory are 389 or 90389.
User Name	Default = Blank. Enter the user name used to log in to the LDAP server.
Password	Default = Blank. Enter the password for the user account used to log into the LDAP server.
Confirm Password	Default = Blank. Confirm the user account password.
User Schema	Default = Blank. Specifies the type of resource in LDAP. For example, the type of user. For IP Office R11.1.2.3 and higher, multiple schemas can be entered as a comma separated list.
Search Filter	Default = Blank. Specifies which objects under the base are of interest. The search applies to the **project name** and Location values for each employee. • The **Search Filter** uses the format defined in RFC2254 except that extensible matching is not supported. • You must ensure that the whole filter, and each object within the filter, are enclosed within `( )` brackets. Example search values: • **Search for all the names starting with A:** - `(name=A*)` • **Get all the phone numbers in a domain, either telephone number or mobile:** - `(|(telephonenumber=*)(mobile=*))` • **Search for a user who is a member of cn=group1, cn=user, dc=acme,dc=com and with a telephone number:** - `(&(memberof=cn=group1,cn=users,dc=acme,dc=com)(telephonenumber=*))`
Base Distinguished Name	Default = Blank. Specifies the point in the LDAP tree to start searching. Specify the hierarchy in reverse order. For example: • `OU=SBSUsers,OU=Users,OU=MyBusiness,DC=dnsroot,DC=ipoyvr,DC=ca`

Table continues…

Field	Description
Number Attributes	Default = Blank. This setting is available when **Directory Services** or **User Synchronization & Directory Services** is selected. Enter the phone number (home or mobile telephone number) to map with the directory service. • `telephoneNumber,homePhone=H,mobile=M`
Name Attribute	Default = Blank This setting is available when **Directory Services** or **User Synchronization & Directory Services** is selected. Enter the name to map with the directory service.
Auth Mechanism	Default = Simple From Simple Authentication and Security Layer (SASL) allows you to select different mechanisms to authenticate the data in the LDAP server. The following mechanisms are supported: • **CRAM-MD5** • **DIGEST-MD5**
Use SSL	Default = No. When enabled, a secure (SSL) connection must be used to connect to the LDAP server and **Security Mechanism** is available to provide secure communication by using the TLS protocols.
Security Mechanism	Provides a secure communication by using the TLS protocols. • **STARTTLS**: Used for securing LDAP communication, and uses the default LDAP port (389) to communicate with the LDAP server. • **LDAPS**: Used for securing LDAP communication, and uses the default LDAP port (636) to communicate with the LDAP server.
Add Certificate	Browse to upload the Root CA certificate of the LDAP server that uses `.pem` format.
Test Connection	When clicked, Web Manager attempts to connect to the LDAP server with the specified credentials. You must provide the password each time you test the connection.
Save	If the **Test Connection** action is successful, **Save** is enabled. Click to save the configuration.

Related links

User Synchronization Using LDAP on page 89

Synchronize User Fields

Navigation: **Solution** > **Solution Settings** > **User Synchronization Using LDAP** > **Synchronize User Fields**

Use this page to map IP Office user fields to LDAP fields.

User Fields

The following IP Office fields can be mapped.

IP Office user fields are described under **Call Management** > **Users** > **Add Users** > **User**

Field	Description
User Identification	Mandatory. This field must be unique for each user to be imported into IP Office.
Name	Mandatory. The name of the user. User names must be unique across the system. If more than one user has the same name, only the first name must be unique.
Full Name	Optional. The full name of the user.
Email	Optional. The email address for the user.
Extensions	Optional. The extension number of the user, if it is provided in LDAP.
Login Code	Optional. The code that has to be entered, as part of a log in sequence, to allow a user to make use of an extension as if it was their own phone. Range = 4 to 15 digits. The value can be entered manually or mapped to a directory field. Only numeric values are allowed. if the mapped LDAP field is non-numeric then the field is left blank.
Voicemail Code	Optional. A code used by the voicemail server to validate access to a mailbox. Range = 0 to 31 digits. The value can be entered manually or mapped to a directory field. Only numeric values are allowed. if the mapped LDAP field is non-numeric then the field is left blank.
Mobile Twinning Number	Optional. Sets the external destination number for mobile twinned calls.
Group Membership	Optional. The groups of which the user has been made a member. The directory field must contain the groups in a comma separated list.
User Provisioning Rule	Optional. Provide a user profile rule (UPR) for the users to be imported into IP Office. To create and manage UPRs, see **Solution** > **Solution Settings** > **User Synchronization Using LDAP** > **Manage User Provisioning Rules**. The name of the directory field providing the UPR must exactly match the name of the UPR created in IP Office.
System Field	• **LAN 1 Address** - Optional. Provide the directory field that maps to the IP Office LAN1 **IP Address** field. If this field is provided, users are created using this IP address. • **LAN 2 Address** - Optional. Provide the directory field that maps to the IP Office LAN2 **IP Address** field. If this field is provided, users are created using this IP address. • **System Name** - Optional. Provide the directory field that maps to IP Office field **System Name**. If this field is provided, users are created using this IP address. • **FQDN** - Optional. Provide the directory field that maps to the IP Office field **FQDN**. If this field is provided, users will be created to this IP address.

Operations in Synchronization

Field	Description
New	Use defined settings to create new users. When a new user is created in the directory, a new IP Office user is created the next time synchronization occurs.
Update	Use defined settings to update existing users. When a user is edited in he directory, the IP Office user is edited the next time synchronization occurs.
Delete	Use defined settings to delete users. When a user is deleted in he directory, the IP Office user is deleted the next time synchronization occurs. • If multiple user synchronizations are in use, for example using LDAP and MS-Teams directories, the **Delete** option is not available.

Schedule Options

Field	Description
Use Schedule	Default = Off
Start Date	Default = Blank. Click the calendar icon to select a start date.
Start Time	Click the arrow to select a start time.
Recurring Schedule	Default = No. Setting to Yes displays the configuration options.
Frequency	Default = Weekly. The options are **Daily**, **Weekly** or **Monthly**.
Day of Week / Day of Month	Default = Blank. Depending on the **Frequency** setting, select a **Day of Week** or **Day of Month**.

Field	Description
Preview Results	Display a preview of the synchronization results based on the current settings.
Synchronize	Click to start the synchronization operation. **Important:** • In order to perform the synchronization operation, you must set the current user for background configuration synchronization tasks. If this was not done when logging on to Web Manager, go to **Menu Bar Current User Icon** > **Preferences** and set **Set current user for configuration synchronization** to **YES**.

Related links

User Synchronization Using LDAP on page 89

View Jobs

Navigation: **Solution** > **Solution Settings** > **User Synchronization Using LDAP** > **View Scheduled Jobs**

Field	Description
Job Name	A system generated name.
Start Time	The scheduling information for the job based on the settings defined on the **Synchronize User Fields** page.
Recurring	
Frequency	
Status	The status can be **Scheduled**, **Running** or **Completed**.
Scheduled By	The user name of the user that scheduled the job.

The following table provides the user synchronization summary of each job.

Field	Description
System	Specifies the user system name.
Users created	Specifies the number of users created.
Users failed	Specifies the number of users failed to synchronize.
Users updated	Specifies the number of user details updated.
Users deleted	Specifies the number of users deleted from the system.
Offline Users	Specifies the number of offline users in the system.
Unknown Mapping	Specifies the number of user details not synchronized or not mapped.
Details for sync failure **User Name**	Specifies the user name.
Error Description	Describes the type of error occurred. Example: *"Extension conflicts with another user"*
System Name	Specifies the user system name.

Related links

User Synchronization Using LDAP on page 89

Manage User Provisioning Rules

Navigation: **Solution** > **Solution Settings** > **User Synchronization Using LDAP** > **Manage User Provisioning Rules**

A user provisioning rule (UPR) is used to apply a set of initial configuration settings when a new user and extension are created by LDAP synchronization. You can create multiple user provisioning rules. The LDAP mapping settings can be used to map a selected user LDAP field to a IP Office UPR in order to define which UPR is used for each new user/extension creation.

The UPR used to create a new user and extension defines the following:

- The IP Office system where the new user and extension are created
- The starting extension number
- The extension template
- The extension type
- The user template

Note:

The user provisioning rule cannot be used LDAP synchronization update actions to change the configuration settings of existing users.

Field	Description
User Provisioning Rule Name	Default = Blank. Enter a descriptive name for the rule.
IP Office Name	Default = Blank. Select the IP Office system from the list.
Start Extension	Default = Blank. Specify the extension number from which to start. Extensions are created on IP Office in ascending order, skipping any existing used extension numbers. This field is mandatory if either **Extension Template** or **Extension Type** fields are used.
Select Extension Template	Default = Blank. Select an extension template from the list. You can define extension templates by selecting **Call Management** > **Extensions** > **Actions** > **Template Management**.
Extension Type	Default = Blank. The options are: • **H323 Extension** • **IP DECT Extension** • **SIP DECT Extension** • **SIP Extension**
Select User Template	Default = Blank. Select a user template from the list. You can define user templates by selecting **Call Management** > **Users** > **Actions** > **Template Management**.

Related links

User Synchronization Using LDAP on page 89

User Synchronization using MS Teams

Navigation: **Solution** > **Solution Settings** > **User Synchronization using Microsoft Teams**

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, which provides access internal resources, such as apps on your corporate network and intranet, along with any cloud apps developed by your own organization.

The IP Office system can use MS Teams user synchronization to create new user (and extension) records, update existing user records and delete user records. This is done by mapping MS Teams fields onto IP Office user configuration fields. In addition to this field mapping, for new user creation, a 'user provisioning rule' (UPR) is used to define the extension type and extension template.

Azure AD synchronization allows the IP Office telephone number directory to be synchronized with the information on Azure AD. MS Teams synchronization is performed using Web Manager.

Related links

The "Solution Settings" Menu on page 86
Connect to Directory Service on page 97
Synchronize User Fields on page 98
View Jobs on page 101
Manage User Provisioning Rules on page 101

Connect to Directory Service

Navigation: **Solution** > **Solution Settings** > **User Synchronization using Microsoft Teams** > **Connect to Directory Service**

Use this page to define the connection to the Azure AD server and to define the parameters for searching the Azure directory. All fields are mandatory.

Configuration Settings

Field	Description
Directory	Default = **Tenant Directory** Select the directory type to route to the respective IDs for synchronization. The following types are available: • **Tenant Directory** • **Group Directory** **Note:** Selecting the **Group Directory** option allows you to add the **Group ID** of the user group.
Tenant ID	Default = Blank. Enter the tenant ID (equivalent to directory ID) of the selected directory in Azure AD.
Group ID	Default = Blank. Enter the group ID to select the user group in Azure AD

Table continues…

Field	Description
Client ID	Default = Blank. Enter the client application ID assigned from the Azure application.
Client Secret	Default = Blank. Enter the client application password assigned from the Azure application.
Test Connection	When clicked, Web Manager attempts to connect to the Azure AD with the specified credentials. You must provide the password each time you test the connection.
Number Attributes	Default = Blank. Enter the phone number (home or mobile telephone number) to map with the directory service. **telephoneNumber,homePhone=H,mobile=M**
Name Attribute	Default = Blank Enter the name to map with the directory service. **Name**
Push user data to Microsoft Teams PowerShell?	Default = **NO** Enabling the setting allows to configure the phone numbers for direct routing.
Microsoft Teams PowerShell Username	Default = Blank. Enter the user name of the Microsoft Teams PowerShell module.
Microsoft Teams PowerShell Password	Default = Blank. Enter the password of the Microsoft Teams PowerShell module.
Voice Routing Policy Name	Enter the name of the Voice Routing Policy previously created in Microsoft Teams.
Voice Routing Policy Usage	Enter the name of the PSTN Usage Record already created for the Voice Routing Policy in Microsoft Teams.
Save	If the **Test Connection** action is successful, **Save** is enabled. Click to save the configuration.

Related links

User Synchronization using MS Teams on page 96

Synchronize User Fields

Navigation: **Solution** > **Solution Settings** > **User Synchronization using Microsoft Teams** > **Synchronize User Fields**

Use this page to map IP Office user fields to MS Teams fields. The following IP Office fields can be mapped.

User Fields

The following IP Office fields can be mapped.

IP Office user fields are described under **Call Management** > **Users** > **Add Users** > **User**

Field	Description
User Identification	Mandatory. This field must be unique for each user to be imported into IP Office.
Name	Mandatory. The name of the user. User names must be unique across the system. If more than one user has the same name, only the first name must be unique.
Full Name	Optional. The full name of the user.
Email	Optional. The email address for the user.
Extensions	Optional. The extension number of the user, if it is provided in LDAP.
Login Code	Optional. The code that has to be entered, as part of a log in sequence, to allow a user to make use of an extension as if it was their own phone. Range = 4 to 15 digits. The value can be entered manually or mapped to a directory field. Only numeric values are allowed. if the mapped LDAP field is non-numeric then the field is left blank.
Voicemail Code	Optional. A code used by the voicemail server to validate access to a mailbox. Range = 0 to 31 digits. The value can be entered manually or mapped to a directory field. Only numeric values are allowed. if the mapped LDAP field is non-numeric then the field is left blank.
Mobile Twinning Number	Optional. Sets the external destination number for mobile twinned calls.
Group Membership	Optional. The groups of which the user has been made a member. The directory field must contain the groups in a comma separated list.
User Provisioning Rule	Optional. Provide a user profile rule (UPR) for the users to be imported into IP Office. To create and manage UPRs, see **Solution** > **Solution Settings** > **User Synchronization Using LDAP** > **Manage User Provisioning Rules**. The name of the directory field providing the UPR must exactly match the name of the UPR created in IP Office.
System Field	• **LAN 1 Address** - Optional. Provide the directory field that maps to the IP Office LAN1 **IP Address** field. If this field is provided, users are created using this IP address. • **LAN 2 Address** - Optional. Provide the directory field that maps to the IP Office LAN2 **IP Address** field. If this field is provided, users are created using this IP address. • **System Name** - Optional. Provide the directory field that maps to IP Office field **System Name**. If this field is provided, users are created using this IP address. • **FQDN** - Optional. Provide the directory field that maps to the IP Office field **FQDN**. If this field is provided, users will be created to this IP address.

Operations in Synchronization

Field	Description
New	Use defined settings to create new users. When a new user is created in the directory, a new IP Office user is created the next time synchronization occurs.
Update	Use defined settings to update existing users. When a user is edited in he directory, the IP Office user is edited the next time synchronization occurs.
Delete	Use defined settings to delete users. When a user is deleted in he directory, the IP Office user is deleted the next time synchronization occurs. • If multiple user synchronizations are in use, for example using LDAP and MS-Teams directories, the **Delete** option is not available.

Schedule Options

Field	Description
Use Schedule	Default = Off
Start Date	Default = Blank. Click the calendar icon to select a start date.
Start Time	Click the arrow to select a start time.
Recurring Schedule	Default = No. Setting to Yes displays the configuration options.
Frequency	Default = Weekly. The options are **Daily**, **Weekly** or **Monthly**.
Day of Week / Day of Month	Default = Blank. Depending on the **Frequency** setting, select a **Day of Week** or **Day of Month**.

Field	Description
Preview Results	Display a preview of the synchronization results based on the current settings.
Synchronize	Click to start the synchronization operation. **Important:** • In order to perform the synchronization operation, you must set the current user for background configuration synchronization tasks. If this was not done when logging on to Web Manager, go to **Menu Bar Current User Icon** > **Preferences** and set **Set current user for configuration synchronization** to **YES**.

Related links

User Synchronization using MS Teams on page 96

View Jobs

Navigation: **Solution** > **Solution Settings** > **User Synchronization using Microsoft Teams** > **View Scheduled Jobs**

Field	Description
Job Name	A system generated name.
Start Time	The scheduling information for the job based on the settings defined on the **Synchronize User Fields** page.
Recurring	
Frequency	
Status	The status can be **Scheduled**, **Running** or **Completed**.
Scheduled By	The user name of the user that scheduled the job.

The following table provides the user synchronization summary of each job.

Field	Description
System	Specifies the user system name.
Users created	Specifies the number of users created.
Users failed	Specifies the number of users failed to synchronize.
Users updated	Specifies the number of user details updated.
Users deleted	Specifies the number of users deleted from the system.
Offline Users	Specifies the number of offline users in the system.
Unknown Mapping	Specifies the number of user details not synchronized or not mapped.
Details for sync failure **User Name**	Specifies the user name.
Error Description	Describes the type of error occurred. Example: *"Extension conflicts with another user"*
System Name	Specifies the user system name.

Related links

User Synchronization using MS Teams on page 96

Manage User Provisioning Rules

Navigation: **Solution** > **Solution Settings** > **User Synchronization using Microsoft Teams** > **Manage User Provisioning Rules**

A user provisioning rule (UPR) is used to apply a set of initial configuration settings when a new user and extension are created by MS Teams synchronization. You can create multiple user provisioning rules. The MS Teams mapping settings can be used to map a selected user MS Teams field to a IP Office UPR in order to define which UPR is used for each new user/extension creation.

The UPR used to create a new user and extension defines the following:

- The IP Office system where the new user and extension are created
- The starting extension number
- The extension template
- The extension type
- The user template

Note:

The user provisioning rule cannot be used MS Teams synchronization update actions to change the configuration settings of existing users.

Field	Description
User Provisioning Rule Name	Default = Blank. Enter a descriptive name for the rule.
IP Office Name	Default = Blank. Select the IP Office system from the list.
Start Extension	Default = Blank. Specify the extension number from which to start. Extensions are created on IP Office in ascending order, skipping any existing used extension numbers. This field is mandatory if either **Extension Template** or **Extension Type** fields are used.
Select Extension Template	Default = Blank. Select an extension template from the list. You can define extension templates by selecting **Call Management** > **Extensions** > **Actions** > **Template Management**.
Extension Type	Default = Blank. The options are: • **H323 Extension** • **IP DECT Extension** • **SIP DECT Extension** • **SIP Extension**
Select User Template	Default = Blank. Select a user template from the list. You can define user templates by selecting **Call Management** > **Users** > **Actions** > **Template Management**.

Related links

User Synchronization using MS Teams on page 96

Application Server

Solution > **Solution Settings** > **Application Server**

If an application server is deployed in the network, select **Application Server** > **Add** and then enter the **Application Server IP Address**. Up to two application servers are supported.

To remove an application server, select **Application Server** > **Remove**.

Related links

The "Solution Settings" Menu on page 86

Chapter 9: The "Actions" Button Menu

Solution > **Actions**

Note that the actions vary depending on the type of server and the number of servers selected. For standalone IP500 V2 servers, see The "Actions" Button Menu (IP500 V2) on page 110.

Setting	Server Edition	Application Server	UCM
Backup	Yes	Yes	Yes
Restore	Yes	Yes	Yes
Transfer ISO	Yes	Yes	Yes
Upgrade	Yes	Yes	Yes
Synchronize Service User and System Password	Yes	–	–
Synchronize Single Sign-On configuration	Yes	–	–
Synchronize APNS configuration	Yes	–	–
Synchronize APNP System-ID	Yes	–	–
Download Configuration	Yes	–	–
Remote Operations Management	Yes		

Related links

Backup on page 105
Restore on page 105
Transfer ISO on page 106
Upgrade on page 106
Synchronize Service User and System Password on page 107
Synchronize Single Sign-On Configuration on page 107
Synchronize APNS configuration on page 108
Synchronize APNP System-ID on page 108
Download Configuration on page 108
Remote Operations Management on page 109

Backup

Navigation:

- **Solution** > **Actions** > **Backup**
- **Solution** > ☰ > **Backup**

The backup menu allows you to backup a server or servers to another server. That other server is defined by configuring a remote server entry that is then used as the backup destination.

During the configuration of the backup, you can select what settings are backed up and whether to perform an immediate backup, scheduled backup or repeating scheduled backup.

For full details of backup and restore, see Backup and Restore on page 638.

Security alert:

Backup and restore actions to a remote server using HTTP/HTTPS must only be performed using servers inside a secure, trusted network. HTTP and HTTPS can only be used to connect to an IP Office server. HTTP/HTTPS backup to a non-IP Office server is not supported.

Note:

When managing a Server Edition solution with Web Manager, it must be managed from the Primary Server if the Primary Server is active. If the Primary Server is not active, you can perform management tasks from the Secondary Server, but not upgrade or backup and restore.

Related links

The "Actions" Button Menu on page 104

Restore

Navigation:

- **Solution** > **Actions** > **Restore**
- **Solution** > ☰ > **Restore**

This option is used to restore a previous backup made using the **Backup** command. During the restore process, you can select which parts of the previous backup should be restored.

For full details of backup and restore, see Backup and Restore on page 638.

Security alert:

Backup and restore actions to a remote server using HTTP/HTTPS must only be performed using servers inside a secure, trusted network. HTTP and HTTPS can only be used to connect to an IP Office server. HTTP/HTTPS backup to a non-IP Office server is not supported.

Note:

When managing a Server Edition solution with Web Manager, it must be managed from the Primary Server if the Primary Server is active. If the Primary Server is not active, you can perform management tasks from the Secondary Server, but not upgrade or backup and restore.

Related links

The "Actions" Button Menu on page 104

Transfer ISO

Navigation: Solution > **Actions** > **Transfer ISO**

The first stage of upgrades Linux-based IP Office system is to transfer an ISO file of the new software using this command. For details of upgrading, refer to Deploying IP Office Server Edition.

Related links

The "Actions" Button Menu on page 104

Upgrade

Navigation: Solution > **Actions** > **Upgrade**

Having transferred an ISO file containing new software to the system, the message “Upgrade Available” is shown to each server in the **Solution** menu. Selecting those servers and then **Upgrade** can be used to start the upgrade process.

For details of upgrading, refer to Deploying IP Office Server Edition.

Warning:

- Before performing any upgrade, you must:
  - take a backup of the servers.
  - read all release notes and documentation relating to the new software and any other intermediate releases.
- When managing a Server Edition solution with Web Manager, it must be managed from the Primary Server if the Primary Server is active. If the Primary Server is not active, you can perform management tasks from the Secondary Server, but not upgrade or backup and restore.
- When upgrading multiple servers, the primary server must be upgraded first. Once upgraded, the remaining servers can be upgraded as a group.

Related links

The "Actions" Button Menu on page 104

Synchronize Service User and System Password

Solution > **Actions** > **Synchronize Service User and System Password**

Note:

This option is not available on IP500 V2 systems.

Synchronizing the service user and system password enables single sign on for all systems and applications across the solution.

- This process synchronizes the security service users and their service user passwords on all systems.
- This process only affects service users and their passwords. It does not affect any other security settings, including the settings of rights groups.

Performing a security settings reset from Manager or Web Manager will disable single sign on since there is no longer a common user with common credentials. In this case, reset the password of the common user to the common value. To synchronize the password, select the Primary Server and one or more additional systems on the Solution page and then select **Actions** > **Synchronize Service User and System Password**.

If the password on one or more systems is not synchronized, the Provide Credentials window opens. In this window, you can enter the common credentials for the service user on each system that is not currently synchronized.

Related links

The "Actions" Button Menu on page 104

Synchronize Single Sign-On Configuration

Navigation: Solution > **Actions** > **Synchronize Single Sign-On configuration**

Synchronize the **Enable Avaya Cloud Account Authorization** and **Token Cache Time** settings on all the selected servers, using the values from the primary server.

- This action requires the IP Office service user account using IP Office Web Manager to have sufficient rights and to be shared on all the IP Office servers.

Related links

The "Actions" Button Menu on page 104

Synchronize APNS configuration

Navigation: Solution > **Actions** > **Synchronize APNS configuration**

Synchronize the **Enable Apple Push Notification** setting on all the selected servers, using the value from the primary server.

- This action requires the IP Office service user account using IP Office Web Manager to have sufficient rights and to be shared on all the IP Office servers.

Related links

The "Actions" Button Menu on page 104

Synchronize APNP System-ID

Navigation: Solution > **Actions** > **Synchronize APNP System-ID**

Synchronize the **System-ID**, **Avaya Spaces API Key** and **Avaya Spaces Key Secret** settings on all the selected servers, using the values from the primary server.

- The **System-ID** is a hidden value generated by an IP Office when the **Enable Apple Push Notification** setting is enabled.
- This action requires the IP Office service user account using IP Office Web Manager to have sufficient rights and to be shared on all the IP Office servers.

Related links

The "Actions" Button Menu on page 104

Download Configuration

Navigation: Solution > **Actions** > **Download Configuration**

Selecting Download Configuration saves a .zip file containing the configuration file to the local machine running Web Manager. The location depends upon your browser settings.

For a deployment with multiple systems, the zip file contains one `.cfg` file for each server in the network plus a single `.cfi` file for the whole network.

Related links

The "Actions" Button Menu on page 104

Remote Operations Management

Navigation: Solution > **Actions** > **Remote Operations Management**

On subscription systems, this command accesses options to enable or disable the connection with the Customer Operations Management service which provides the system's subscriptions and other services.

Related links

The "Actions" Button Menu on page 104

Chapter 10: The "Actions" Button Menu (IP500 V2)

Solution > **Actions**

This table lists the actions available when managing a standalone IP500 V2 server. For other types of server, see The "Actions" Button Menu on page 104.

Command		IP500 V2
Backup		Yes[1]
Restore		Yes[1]
Upgrade		Yes[1]
Upload Configuration		Yes
Download Configuration		Yes
Backup Status		Yes
Restore Status		Yes
On-boarding		Yes
Initial Configuration		Yes
Service Commands	**Reboot**	Yes
	System Shutdown	Yes
	Erase Security Settings	Yes
	Service Status	Yes
	Erase Configuration	Yes
	Memory Card Start	Yes
	Memory Card Stop	Yes
	Copy to Optional SD	Yes

1. No longer supported by current web browsers.

Related links

Backup on page 111
Restore on page 111
Upgrade on page 112
Download Configuration on page 112
Upload Configuration on page 113

Backup Status on page 113
Restore Status on page 113
On-boarding on page 113
Initial Configuration on page 114
Service Commands (Standalone IP500 V2) on page 114

Backup

Solution > **Actions** > **Backup**

This command can be used to start one of 2 different types of backup:

- **On Device** - Copy the contents of the System SD card's `/primary` folder to its `/backup` folder.
- **Client Machine** - Copy the contents of the System SD card's `/backup` folder to a location specified on the PC running web manager.

  Note:

  - This option is not supported by current browsers. The option is not available in later versions of IP Office Web Manager.

  This action requires the IP Office service user account using IP Office Web Manager to have sufficient rights and to be shared on all the IP Office servers.

Note that these processes take approximately 25 minutes. The progress can be checked using the **Solution** > **Actions** > **Backup Status** command.

Related links

The "Actions" Button Menu (IP500 V2) on page 110

Restore

Solution > **Actions** > **Restore** (Standalone IP500 V2)

This process restores a previous backup taken using web manager. This command can be used to start one of 2 different types of restore operation:

- **On Device** - Copy the contents of the System SD card's `/backup` folder to the `/primary` folder.
- **Client Machine** - Copy the contents of the previous backup to the System SD card's `/backup` folder.

Note:

- This option is not supported by current browsers. The option is not available in later versions of IP Office Web Manager.

This action requires the IP Office service user account using IP Office Web Manager to have sufficient rights and to be shared on all the IP Office servers.

Warning:

- The processes requires the IP Office system to reboot in order to apply any changes made. The reboot ends all current calls and services.

Note that these processes take approximately 25 minutes. The progress can be checked using the **Solution** > **Actions** > **Backup Status** command.

Related links

The "Actions" Button Menu (IP500 V2) on page 110

Upgrade

Solution > **Actions** > **Upgrade** (Standalone IP500 V2)

Note:

- This option is not supported by current browsers. The option is not available in later versions of IP Office Web Manager.

This action requires the IP Office service user account using IP Office Web Manager to have sufficient rights and to be shared on all the IP Office servers.

Related links

The "Actions" Button Menu (IP500 V2) on page 110

Download Configuration

- **Solution** > **Actions** > **Download Configuration** (Standalone IP500 V2)
- **Solution** > ☰ > **Download Configuration** (Other servers)

This commands allows you to download a copy of the configuration of the IP Office service being run by the server. This configuration may be requested to resolve support requests.

Related links

The "Actions" Button Menu (IP500 V2) on page 110

Upload Configuration

Solution > **Actions** > **Upload Configuration** (Standalone IP500 V2)

This command allows an IP Office configuration file to be uploaded to the server.

- Download a copy of the system's existing configuration before performing this action.
- You must ensure that the configuration matches the physical configuration of the system and its operating mode.
- This action will cause the system to reboot, ending all current calls and services.

Related links

The "Actions" Button Menu (IP500 V2) on page 110

Backup Status

Solution > **Actions** > **Backup Status** (Standalone IP500 V2)

This command displays the progress of a backup started using the **Solution** > **Actions** > **Backup** command.

Related links

The "Actions" Button Menu (IP500 V2) on page 110

Restore Status

Solution > **Actions** > **Restore Status** (Standalone IP500 V2)

This command displays the progress of a restore started using the **Solution** > **Actions** > **Restore** command.

Related links

The "Actions" Button Menu (IP500 V2) on page 110

On-boarding

- **Solution** > **Actions** > **On-boarding** (Standalone IP500 V2)
- **Solution** > ☰ > **On-boarding** (Other servers)

On-boarding refers to the configuration of an SSL VPN service in order to enable remote management services to customers, such as fault management, monitoring, and administration.

Warning:

The process of 'on-boarding automatically creates an SSL VPN service in the system configuration when the on-boarding file is uploaded to the system. Care should be taken not to delete or modify such a service except when advised to by Avaya.

Field	Descriptions
TAA series hardware	Set to **On** if your catalog description ends with the letters "TAA". For example: IP OFFICE 500 VERSION 2 CONTROL UNIT TAA. This assists in creating an accurate install base record. If you are unsure whether the catalog description ends in TAA or not, leave this box unmarked.
Get Inventory File	When you configure the SSL VPN service on a new system, you must begin by generating an inventory of the IP Office system.
Register IP Office	Opens a browser window for the GRT web site. You are prompted for a user ID and password. On the GRT web site, enter the required data for the IP Office system.
Upload On-boarding file	The inventory file that you generated is uploaded to the GRT and the inventory data is populated in the Avaya Customer Support (ACS) database.

Related links

The "Actions" Button Menu (IP500 V2) on page 110

Initial Configuration

- **Solution** > **Actions** > **Initial Configuration** (Standalone IP500 V2)
- **Navigation:Solution** > ☰ > **Initial Configuration** (Other servers)

This command reruns the initial configuration process that was previously run during the initial deployment of the server. See The Setup Wizard/Initial Configuration on page 64.

Note that re-running the initial configuration does not allow the **System Mode** to be changed. For example it cannot be used to change a subscription mode system to a non-subscription mode.

Related links

The "Actions" Button Menu (IP500 V2) on page 110

Service Commands (Standalone IP500 V2)

Solution > **Actions** > **Service Commands**

The following are the service commands supported for standalone IP500 V2 servers. For other types of server, see Service Commands on page 128.

Command	IP500 V2
Reboot	Yes
System Shutdown	Yes
Erase Security Settings	Yes
Service Status	Yes
Erase Configuration	Yes
Memory Card Start	Yes
Memory Card Stop	Yes
Copy to Optional SD	Yes

Related links

The "Actions" Button Menu (IP500 V2) on page 110
Reboot on page 115
System Shutdown (IP500 V2) on page 116
Erase Security Settings (IP500 V2) on page 116
Service Status on page 117
Erase Configuration on page 117
Memory Card Start on page 117
Memory Card Stop on page 118
Copy to Optional SD on page 118

Reboot

- **Solution** > **Actions** > **Service Commands** > **Reboot** (Standalone IP500 V2)
- **Solution** > ☰ > **Service Commands** > **Restart IP Office Service** (Other servers)

This commands restarts the IP Office service:

- For IP500 V2 servers, it physically reboots the server and any attached expansion modules.
- For other servers, it restarts the IP Office service being run on the server.

When this command is selected, the **Reboot** window opens. When the reboot occurs can be selected as follows:

- **Immediate** Send the configuration and then reboot the system.
- **Free** Send the configuration and reboot the system when there are no calls in progress.
- **Timed** The same as **When Free** but waits for a specific time after which it then waits for there to be no calls in progress. The time is specified by selecting a time from the drop down list.

Related links

Service Commands (Standalone IP500 V2) on page 114

System Shutdown (IP500 V2)

- **Solution** > **Actions** > **Service Commands** > **System Shutdown**
- For other servers, use the shutdown command in the **Platform View** menus. See The Platform View menus on page 131.

This command can be used to shutdown IP500 V2 systems. The shut down can be either indefinite or for a set period of time after which the system will reboot. For Linux based systems, use the service commands in IP Office Web Manager

⚠ Warning:

- A shutdown must always be used to switch off the system. Simply removing the power cord or switching off the power input may cause the loss of configuration data.
- This is not a polite shutdown, any user calls and services in operation will be stopped. Once shutdown, the system cannot be used to make or receive any calls until restarted.

The shutdown process takes up to a minute to complete. When shutting down a system with a Unified Communications Module installed, the shutdown can take up to 3 minutes while the module safely closes all open files and closes down its operating system. During this period the module's LED 1 remains green.

- LED1 on each IP500 base card installed will also flash red rapidly plus LED 9 if a trunk daughter card is fitted to the base card.
- The CPU LED on the rear of the system will flash red rapidly.
- The System SD and Optional SD memory card LEDs on the rear of the system are extinguished.

To restart a system when shutdown indefinitely, or to restart a system before the timed restart, switch power to the system off and on again.

Once you have selected the system from the Select IP Office window, the System Shutdown Mode window opens. Select the type of shutdown required:

- If a **Timed** shutdown is selected, the system will reboot after the set time has elapsed.
- If **Indefinite** is used, the system can only be restarted by having its power switched off and then on again. For Linux based telephone systems, the telephony service must be restarted through the server's web control pages.

Related links

Service Commands (Standalone IP500 V2) on page 114

Erase Security Settings (IP500 V2)

- **Solution** > **Actions** > **Service Commands** > **Erase Security Settings** (Standalone IP500 V2)
- **Solution** > ☰ > **Service Commands** > **Erase Security Settings** (Other servers)

The **Erase Security Settings** command returns the security settings of a system back to their default values. This action does not affect the system's configuration or audit trail record.

Note that any security certificates stored and being used by the system are deleted. Any services currently using those certificates are disconnected and disabled until the appropriate certificates

are added back to the system's security configuration. That includes SSL VPN connections being used to perform system maintenance.

For IP500 and IP500 V2 control units, if the security settings cannot be defaulted using this command, they can be defaulted using a DTE cable connection to the system. Refer to the Deploying an IP500 V2 IP Office Subscription System manual.

Warning:

- Whilst defaulting the security settings does not require a system reboot, it may cause service disruption for several minutes while the system generates a new default security certificate.

Related links

Service Commands (Standalone IP500 V2) on page 114

Service Status

Solution > **Actions** > **Service Commands** > **Service Status** (Standalone IP500 V2)

This command can be used to disable the server's telephony services if required. While disabled:

- All telephony services are stopped.
- Avaya 9600 Series and J100 Series telephones display "*System Unlicensed*".

Related links

Service Commands (Standalone IP500 V2) on page 114

Erase Configuration

- **Solution** > **Actions** > **Service Commands** > **Erase Configuration** (Standalone IP500 V2)
- **Navigation:Solution** > ☰ > **Service Commands** > **Erase Configuration** (Other servers)

The **Erase Configuration** command returns the configuration settings of the IP Office service back to their default values. It does not affect the system's security settings or audit trail record.

Related links

Service Commands (Standalone IP500 V2) on page 114

Memory Card Start

Solution > **Actions** > **Service Commands** > **Memory Card Start** (Standalone IP500 V2)

The operation of the memory card is automatically restarted when it is physically inserted into the server or the server is restarted. However, this command can be used to restart operation of a memory card that has been shut down but not removed.

Related links

Service Commands (Standalone IP500 V2) on page 114

Memory Card Stop

Solution > **Actions** > **Service Commands** > **Memory Card Stop** (Standalone IP500 V2)

This command can be used to shutdown the operation of IP500 V2 unit memory cards.

This action or a system shutdown must be performed before a memory card is removed from the unit. Removing a memory card while the system is running may cause file corruption. Card services can be restarted by either reinserting the card or using the **Memory Card Start** command.

Shutting down the memory card will disable all services provided by the card including Embedded Voicemail if being used. Features licensed by the memory card will continue to operate for up to 2 hours.

Related links

Service Commands (Standalone IP500 V2) on page 114

Copy to Optional SD

Solution > **Actions** > **Service Commands** > **Copy to Optional SD** (Standalone IP500 V2)

This process copies all files on the System SD card to the Optional SD card if present. It includes the `/primary` and `/backup` folders and the Embedded Voicemail files including message files. Any matching files and folders on the Optional SD card are overwritten.

The process is a simple copy. Any files already copied that change while the process are not recopied. Any new files added while the process is running, for example voicemail messages, may not be copied.

This process takes at least 90 minutes and may take much longer depending on the amount of data to be copied, for example it will be longer if Embedded Voicemail is being used by the IP Office system to take messages.

Related links

Service Commands (Standalone IP500 V2) on page 114

Chapter 11: The "Configure" Button Menu

Solution > **Configure**

Web manager on IP Office Server edition is used to manage multiple servers in the network. The **Configure** button provides options for adding, removing and editing the servers in the network.

Setting	Server Edition	IP500 V2	Application Server	UCM
Add System to Solution	Yes	–	–	–
Remove System from Solution	Yes	–	–	–
Convert to Select Licensed System	Yes	–	–	–
Resiliency Administration	Yes	–	–	–
Set All Nodes License Source	Yes	–	–	–
Set All Nodes to Subscription	Yes	–	–	–
Link Expansions	Yes	–	–	–

Related links

Add System to Solution on page 119
Remove System from Solution on page 121
Convert to Select Licensed System on page 121
Resiliency Administration on page 121
Set All Nodes to Subscription on page 121
Set All Nodes License Source on page 122
Link Expansions on page 122

Add System to Solution

Navigation: Solution > **Configure** > **Add System to Solution**

Perform the following steps to add a system to a IP Office Server Edition Solution. When you add a system, an IP Office Lines connecting it to the primary, and if present secondary, are automatically added to the server configurations.

Important:

If the Manager setting **File** > **Preferences** > **Preferences** > **SE Central Access** is set to **On**, an IP Office Line is not configured from the new system to the Server Edition Primary Server. The status of the new system is **Offline**. You must configure an IP Office Line from the new system to the Server Edition Primary Server.

1. Select **Solution** > **Configure** > **Add System to Solution**.
2. Depending on the system type, select **Secondary server** or **Expansion System**.
3. Perform one of the following:

   Adding an offline or inaccessible system:

   a. Click the check box **Offline or Inaccessible System**
   b. In the **IP Address of the system to Add** field, enter the IP address of the system.
   c. Enter and confirm a **Websocket Password**. The password must have a minimum of eight characters.
   d. Click **Next**.

   Discover a system:

   a. Click **Discover**.
   b. Select a system from the discovered list.
   c. Enter and confirm a **Websocket Password**. The password must have a minimum of eight characters.
   d. Click **Next**.

You can change the system discovery settings by clicking **Discover** or **Discovery Preferences**. The Discovery Preferences window contains the following fields.

Field	Description
HTTP Discovery	Controls whether HTTP is used to discover systems.
IP Address Range	• Address ranges can be specified using dashes, for example 135.64.180.170 - 135.64.180.175. • Multiple ranges can be entered separated by commas, for example 10.133.39.1-10.133.39.115, 148.147.214.40-148.147.214.254 **Note:** Only IP Office systems running release 9.1.x or higher will be discovered.
UDP Discovery	Controls whether Manager uses UDP to discover systems.
Broadcast IP Address	The broadcast IP address range used during UDP discovery. Since UDP broadcast is not routable, it will not locate systems that are on different subnets.

Related links

The "Configure" Button Menu on page 119

Remove System from Solution

Navigation: Solution > **Configure** > **Remove System from Solution**

Use this command to remove a system from the IP Office Server Edition Solution.

1. On the Solution page, click the check box for the system or systems you want to remove.
2. Click **Solution** > **Configure** > **Remove System from Solution**.

Related links

The "Configure" Button Menu on page 119

Convert to Select Licensed System

Navigation: Solution > **Configure** > **Convert to Select Licensed System**

If **Select** licensing mode is being used, all servers in the network must be converted to **Select** licensing. Use this command to convert any server in the network that has been initially configured in a different mode.

Related links

The "Configure" Button Menu on page 119

Resiliency Administration

Navigation: Solution > **Configure** > **Resiliency Administration**

In a network of systems, the remaining systems can provide support continued operation when one of the other servers in the network become unavailable for some reason. For full details of resiliency operation and features, refer to IP Office Resilience Overview.

This menu allows you to select which server should provide what resiliency support for other servers in the network. By default, resilience is configured between the primary and secondary servers and all expansion servers to the primary.

Related links

The "Configure" Button Menu on page 119

Set All Nodes to Subscription

Navigation: Solution > **Configure** > **Set All Nodes to Subscription**

If the primary server has been configured for subscription mode, all other server in the network must also run in subscription mode. You can use this option to convert all other nodes to match the primary server.

Related links

The "Configure" Button Menu on page 119

Set All Nodes License Source

Navigation: Solution > **Configure** > **Set All Nodes License Source**

For non-subscription mode network, all systems in the Server Edition solution must use the same license source. The license source is defined by the configuration setting **System Settings** > **Licenses** > **Server Menu** > **Manage Licenses** > **License Source**.

Use this command to set to set all nodes to use the same license source.

Related links

The "Configure" Button Menu on page 119

Link Expansions

Navigation: Solution > **Configure** > **Link Expansions**

Normally IP Office lines linking the systems in a network to the primary and, if present, secondary servers are automatically added when during the initial configuration of a new server.

For Select and subscription systems, it is also possible to add links between expansion systems. That is done using this command. When selected, the following menu options are available.

First Expansion System **Second Expansion System**	Use these fields to select the two expansion systems for which you want links added to each systems configuration.
Select Link Type	Default = SCN Websocket (Secure) Select the security level for the line. The options are: • **SCN Websocket (Secure)**: Recommended for security and NAT traversal. • **SCN Websocket**: Supports NAT traversal with limited security. • **SCN**: Legacy SCN line. Not recommended for new deployment.
Password **Confirm Password**	If the **Link Type** is set to **SCN Websocket (Secure)** or **SCN Websocket**, you must configure a password. The password must have a minimum of eight characters.

Related links

The "Configure" Button Menu on page 119

Chapter 12: The "Hamburger" Server Menu

Solution > ☰

The **Solution** page shows details of the server (or servers in a network). The ☰ icon next to each, accesses a menu of commands that can be applied to that server.

Command		Server Edition	IP500 V2	Application Server	UCM
Dashboard		Yes	–	–	–
Platform View		Yes	–	Yes	Yes
Backup		Yes	Yes[1]	Yes	Yes
Restore		Yes	Yes[1]	Yes	Yes
On-boarding		Yes	Yes[1]	Yes	Yes
Launch SSA		Yes	–	Yes	Yes
Service Commands	**Restart IP Office Service**	Yes	–	Yes	Yes
	Erase Configuration	Yes	Yes[1]	Yes	Yes
	Erase Security Settings	Yes	Yes[1]	Yes	Yes
Initial Configuration		Yes	Yes[1]	Yes	Yes
Download Configuration		Yes	Yes[1]	Yes	–
View Upgrade Report		Yes	–	Yes	Yes

1. For standalone IP500 V2 systems, these commands are available through the server's **Actions** menu. See The "Actions" Button Menu (IP500 V2) on page 110.

Related links

Dashboard on page 125
Platform View on page 125
Backup on page 125
Restore on page 126
On-boarding on page 127
Launch SSA on page 127
Service Commands on page 128
Initial Configuration on page 129
Download Configuration on page 130
View Upgrade Report on page 130

Dashboard

Navigation: Solution > ☰ > **Dashboard**

The **Dashboard** is a read only detailed inventory of the server. The following information is displayed:

- Control Unit type
- Hardware Installed
- System Information
- Feature Configured
- Licenses Installed
- Users by Profile
- Available Extensions
- Available Groups

Clicking a link brings you to the main page for the record type.

Related links

The "Hamburger" Server Menu on page 124

Platform View

Navigation: Solution > ☰ > **Platform View**

The **Platform View** gives access to a set of menus for the underlying server configuration. See The Platform View menus on page 131 for detailed description of the **Platform View** menus.

Related links

The "Hamburger" Server Menu on page 124

Backup

Navigation:

- **Solution** > **Actions** > **Backup**
- **Solution** > ☰ > **Backup**

The backup menu allows you to backup a server or servers to another server. That other server is defined by configuring a remote server entry that is then used as the backup destination.

During the configuration of the backup, you can select what settings are backed up and whether to perform an immediate backup, scheduled backup or repeating scheduled backup.

For full details of backup and restore, see Backup and Restore on page 638.

Security alert:

Backup and restore actions to a remote server using HTTP/HTTPS must only be performed using servers inside a secure, trusted network. HTTP and HTTPS can only be used to connect to an IP Office server. HTTP/HTTPS backup to a non-IP Office server is not supported.

Note:

When managing a Server Edition solution with Web Manager, it must be managed from the Primary Server if the Primary Server is active. If the Primary Server is not active, you can perform management tasks from the Secondary Server, but not upgrade or backup and restore.

Related links

The "Hamburger" Server Menu on page 124

Restore

Navigation:

- **Solution** > **Actions** > **Restore**
- **Solution** > ☰ > **Restore**

This option is used to restore a previous backup made using the **Backup** command. During the restore process, you can select which parts of the previous backup should be restored.

For full details of backup and restore, see Backup and Restore on page 638.

Security alert:

Backup and restore actions to a remote server using HTTP/HTTPS must only be performed using servers inside a secure, trusted network. HTTP and HTTPS can only be used to connect to an IP Office server. HTTP/HTTPS backup to a non-IP Office server is not supported.

Note:

When managing a Server Edition solution with Web Manager, it must be managed from the Primary Server if the Primary Server is active. If the Primary Server is not active, you can perform management tasks from the Secondary Server, but not upgrade or backup and restore.

Related links

The "Hamburger" Server Menu on page 124

On-boarding

- **Solution** > **Actions** > **On-boarding** (Standalone IP500 V2)
- **Solution** > ☰ > **On-boarding** (Other servers)

On-boarding refers to the configuration of an SSL VPN service in order to enable remote management services to customers, such as fault management, monitoring, and administration.

Warning:

The process of 'on-boarding automatically creates an SSL VPN service in the system configuration when the on-boarding file is uploaded to the system. Care should be taken not to delete or modify such a service except when advised to by Avaya.

Field	Descriptions
TAA series hardware	Set to **On** if your catalog description ends with the letters "TAA". For example: IP OFFICE 500 VERSION 2 CONTROL UNIT TAA. This assists in creating an accurate install base record. If you are unsure whether the catalog description ends in TAA or not, leave this box unmarked.
Get Inventory File	When you configure the SSL VPN service on a new system, you must begin by generating an inventory of the IP Office system.
Register IP Office	Opens a browser window for the GRT web site. You are prompted for a user ID and password. On the GRT web site, enter the required data for the IP Office system.
Upload On-boarding file	The inventory file that you generated is uploaded to the GRT and the inventory data is populated in the Avaya Customer Support (ACS) database.

Related links

The "Hamburger" Server Menu on page 124

Launch SSA

Navigation: Solution > ☰ > **Launch SSA**

The System Status Application is a diagnostic tool for system managers and administrators and is used to monitor and check the status of systems. Select **Launch SSA** from the menu for a server to check the status of that server.

For more information, refer to Using IP Office System Status.

Note:

- This option is not supported by current browsers. The option is not available in later versions of IP Office Web Manager.

This action requires the IP Office service user account using IP Office Web Manager to have sufficient rights and to be shared on all the IP Office servers.

Related links

The "Hamburger" Server Menu on page 124

Service Commands

Solution > ☰ > **Service Commands**

For the service commands for standalone IP500 V2 servers, see Service Commands (Standalone IP500 V2) on page 114.

Command	Server Edition	Application Server	UCM
Restart IP Office Service	Yes	Yes	Yes
Erase Configuration	Yes	Yes	Yes
Erase Security Settings	Yes	Yes	Yes

Related links

The "Hamburger" Server Menu on page 124
Restart IP Office Service on page 128
Erase Configuration on page 129
Erase Security Settings on page 129

Restart IP Office Service

- **Solution** > **Actions** > **Service Commands** > **Reboot** (Standalone IP500 V2)
- **Solution** > ☰ > **Service Commands** > **Restart IP Office Service** (Other servers)

This commands restarts the IP Office service:

- For IP500 V2 servers, it physically reboots the server and any attached expansion modules.
- For other servers, it restarts the IP Office service being run on the server.

When this command is selected, the **Reboot** window opens. When the reboot occurs can be selected as follows:

- **Immediate** Send the configuration and then reboot the system.
- **Free** Send the configuration and reboot the system when there are no calls in progress.
- **Timed** The same as **When Free** but waits for a specific time after which it then waits for there to be no calls in progress. The time is specified by selecting a time from the drop down list.

Related links

Service Commands on page 128

Erase Configuration

- **Solution** > **Actions** > **Service Commands** > **Erase Configuration** (Standalone IP500 V2)
- **Navigation:Solution** > ☰ > **Service Commands** > **Erase Configuration** (Other servers)

The **Erase Configuration** command returns the configuration settings of the IP Office service back to their default values. It does not affect the system's security settings or audit trail record.

Related links

Service Commands on page 128

Erase Security Settings

- **Solution** > **Actions** > **Service Commands** > **Erase Security Settings** (Standalone IP500 V2)
- **Solution** > ☰ > **Service Commands** > **Erase Security Settings** (Other servers)

The **Erase Security Settings** command returns the security settings of a system back to their default values. This action does not affect the system's configuration or audit trail record.

Note that any security certificates stored and being used by the system are deleted. Any services currently using those certificates are disconnected and disabled until the appropriate certificates are added back to the system's security configuration. That includes SSL VPN connections being used to perform system maintenance.

For IP500 and IP500 V2 control units, if the security settings cannot be defaulted using this command, they can be defaulted using a DTE cable connection to the system. Refer to the Deploying an IP500 V2 IP Office Subscription System manual.

⚠ **Warning:**

- Whilst defaulting the security settings does not require a system reboot, it may cause service disruption for several minutes while the system generates a new default security certificate.

Related links

Service Commands on page 128

Initial Configuration

- **Solution** > **Actions** > **Initial Configuration** (Standalone IP500 V2)
- **Navigation:Solution** > ☰ > **Initial Configuration** (Other servers)

This command reruns the initial configuration process that was previously run during the initial deployment of the server. See The Setup Wizard/Initial Configuration on page 64.

Note that re-running the initial configuration does not allow the **System Mode** to be changed. For example it cannot be used to change a subscription mode system to a non-subscription mode.

Related links

The "Hamburger" Server Menu on page 124

Download Configuration

- **Solution** > **Actions** > **Download Configuration** (Standalone IP500 V2)
- **Solution** > ☰ > **Download Configuration** (Other servers)

This commands allows you to download a copy of the configuration of the IP Office service being run by the server. This configuration may be requested to resolve support requests.

Related links

The "Hamburger" Server Menu on page 124

View Upgrade Report

Navigation: Solution > ☰ > **View Upgrade Report**

If the server has been upgraded at any time, this command displays a summary of the upgrade details and the newly installed components.

Related links

The "Hamburger" Server Menu on page 124

Chapter 13: The Platform View menus

Navigation: Solution > ☰ > **Platform View**

The **Platform View** menus are used to configure a range of settings that underlay the operation of Linux-based IP Office servers. For example, setting the date and time settings of the server.

In addition to access through IP Office Web Manager, these menus can be accessed directly using the server address and port `7071`.

Note:

This option is not available on IP500 V2 systems.

The following are the **Platform View** menus.

Menus	Description
System	This menu gives an overview of the status of the applications hosted on the IP Office server.
Logs	This menu has sub-menus for viewing and managing log records and log files. • **Debug Logs** - View the current log files for the server and the application services hosted by the server. • **Syslog Event Viewer** - View Syslog log records received or generated by the server. • **Download** - Create and download archive files of existing log records.
Updates	Display the versions of applications and components installed and the alternate versions available.
Settings	This menu has sub-menus for various areas of server configuration and operation. • **General** - General server settings such as the locations of software update repositories. • **System** - View and manage the server setting for date, time and IP address details.
AppCenter	You can download the installation packages for applications such as the Voicemail Pro client application from this page.

Related links

System on page 132
Logs on page 134
Updates on page 136

Settings on page 137
AppCenter on page 154

System

Navigation: **Solution** > ☰ > **Platform View** > **System**

The **System** menu provides an overview of the server status including the status of the application services running on the server.

The main content pane contains two sections: **Services** and **System**.

Services

This table lists the services supported by the server. In addition to showing the status of the service, it also contains buttons to start or stop each service. Click on the link for **Mem/CPU usage** usage will display a summary graph of CPU and memory usage by the application.

The services available depending on the type of server.

Application	Description
IP Office or **Management Services**	**IP Office** is the media gateway service for voice and video calls using IP (H323 and SIP) trunks and telephones. • On Unified Communications Module and IP OfficeApplication servers, it is replaced by the **Management Services** service.
one-X Portal	This is a web browser based application that users can use to control making and answering calls on their phone. It also provides a range of gadgets for the user to access features such as their directory, call log and voicemail messages. The Avaya one-X® Portal for IP Office application is configured and managed remotely via web browser. • The portal service status appears as 'amber' (starting) when the server configured for portal resilience support is passive. It changes to green when the portal server is active. • If portal resiliency is not configured, the portal service on the Server Edition Secondary server is automatically stopped and cannot be manually started.
Voicemail	This is the voicemail service for Voicemail Pro.
Collaboration Services	This service handles support for connections between IP Office systems and services such as LDAP v3 or MS Teams.
Web License Manager	This service allows the server to act as a WebLM server. IP Office systems can then use the WebLM service to host, validate and distribute licenses.
Web Manager	This is a browser-based application that you can configure and manage the IP Office server. For servers that are part of an IP Office Server Edition or Select network, the menus for all servers in the network are aggregated into one set of menus.

Table continues…

Application	Description
Optional services The server can include a number of additional services. Click **Show optional services** to display those services. These services are not supported on the Unified Communications Module.	
Local Media Manager	This service is used to provide the local Media Manager. It is not required for centralized Media Manager. Media Manager is used for the long term storage and retrieval of call recordings. The recordings are still made by Voicemail Pro, but are then collected and stored by Media Manager.
WebRTC Gateway	This service is used for WebRTC connection to the system through Avaya one-X® Portal for IP Office. For example, for WebRTC from Space Calling and Avaya one-X® Portal for IP Office Chrome browser clients. It is not used for WebRTC from IP Office User Portal clients.
Web Client	This service allows users to use the Avaya IP Office Web Client for WebRTC softphone connections to Avaya one-X® Portal for IP Office using the **WebRTC Gateway** service. Users can access it using a Chrome browser on Windows and Mac PCs.
Web Collaboration	This service works with Avaya one-X® Portal for IP Office. It provides users with web collaboration services usable in parallel with audio conference hosted by IP Office. • This service is not supported for IP Office R12.0 and higher.

System

This table gives a general overview of the server status. This section also provides controls to shutdown or reboot the server.

Field	Description
OS/Kernel	The overall version of the Linux operating system installed on the server and the version of the operating system kernel.
Up Time	The system running time since the last server start.
Server Time	The current time on the server.
Average CPU Load	The average CPU load (percentage use) for the preceding minute, 5 minute and 15 minute periods. Note, it can take up to 10 minutes for CPU usage data to appear after a server reboot.
Material Code	The material code for the server. This code is used as part of the system registration with the Avaya Global Registration Tool (GRT).
Model Info	The model information for the server.
System Manufacturer Serial No	The manufacturer's serial number for the server.
Speed	The processor speed.
Cores	The number of processor cores.

Table continues…

Field	Description
Hard Disk Size	The hard disk size.
RAM	The amount of RAM memory.
Disk RAID Levels	The RAID type, if any, being used.
Disk Array Types	The type of disk array being used for RAID.
Quota available for backup data	Displays the amount of space reserved for local backups if **Enable HTTP file store for backup/restore** is enabled.
Virtualized	Indicates if the server is running as a virtualized session.
Last Successful Logon	The date and time of the last successful logon, including the current logon.
Unsuccessful Logon Attempts	A count of unsuccessful logon attempts.

Control	Description
Shutdown	Selecting this button starts a process that stops all services and then shuts down the server.
Reboot	Selecting this button starts a process that stops all services and then stops and restart the server.

Related links

The Platform View menus on page 131

Logs

Navigation: **Solution** > ☰ > **Platform View** > **Logs**

The **Logs** page contains a menu bar with the following items.

Log type	Description
Debug Logs	View the current log files for the server and the application services hosted by the server.
Syslog Event Viewer	View Syslog log records received or generated by the server.
Download	Create and download archive files of existing log records.

Related links

The Platform View menus on page 131
Debug Logs on page 135
Syslog Event Viewer on page 135
Download on page 135

Debug Logs

Navigation: **Solution** > ☰ > **Platform View** > **Logs** > **Debug Logs**

The menu shows the server application logs and audit log records.

Settings	Description
Application Log	This table lists the last 1000 log records for a selected server application. The **Application** drop-down selects the records shown. Clicking on a column header sorts the records using that column. For Voicemail Pro the level of log information output is set through the **Debug** section of the **Settings** > **General** menu. For Avaya one-X® Portal for IP Office the level of log information output is set through the Avaya one-X® Portal for IP Office administration menus.
Audit Log	This table lists the actions performed by users logged in through the IP Office Server Edition web browser interface. Clicking on a column header sorts the records using that column.

Related links

Logs on page 134

Syslog Event Viewer

Navigation: **Solution** > ☰ > **Platform View** > **Logs** > **Syslog Event Viewer**

This menu displays the server's Syslog records. These are combined records from the various applications (Voicemail Pro, Avaya one-X® Portal for IP Office, etc) running on the server and the server operating system itself. It also shows Syslog records received by the server from other servers. For example. in a Server Edition network, by default the Server Edition Secondary is configured to send its Syslog records to the Server Edition Primary.

You can use the **Settings** > **General** menu to configure the sending and receiving of Syslog records to and from other servers. You can also configure how long the server keeps different types of records and how many records it keeps.

The **Refresh** button is used to update the table of records shown using the options in the drop-down filters (**Host**, **Event Type**, **View** and **Tag**). Note however that the filter options are set when the menu is opened. To update the options, select another menu and then return to this menu. For example, if another host is added to the network and sends records to the server, the new server only appears in the **Host** drop-down after reloading the menu.

Related links

Logs on page 134

Download

Navigation: **Solution** > ☰ > **Platform View** > **System** > **Logs** > **Download**

You can use the menu to create and download archives files . For support issues, Avaya will require the archive files downloaded from the server. The server compresses the log files into a `.tar.gz` format file. You can then download the file by clicking on the link.

For IP Office 10.0, you can configure the server to include packet capture logs for the server, see Packet Capture Settings on page 143.

Related links

Logs on page 134

Updates

Navigation: **Solution** > ☰ > **Platform View** > **Updates**

This menu displays the different versions of server operating system files and application files available in the file repositories. The file repository locations are configured through the **Settings** > **General** page.

System

You can access this menu by selecting **Updates**. The **System** section shows details of the operating system.

Control	Description
Check Now	Clicking this button makes the IP Office Server Edition recheck the version of update files available in the file repository. Normally it does this automatically when the Updates page is loaded.
Review updates	Clicking this button will display a list of the available update files. This list allows selection of which updates you want to install.
Update All	Clicking this button will install all the available updates without going through the process of selecting with updates to install.

Services

You can access this menu by selecting **Updates**. The **Services** section shows details of the current version of each application installed and the latest version available.

The **Change Version**, **Update**, **Update All**, and buttons in the panel are not useable unless appropriate update files are available in the applications software repository . This also affects the availability of the **Install** button option.

Control	Description
Change Version	Clicking on this button shows the update files available for the application in the server's file repository with the current version selected. Selecting another version and clicking **Apply** upgrades or downgrades to that version.
Update	Clicking on this button starts an update of the related application to the latest available version in the application file repository.

Table continues…

Control	Description
Uninstall	Clicking on this button uninstalls the selected application. • If there are installation files for the application in the application file repository, the button becomes an **Install** button. • If there are no installation files for the application in the file repository, the menu no longer list the application.
Install	This button appears for uninstalled applications if the server has files for the application the application file repository.
Check Now	Clicking this button makes the IP Office Server Edition recheck the version of update files available in the file repository. Normally it does this automatically when the **Updates** page is loaded.
Clear Local Cache	Clicking this button removes older update installation files and other material that may accumulate on the server over time.
Update All	Clicking this button upgrade those applications that support upgrading without being uninstalled (see above) to the latest versions available in the application file repository.

Related links

The Platform View menus on page 131

Settings

Navigation: Solution > ☰ > **Platform View** > **Settings**

The **Settings** page contains a menu bar with the following items.

- **General**: General server settings such as the locations of software update repositories.
- **System**: View and manage the server settings.

Related links

The Platform View menus on page 131
General Settings on page 137
System Settings on page 145

General Settings

Navigation: Solution > ☰ > **Platform View** > **Settings** > **General**

Related links

Settings on page 137
Software Repositories on page 138
Syslog on page 138
Certificates on page 139

Web Control on page 141
Backup and Restore on page 141
Voicemail Settings on page 142
EASG Settings on page 142
Packet Capture Settings on page 143
Watchdog on page 144
Set Login Banner on page 144
one-X Portal Settings on page 144
Media Manager on page 145

Software Repositories

The IP Office Server Edition can use either remote or local software repositories to store software update files. The server has separate repositories for operating system updates, IP Office application installation files and Windows client files. The **Updates** and **AppCenter** menus use the files present in the appropriate repository.

Field / Control	Description
Repository	If not using the **Local** option, this field sets the URL of a remote Linux OS repository. Note that you cannot use the same URL for more than one repository.
Local	This checkbox sets whether the file repository used is local (files stored on the IP Office Server Edition) or remote (a folder on a HTTP web server specified in the Repository field).
File / Browse / Add	With **Local** selected, you can use this field and adjacent buttons to browse for a specific update file. After selecting the file, click Add to upload the file to the server's file store.

Related links

General Settings on page 137

Syslog

These settings control the receiving and the forwarding of Syslog records by the server. These options are not shown for an Server Edition Expansion System (L). For details of system monitor Syslog records, refer to the Using IP Office System Monitor" manual.

Field/Control	Description
Log files age (days)	Default = 1 day. Set the number of days the server retains each type of record before automatically deleting it. Separate settings are available for **General log files**, **Security log files**, **Audit log files**, **Operational log files** and **Debug log files**. These settings are not applied to the server's own Syslog monitor records which are retained for 3 days. • **Apply general settings to all file types**: If selected, the setting for **General log files** is applied to all file types.

Table continues…

Field/Control	Description
Max log size (MB)	Default = 29MB. Set the maximum total size of each type of records the server retains before automatically deleting the oldest records. Separate settings are available for **General log files**, **Security log files**, **Audit log files**, **Operational log files** and **Debug log files**. These settings are not applied to the server's own Syslog monitor records. • **Apply general settings to all file types**: If selected, the setting for **General log files** is applied to all file types.
Receiver Settings	These settings control if and how the server can receive Syslog records. • **Enable**: If selected, the server can receive Syslog records using the port configured below. • **TCP Port**: Sets the port number used for receiving Syslog records using **TCP**. • **TLS Port**: Sets the port number used for receiving Syslog records using **TLS**. • **UDP Port** - Sets the port number used for receiving Syslog records using **UDP**.
Forward Destination 1	These settings control whether the server forwards copies of Syslog records it receives to another server. • **Enable**: If selected, the server will forward copies of the Syslog records it receives. • **IP Address: Port**: Sets the address of the destination server and the destination port for the forwarded records. • **Protocol**: Set the protocol, **UDP**, **TLS** or **TCP**, for the forwarding.
Forward Destination 2	These settings control whether the server forwards copies of the Syslog records it receives to a second server. The settings are the same as for the first forwarding destination.
Select Log Sources	These options allow selection of which server reporting to include in the Syslog reports. The available options are: • **Authentication and authorization privileges** • **Information stored by the Linux audit daemon (auditd)** • **NNTP(News)/UUCP(Usenet) protocols** • **Apache web server access_log and error_log**

Related links

General Settings on page 137

Certificates

This menu allows the generation or downloading of the security certificate that can then be used by the IP Office applications hosted by the server. These menus are not available on Server Edition Secondary server and Server Edition Expansion System (L) servers.

Field/Control	Description
CA Certificate	

Table continues…

Field/Control	Description
Create new	If selected, the server generates a new own security certificate when **Regenerate** is clicked.
Renew existing	If selected, the server's current self-generated security certificate is renewed when **Regenerate** is clicked.
Import	If select, the fields for browsing to and selecting a certificate file to upload to the server appear. Select the file and click **Upload**.
Export	The server's current security certificate is not included in any application backup and restore operations. The **Export** option allow you to export the server's current certificate as an encrypted file. You can then later restore the certificate back to the same server using the **Import** option. • **Password/Confirm Password**: Enter a password that the server then applies to the encrypted certificate file when using **Encrypt and Download**.
Encrypt and Download	When pressed, the server displays a pop-up link from which you can download an encrypted file containing the server's current certificate. Once you have downloaded the file it is deleted from the server.
Regenerate	Create a certificate or renew the existing certificate.
Download (PEM-Encoded)	Download the certificate as a PEM file. You can then apply the certificate to any remote device that needs to establish secure encrypted connection with the server.
Download (DER-Encoded)	Download the certificate as a CRT file. You can then the certificate to any remote device that needs to establish secure encrypted connection with the server.

Field/Control	Description
Identity Certificates	
Renew automatically	If selected, the server automatically generates a new security certificate following any major change such as changes to its LAN settings. The server automatically applies the new certificate to the application services run on the server.
Create certificate for a different machine	If selected, the server can generate a new security certificate for another server. Note however that this requires a settings to exactly match those of the other server in order for the certificate to be regarded as valid for one offered by that other server.
Regenerate and Apply	When clicked, the server generates a new security certificate using the identity settings specified. The server then applies the security certificate to the IP Office application services run by the server. Note that this process requires the services to all be automatically stopped and restarted which will end any current connections.
Download (PEM-Encoded)	Download the certificate as a PEM file. You can then apply the certificate to any remote device that needs to establish secure encrypted connection with the server.

Table continues…

Field/Control	Description
Download (DER-Encoded)	Download the certificate as a CRT file. You can then the certificate to any remote device that needs to establish secure encrypted connection with the server.

Related links

General Settings on page 137

Web Control

Note that changing any of these settings will require you to login again.

Field/Control	Description
Inactivity Timeout	Default = 10 minutes. Select the period of inactivity after which the server automatically logs out the web session. Changing this value requires you to login again. The options are **5 minutes**, **10 minutes**, **30 minutes**, and **1 hour**.

Related links

General Settings on page 137

Backup and Restore

These controls allow you to backup and restore the application settings of selected IP Office applications.

- This is a local backup onto the same server and should only be used when directed by Avaya support.
- For more advanced backup and restore functions, see Backup and Restore on page 638.
- These options are not shown if the web control menus are accessed as an embedded window from within Web Manager.

Applications	Description
IP Office	These control provides options to backup/restore the configuration settings of the IP Office application running on the server.

Table continues…

Applications	Description
Voicemail	For the Voicemail Pro server, these controls can only be used to restore an existing backup. Using the Voicemail Pro client, you can configure the voicemail server to perform regular (daily, weekly and or monthly) automatic backups of selected options including messages and prompts. You can also use the Voicemail Pro client to perform an immediate backup. • Selecting the **Restore** button displays the backups available in the backup folder (`/opt/vmpro/Backup/Scheduled`). The backup name includes the date and time and whether the backup was a manual or scheduled backup. Selecting a backup and clicking **OK** starts the restoration process. For details, refer to the Voicemail Pro client help. • The restoration process requires the voicemail service to shutdown and restart. This does not occur if any Voicemail Pro client is connected to the service during the restore and leads to an incorrect restoration of files.
WebRTC Gateway	Allow backup and restoration of the WebRTC settings.

Related links

General Settings on page 137

Voicemail Settings

This setting sets the debug logging level used by the Voicemail Pro application if running. Log files are retrievable through the **Logs** > **Download** menu.

Field/Control	Description
Debug Level	Default = Information This control sets the level of information that the service includes in its log files. The options are **None**, **Critical**, **Error**, **Warning**, **Information** and **Verbose**.

Related links

General Settings on page 137

EASG Settings

The server uses these settings for connections from an Avaya Enhanced Access Security Gateway (EASG) server. EASG is used by systems' being supported directly by Avaya. It allows Avaya technician access to the server for server maintenance.

Note that only users with Web Services Security rights are able to change the EASG settings.

Filed/Control	Description
Status	This field sets whether the EASG service is enabled on the server. In order to use EASG the server's product ID must be registered through the Avaya Global Registration Tool (GRT) website.

Table continues…

Filed/Control	Description
Port	Default = 2222 This field sets the port on which the service listens for connections. The default port is 2222.
Service Listening	Select whether the server listens on any connection (**Any**) or just on SSL VPN tunnels (**Any Tunnel**). • **Any**: If selected, the server listens on any connection. This setting is deprecated as it is less secure than Any Tunnel. • **Any Tunnel**: If selected, the server only listens on SSL VPN connections. This requires the IP Office configuration to include an SSL VPN tunnel.
EASG Users	Default = *craft* This drop down lists the different types of user logins (*craft*, *init*, *inads*, *rasaccess* and *sroot*) that may be used by the EASG service and technicians.
EASG User Enabled	Sets whether access by the **EASG Users** currently selected above is enabled or disabled.
EASG Technician Certificates	Lists the current technician certificates present on the server. • **Delete Selected Certificate**: Delete the certificate currently selected in the EASG Technician Certificates selector above. • **View Selected Certificate**: View the certificate currently selected in the EASG Technician Certificates selector above.
Upload Technician Certificate	Certificates are used to control technician access to the server for maintenance actions. If a technician requires access to the server for maintenance, they will provide a certificate that must first be uploaded to the server using this menu. Typically these are short-lived certificates valid for the period of potential maintenance access needed, for example 14 days. • **Browse**: Browse for the certificate file to upload. • **Password**: Enter the password for the certificate. • **Upload**: Click to upload the selected certificate file.
Product Id	The product ID. This is the ID registered with the EASG server from which the server is maintained.
Change Product Id	If clicked a new ID is generated for the server. This will require the server to be re-registered with the Avaya GRT website.

Related links

General Settings on page 137

Packet Capture Settings

Supported for IP Office Release 10.0 and higher. This menu allows the configuration of packet capture on one or all of the server's LAN interfaces. When enabled, traffic is logged to tcpdump log files that can be downloaded from the **Logs** > **Download** menu along with other log files.

Field/Controls	Description
Interface	Default = All This field allows selection of the server LAN interface to which packet capture is applied when run.
Maximum File Size (MB)	Default = 100MB, Range = 1MB to 2000MB This field sets the maximum size of each individual log file size. When the current file reaches this size a new log file is started.
Maximum File Number	Default = 10, Minimum = 1 This field sets the maximum number of packet capture log files. On reaching this limit, when the server starts a new log file it also automatically deletes the oldest log file.
Maximum Total Size (MB)	Default = 5120MB This field shows the total allowed file space for packet capture log files. The combined values of the fields above cannot exceed this value.
Start/Stop	Default = Stopped These buttons control whether packet capture logging is running or not.

Related links

General Settings on page 137

Watchdog

Field/Control	Description
Log files age (days)	Default = 5 days. Sets the number of days that log file records are retained. This does not affect log file archives . Not applied to Avaya one-X® Portal for IP Office.

Related links

General Settings on page 137

Set Login Banner

Field/Control	Description
Login Banner Text	You can use this field to set the additional text displayed on the login menu. After changing the text click Save. By default the field is blank.

Related links

General Settings on page 137

one-X Portal Settings

For a Server Edition network, the Avaya one-X® Portal for IP Office service normally run on the IP Office Server Edition server can be replaced by the portal service running on an IP OfficeApplication Server. After stopping and disabling the auto-start of the primary server's portal service, the following fields are used to

For IP Office Release 10, the Server Edition Secondary server can also host a portal service for resiliency, refer to the *Administering Avaya one-X Portal for IP Office* manual for full details. In that case, again, the portal service on the secondary can be replaced by one running on an IP OfficeApplication Server in the same way.

Field/Control	Description
Use Local IP	Select this option if the server is hosting the Avaya one-X® Portal for IP Office application. If not selected, the Avaya one-X® Portal for IP Office service should be stopped and its auto-start options disabled. The IP address of the IP OfficeApplication Server hosting the alternate Avaya one-X® Portal for IP Office must be indicated in the **Remote IP** field below.
Remote IP	If **Use Local IP** is not selected, this field sets the IP address of the separate IP OfficeApplication Server hosting the Avaya one-X® Portal for IP Office application.

Related links

General Settings on page 137

Media Manager

Filed/Controls	Description
Call ID	Enter the call ID of the recording that should be deleted. Multiple IDs can be entered, separated by spaces. The call ID for particular recordings are shown in the recordings menu in web manager (**Applications** > **Media Manager** > **Recordings**).
Delete Recordings	Delete the recordings associated with the call IDs entered.

Related links

General Settings on page 137

System Settings

Navigation: Solution > ☰ > **Platform View** > **Settings** > **System**

Related links

Settings on page 137
Network on page 146
Avaya IP Office LAN Settings on page 148
Date and Time on page 148
Authentication on page 149
Increase Root Partition on page 150
HTTP Server on page 150
Change Root Password on page 151
Change Local Linux Account Password on page 151
Password Rules Settings on page 151
System Identification on page 152
Firewall Settings on page 152
Additional Hard Drive Settings on page 153

Network

Navigation: **Server Menu** > **Platform View** > **Settings** > **System**

Warning:

- **! = Host PLDS ID Field**

  For a virtualized server, IP Office uses the fields marked with a **!** symbol to generate the **Host PLDS ID**. Changing any of the fields can change that ID. If you have used the ID to generate local (nodal) PLDS licenses, those licenses become invalid. This does not affect WebLM (centralized) PLDS licenses. Refer to the manual "Deploying Avaya IP Office Servers as Virtual Machines" for further details.

Important:

- *** = Security Certificate Field**

  The IP Office uses fields marked with a ***** symbol as part of the self-signed certificate it generates. If you change one of these fields, the IP Office generates a new self-signed certificate. Certificate generation disrupts access to the server for several minutes. In addition, you must update the certificate used by any applications.

Settings	Description
Network Interface	Default = Eth0 Selects the network interfaces you are configuration. Within the IP Office configuration, **Eth0** matches **LAN1**, **Eth1** matches **LAN2**.
Enable IPv6	Default = Disabled When enabled, the IP Office system supports IPv6 features on the selected LAN. IP Office supports IPv6 on Linux-based IP Office systems only.
Host Name ! *	Sets the host name that the IP Office Server Edition should use. This setting requires the local network to support a DNS server. Do not use **localhost**. • For internal use, this value must be resolvable by DNS within the customer network. • If the IP Office is also supporting external client connections, the value must also be resolvable to the IP Office by external DNS. External access must also include a firewall and/or SBC. • Consult with the customer's IT support to ensure the name is acceptable and that routing to it is configured correctly.
Use DHCP ! *	If selected, the IP Office obtains its IP address, subnet mask and default gateway information by making a DHCP request. The menu displays the values obtained.
IP Address ! *	Displays the IP address set for the server. If not using DHCP, you can edit the field to change the setting.
Subnet Mask	Displays the subnet mask applied to the IP address. If not using DHCP, you can edit the field to change the setting.
Default Gateway	Displays the default gateway settings for routing. If not using DHCP, you can edit the field to change the setting.

Table continues…

Settings	Description
System DNS	The address of the primary DNS server. Disabled when **Automatically obtain DNS from provider** is enabled.
Automatically obtain DNS from provider	Default = Enabled This setting is available after enabling **Use DHCP**. • If enabled, the IP Office requests DNS server details from the DHCP server. If disabled, the IP Office uses the **System DNS** value.
Create Subinterface	Create a subinterface.
Delete Subinterface	Delete the subinterface.

IPv6 address settings

You can use the following settings after enabling **Enable IPv6**.

Settings	Description
Use DHCPv6	Default = Enabled The IP Office system request IPv6 address information from a DHCPv6 server on the LAN.
IPv6 Address	Default = Blank Sets or shows the IP Office IPv6 address on the LAN. • You cannot change the address if the IP Office is a DHCPv6 client. • You cannot change the address if the IP Office is using **Stateless Address Auto-configuration (SLAAC)**. • If setting a static address, the IP Office supports /64 subnet prefixes only. - The IP Office supports IPv6 addresses in the following formats: • Full address: For example, `2001:0000:040F:0000:0000:0000:805B:001B`. • Replace one series of `:0000:` parts with `::`. For example, `2001:0000:040F::805B:001B`. • Replace any individual `:0000:` parts with `:0:`. For example, `2001:0:040F::805B:001B`. • Remove leading `0` zeros after any `:` colon. For example, `2001:0:40F::805B:1B`.
Prefix	Default = 64 When using a static IPv6 address, the IP Office uses a fixed */64* prefix.
Default Gateway	Display = Blank Displays the default gateway settings for routing. If not using DHCP, you can edit the field to change the setting.

Table continues…

Settings	Description
System DNS	Default = Blank The address of the primary DNS server. Disabled when **Automatically obtain DNS from provider** is enabled.
Automatically obtain DNS from provider	Default = Enabled This setting is available after enabling **Use DHCPv6**. • If enabled, the IP Office requests DNS server details from the DHCP server. If disabled, the IP Office uses the **System DNS** value.

Related links

System Settings on page 145

Avaya IP Office LAN Settings

Settings	Descriptions
Avaya IP Office LAN1	These settings are used for the LAN1 interface of the IP Office application run by the server. LAN1 is also referred to as LAN. **Enable Traffic Control**: Default = Disabled. When enabled, the server throttles the rate at which it sends UDP packets from the IP Office service to System Status Application. This may be necessary if the System Status Application traces indicate a high number of lost packets. **Network Interface**: Use the drop-down to select which port on the server should be used for LAN1.
Avaya IP Office LAN2	These settings are used for the LAN2 interface of the IP Office application run by the server. LAN2 is also referred to as WAN.

Related links

System Settings on page 145

Date and Time

The server uses these settings to set or obtain a UTC date and time.

Important:

- Avaya strongly recommend **Enable Network Time Protocol Client** is enabled and a list of **NTP Servers** set. An accurate time is essential for features which use certificates and/or subscriptions.

Settings	Description
Date	This field shows the current server date. If not using NTP: • On physical servers, you can use the field to change the date. • On virtual servers, the virtual server will take the date from the virtual server host platform.
Time	This field shows the current server UTC time. If using NTP: • On physical servers, you can use the field to change the time. • On virtual servers, the virtual server will take the time from the virtual server host platform.
Time Zone (!)	Some features require the local time rather than the UTC time. The **Time Zone** field determines the appropriate offset to applied to the UTC time. Note that changing the timezone can cause a "Session expired" message to appear in the browser in which case you need to login again.
Enable Network Time Protocol Client	When selected, the server obtains the current date and time from the NTP servers listed in the **NTP Servers** list below. The server uses the date and time supplied and makes regular NTP requests for updates.
NTP Servers:	With **Enable Network Time Protocol Client** selected, use this field to enter the IP address of an NTP server or servers to use. Enter each address as a separate line. The network administrator or ISP may have an NTP server for this purpose. • A list of publicly accessible NTP servers is available at http://support.ntp.org/bin/view/Servers/WebHome. However, it is your responsibility to comply with the usage policy of the chosen server. • Choose several NTP servers in case one of the NTP servers becomes unreachable or unreliable. The server uses the responses it receives from each NTP server to determine reliability.

Related links

System Settings on page 145

Authentication

This menu controls the method of password storage and authentication used by server applications.

- These settings are only accessible if logged in using referred authentication or as the local Linux root. When disabled, the setting can only be re-enabled by logging in using the local Linux root name and password.

Settings	Description
Enable referred authentication	Default = Enabled The password authentication used for access to the some services hosted by the server use either each services' own security settings or the security user accounts configured in the IP Office service running on the IP Office Server Edition. This setting controls which method is used. • **Enabled** The security settings of the IP Office service running on the server control access to the following other services: - Web control menus - Voicemail Pro admin - Avaya one-X® Portal for IP Office - IP Office Web Manager • **Disabled** Each service controls access using its own local account settings.

Related links

System Settings on page 145

Increase Root Partition

This menu option is supported for VMware virtualized servers. If through the VMware menus you increase the size of the root disk, you also need to use this menu to instruct the virtual server to use the additional space.

Settings	Description
Increase Partition Size	This menus indicates when additional disk space is available. Clicking the button instructs the server to adjust its root partition to include that additional space and to format the additional space appropriately. After clicking **Save**, you must restart the server.

Related links

System Settings on page 145

HTTP Server

This setting controls where the server allows storage for HTTP/HTTPS backup.

Settings	Description
Enable HTTP file store for backup/ restore	If selected, the server can act as the 'remote server' destination for backups configured through the Web Manager menus. See Deploying IP Office Server Edition. When enabled, the **System** menu displays the quota available for backups. • Servers without Voicemail Pro only support this option on disks larger than 95GB. • Servers with Voicemail Pro only support this option on disks larger than 155GB.

Related links

System Settings on page 145

Change Root Password

Server installation creates two Linux user accounts; *root* and *Administrator*. You can use these fields to change the Linux *root* account password.

- These settings are only accessible if logged in via referred authentication or as the local Linux root. Therefore, when disabled, the setting can only be re-enabled by logging in using the local Linux root name and password.
- Note that this is separate from the password for the IP Office *Security* account. Whilst both accounts are given the same password during server ignition, this menu changes just the Linux account password. You can change the IP Office *Security* account password through the IP Office security settings.

Related links

System Settings on page 145

Change Local Linux Account Password

Server installation creates two Linux user accounts; *root* and *Administrator*. You can use these fields to change the Linux *Administrator* account password.

- These settings are only accessible if logged in via referred authentication or as the local Linux root. Therefore, when disabled, the setting can only be re-enabled by logging in using the local Linux root name and password.
- Note that this is separate from the password for the IP Office *Administrator* account. Whilst both accounts are given the same password during server ignition, this menu changes just the Linux account password. You can change the IP Office *Administrator* account password through the IP Office security settings.

Related links

System Settings on page 145

Password Rules Settings

These settings set the password requirements used when changing passwords through using these menus.

Settings	Description
Minimum password length	This field set the minimum length of new passwords. Note that the combined requirements of the fields below for particular character types may create a requirement that exceed this value. Note also that the maximum password length is 31 characters.
Minimum number of uppercase characters	This field sets the number of uppercase alphabetic characters that new passwords must contain.

Table continues…

Settings	Description
Minimum number of lowercase characters	This field sets the number of lowercase alphabetic characters that new passwords must contain.
Minimum number of numeric characters	This field sets the number of numeric characters that new passwords must contain.
Minimum number of special characters	This field sets the number of non-alphanumeric characters that new passwords must contain.
Allow character sequences	When selected, the server allows character sequences such as `1234`, `1111`, or `abcd`. When not selected, the field below sets the maximum length of any sequence.
Maximum allowed sequence length	When **Allow character sequences** is not selected, this field sets the maximum allowed length of any character sequence.

Related links

System Settings on page 145

System Identification

These settings are shown are for information only.

Settings	Description
Platform Hash **System ID (SID)**	This is the unique system reference used to validate licenses issued for this particular system. • For a physical server, this is a value based on the server hardware. • For a virtual server, this is a value based on several factors including the LAN1 and LAN2 IP addresses, the host name, and the timezone. If any of those are changed, this value can change and any existing licenses become invalid.
Licensing Mode	Indicates the licensing method used by the system. **Internal** indicates that the system uses the unique above.

Related links

System Settings on page 145

Firewall Settings

The IP Office server can apply firewall controls to the incoming traffic it receives. These are in addition to firewall profile settings added to the IP Office service configuration.

Settings	Description
Activate	Default = On Sets whether the firewall is active. You must enable this setting if the IP Office configuration is using any firewall profile settings.

Table continues…

<table>
<tr><th>Settings</th><th>Description</th></tr>
<tr><td>Enabled Filtering</td><td>Default = Off

Sets whether the firewall should apply the following filtering settings to traffic when Active.</td></tr>
<tr><td>Enable TCP ports

Enable UDP ports</td><td>Select whether the server allows the following TCP and UDP ports when Enabled Filtering is enabled.

<table>
<tr><th>Port</th><th>Default Settings</th></tr>
<tr><td>21</td><td>Default = On</td></tr>
<tr><td>25</td><td>Default = On</td></tr>
<tr><td>80</td><td>Default = On</td></tr>
<tr><td>8000</td><td>Default = Off

Warning:
• Enabling filtering with port 8000 disabled blocks centralized upgrading from the primary server of associated secondary, application and expansion servers.</td></tr>
<tr><td>8069</td><td>Default = On</td></tr>
<tr><td>8080</td><td>Default = On</td></tr>
<tr><td>8666</td><td>Default = Off</td></tr>
<tr><td>9080</td><td>Default = On</td></tr>
</table>
</td></tr>
<tr><td>Enable UDP ports</td><td>
<table>
<tr><th>Port</th><th>Default Setting</th></tr>
<tr><td>69</td><td>Default = On

If selected, allow port UDP 69.</td></tr>
</table>
</td></tr>
</table>

Related links

System Settings on page 145

Additional Hard Drive Settings

These additional settings appear on servers with an additional hard disk.

Settings	Description
Additional Hardware Info	The fields vary depending on the type and location of the additional hard disk.

Table continues…

Settings	Description
Mount	• **Activate**: Enabling this option automatically mounts the additional hard disk. • **Mount Point Path**: This is the root name assigned for the additional hard disk and the disk partition. The full mount path name for each partition is automatically configured by the system adding /partition1, /partition2, etc. as a suffix. For Media Manager set the name to /additional-hdd#1. • **Current Partition Mount Points**: This field shows the full path for the partitions created on the disk. This is the path that should be used for other applications to use the partition. For example this is the value to use for the Media Manager application's **Call Storage Path** setting.
Format Hard Drive	These options are shown for an additional hard drive added after initial system installation. • **Enable**: Is selected, format the additional drive using the partition settings below. This will erase any existing data on the additional drive. • **Partition X size (GB)**: Set the size for the partitions, up to 3, to be created on the additional drive when formatted.

Related links

System Settings on page 145

AppCenter

Solution > ☰ > **Platform View** > **AppCenter**

You can access this menu by selecting **AppCenter**. You can use the menu to download files for use on the local PC. For example, the Voicemail Pro client used to administer the Voicemail Pro server application.

Note that some packages require the addition of licenses to the system and configuration changes. Refer to the specific installation manuals for those applications:

File	Description
`VmPro...ClientOnly.exe`	This is the installation package for the Voicemail Pro client application used to administer the Voicemail Pro server application.
`VmPro...Mapi.exe`	This is the installation package for the MAPI proxy. This is installed on a Windows PC in the same network as the Windows Exchange server. It allows the Voicemail Pro server to access UMS services. See the Administering IP Office Voicemail Pro manual.

Table continues…

File	Description
`AdminLite...`	This is the installation package for the IP Office Manager, SysMonitor and System Status Application tools. • Note: The version of IP Office Manager installed by this package runs in English only and does not include the files needed for actions such as IP500 V2 system upgrades, phone firmware support, SD card recreation, and so on. If needed, download the full administration suite installer from support.avaya.com.
`DLink...`	This is the installation package for the IP Office DevLink third-party TAPI interface.
`TAPI...`	This is the installation package for the IP Office first-party TAPI interface.
`Softconsole...`	This is the installation package for the IP Office SoftConsole application. This application is used by receptionist and operator users to answer and distribute incoming calls.

Related links

The Platform View menus on page 131

Part 3: The Call Management Menu

The Call Management Menus

The **Call Management** menu provides access to various configuration records for key features. The lists for each type can be used to add, edit and delete those records.

Sub-Menu	Description
Auto Attendants	Auto-attendants are services that the system can provide to answer calls and prompt the caller for which service they require or who they want to talk to. Auto attendants can be used as the destination for incoming call routes.
Conferences	In addition to ad-hoc and personal conference features, systems support system meet-me conferences.
Extensions	Each physical phone (desk phone) registered with the system requires a matching extension record in the system configuration.
Groups	Groups are collections of multiple users. Each group has an extension number and can be used as the destination for calls.
Users	Users are the individual users who make and answer calls. They can do this via physical phones or softphone applications.

Chapter 14: Users

Navigation: **Call Management** > **Users**

Additional configuration information

This section provides the **Users** field descriptions.

For additional configuration information, see Configure User Settings on page 831.

Main content pane

The **Users** main content pane lists provisioned users. The contents of the list depends on the filter option selected. Click the icons beside a record to edit or delete.

Bulk delete: You can delete multiple records. Select the check box to the right of each record you want to delete and click **Delete**. You receive a prompt to confirm the deletion.

Click **Actions** for import, export, and template management options.

Click **Add/Edit Users** to open the Add Users window where you can provision a user. When you click **Add/Edit Users**, you are prompted to specify the server on which the user will be provisioned.

User Filters

Filter	Description
Show All	List all provisioned users on all systems.
Systems	List the users provisioned on a specific system.
User Type	List a specific provisioned user type on all systems.
User Rights	List users provisioned with specific user rights on all systems.
Hunt Groups	List users that are members of a hunt group.

Related links

User Actions on page 158
Users on page 160
Voicemail on page 168
Button Programming on page 174
Telephony on page 174
Short Codes on page 185
Forwarding on page 186
Mobility on page 190
Group Membership on page 194
Voice Recording on page 194

Do Not Disturb on page 196
Announcements on page 197
Personal Directory on page 199
SIP on page 200
Menu Programming on page 201
Dial In on page 204
Source Numbers on page 204
User Portal on page 205

User Actions

Navigation: **Call Management** > **Users** > **Actions**

Related links

Users on page 157
Import Users on page 158
Export users on page 158
User Template Management on page 159
Create From Template on page 159
Provision Users on page 159

Import Users

Navigation: **Call Management** > **Users** > **Actions** > **Import Users**

Bulk provision users by importing a xml or csv file. You can download example files.

Field	Descriptions
Import To	Specify the system where the file will be imported to.
Select a File	Select the file on the local machine.
Sample Import Files	Download a sample user file.

Related links

User Actions on page 158

Export users

Navigation: **Call Management** > **Users** > **Actions** > **Export Users**

Export a list of users to an .xml file on the local machine. When the Export window opens, you have the option to export all users or only the users currently listed in the main content pane.

Related links

User Actions on page 158

User Template Management

Navigation: **Call Management** > **Users** > **Actions** > **Template Management**

Select the **Template Management** action to open the User Templates page. Click **Add** to define a user template.

Related links

User Actions on page 158

Create From Template

Navigation: **Call Management** > **Users** > **Actions** > **Create From Template**

Use this page to add users using a template. You can define user templates by selecting **Call Management** > **Users** > **Actions** > **Template Management**.

When you click **Create From Template** and then select a server, the Select Template window opens.

Once you have defined the settings below and click **OK**, the Provision Users page opens.

Field	Description
Enter number of records	Enter the number of records you want to create.
Enter starting extension	Enter the extension number of the first record.
Select Template	Select a template from the list.

Related links

User Actions on page 158

Provision Users

Navigation: **Call Management** > **Users** > **Actions** > **Create From Template** > **Select Template** > **Provision Users**

This page displays the user records that will be created based on the values entered in the Select Template window.

At the top of the page, the **Preview Users Data** area indicates the server on which the users will be created, the number of records (**Total Records Read**) and the **Records with Error**.

The table lists the user records that will be created and the values that have been populated based on the template. You can remove records from the list using **Delete Selected Records**. You can modify the display by turning **Show Error Records** on or off.

You can modify a record by clicking the edit icon for the record to open the User - Edit window.

When you are ready to create the new user records, click **Create**.

Related links

User Actions on page 158

Users

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **User**

Additional configuration information

- For a summary of user management, including a description of centralized users, see User Management Overview on page 831.
- The **Unique Identity** setting is used to configure Gmail Integration. For additional information, see Configuring Gmail Integration on page 833.

Users are the people who use the system or are Dial In users for data access. A user does not have to have an extension number that physical exists - this is useful if the user do not require a physical extension but wish to use system features.

- The **NoUser** user is used to apply settings to extensions which have no associated user. Do not delete this user/
- The **Remote Manager** user is used as the default settings for dial in connections.

Configuration Settings

You can edit these settings online without needing to reboot the IP Office.

- Except adding/removing centralized branch users which requires a system reboot.

Field	Description
Name	Range = Up to 15 characters. This is the user's account name used for RAS Dial In, caller display and voicemail mailbox. As the display on caller display telephones is normally 16 characters, it is useful to keep the name short. • Only alphanumeric characters and space are supported in this field. • Names should not start with a space. • Do not use punctuation characters such as #, ?, /, ^, > and ,. • This field is case sensitive and must be unique. • If the IP Office system includes voicemail: - Voicemail uses the name to create a matching user mailbox. Changing a user's name will routes their voicemail calls to a new mailbox. - Voicemail Pro is not case sensitive. It treats names such as *"Steve Smith"*, *"steve smith"* and *"STEVE SMITH"* as all being the same user. • If the IP Office system includes Avaya one-X Portal: - Do not use the Name *"admin"*. That user name is a reserved value for Avaya one-X Portal use. - Do not use names that include a _ character.

Table continues…

Field	Description
Authentication Name	Default = Blank. Range = Up to 31 alphanumeric characters. Used on an IP500 V2 system configured as an Avaya Aura X for Avaya Cloud Office (ACO) gateway. See the Deploying IP Office as an Avaya Aura X for Avaya Cloud Office (ACO) ATA Gateway manual.
Password	Default = Blank. Range = Up to 31 alphanumeric characters. This password is used by user applications such as IP Office SoftConsole, User Portal and TAPI. It is also used for users with Dial In access. • Note that this is not the user's voicemail mailbox password (see **Call Management** > **Users** > **Add/Edit Users** > **Voicemail** > **Voicemail Code**) or their phone log in code (see **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Supervisor Settings** > **Login Code**). • The password complexity rules are set through the IP Office security settings. IP Office Manager will display an error if the password does not meet the complexity requirements. However, IP Office Manager will still allow you to save the configuration (unless the system locale is set to **France2**).
Unique Identity	Default = Blank. An email address for the user. The address must be unique for each user. This email address is used for: • Avaya Spaces/Avaya Workplace Client login. - When used in these roles, for pre-R11.1.2 systems, the unique identity is limited to 15 characters maximum before the @ character. • Gmail voicemail to email messages. This setting is separate, though it can be the same address, from the user's **Email Address** setting (see below) which is used for other email functions such as voicemail email.

Table continues…

Field	Description
Login Code **Confirm Login code**	Default = Blank. Range = Up to 31 digits. • Login code must be at least 4 digits for DS port users. • Login codes of up to 15 digits are supported with **Extn Login** buttons. • Login codes of up to 31 digits are supported with **Extn Login** short codes. This code is used for logging in on a phone (and for restricting access to features on phones. See Hot Desking on page 876. • Hot desking is not supported for centralized users. Centralized users use the **Login Code** for SIP registration on Session Manager. • Normally users can only log out if they have a **Login Code** set or if they are currently logged in at an extension whose **Base Extension** number no longer matches their own **Extension** setting. • When set, the short code feature **Change Login Code** can be used by users to change their login code. • If the user has a login code set, it is used by the **Outgoing Call Bar Off** short code feature. • If the user has a login code set, access to a range of programmable button features requires entry of the login code. For example, access **Self Admin** and **System Phone** features.
Audio Conference PIN	Default = Blank. Range = Up to 15 numeric characters. Use this field to configure PIN access for meet me conferences. • An **L** in this field disabled the unscheduled meet-me conference feature for the user.
Account Status	Default = Enabled. Use this setting set the user account to **Enable**, **Disable**, or **Force New Password**. • When set to **Force New Password**, the user can only set a new password by logging in using Avaya one-X Portal. The IP Office system can change if they make too many failed log in attempts. This uses settings configured in the IP Office security setting: • If a user exceeds the **Password Reject Action**, then the **Password Reject Action** is implemented. - If the **Password Reject Action** is **Log and Disable Account**, then the account status is changed to **Locked - Password Error**. - If the **Password Reject Action** is **Log and Temporary Disable**, then the account status is changed to **Locked - Temporary**.

Table continues…

Field	Description
Full Name	Default = Blank Use this field to enter the user's full name. When set, the **Full Name** is used in place of the **Name** for display by phones and user applications. • Names should not start with a space. • Do not use punctuation characters such as @, #, ?, /, ^, > and ,. • The recommended format is <first name><space><last name> for the name to be used correctly by voicemail dial by name features.
Extension	Range = 2 to 15 digits. In general all extensions should have the same number of digits. This setting can be left blank for users used just for dial in data connections. • Users associated with IP phones or who may log in as such devices should not be given extension numbers greater than 7 digits. • Centralized users' extension numbers can be up to 13 digits in length. Although IP Office supports extension numbers up to 15 digits, the 13-digit length is determined by the maximum extension number length allowed for provisioning Centralized users in Communication Manager.
Email Address	Default = Blank This address is used as the user's email address for a range of functions. Primarily it is used for voicemail-email functions if required. It is also used for any other emails that the system may send to the user.
Locale	Default = Blank (Use system locale) Configures the language used for voicemail prompts played to the user, assuming the language is available on the voicemail server. See Avaya IP Office Locale Settings. On a digital extension it also controls the display language used for messages from the system. Note however that some phones have their own menu options for the selected language for the phone menus.
Priority	Default = 5. Range = 1 (Lowest) to 5 (Highest) This setting is used by ARS.
System Phone Rights	Default = None Users set as a system phone user are able to access additional functions. The settings are: • **None**: The user cannot access any system phone options. • **Level 1**: The user can access all system phone options supported on the type of phone they are using except system management and memory card commands. • **Level 2**: The user can access all system phone options supported on the type of phone they are using including system management and memory card commands. Due to the nature of the additional commands a login code should be set for the user to restrict access.

Table continues…

Field	Description
Exclude From Directory	Default = Off When on, the user does not appear in the directory list shown by the user applications and on phones with a directory function. For users logging on as agents in an Outbound Contact Express deployment, **Exclude From Directory** must be **Off**.
Device Type	This field shows the type of phone at which the user is current logged in. • If the user is logged out but associated with a **Base Extension**, the device type for the extension port is shown. • If the user has logged out and is not associated with a **Base Extension**, the device type is listed as **Device Type Unknown**.

Profile Settings

Each user can be assigned to a particular profile. Each profile, other than **Basic User**, requires the system to have a matching license or subscription available for the user.

The profile assigned to the user controls whether they can have a number of additional settings enabled. The tables below list those settings and profiles. The items in ( ) brackets indicate the default status for the settings when that profile is selected.

IP500 V2 PLDS Licensed Systems

Option	Basic User	Office Worker	Teleworker	Mobile Worker	Power User
Enable Softphone	–	–	✓ *(On)*	–	✓ *(On)*
Enable one-X Portal Services	–	✓ *(On)*	✓ *(On)*	–	✓ *(On)*
Enable one-X Telecommuter	–	–	✓ *(On)*	–	✓ *(On)*
Enable Remote Worker [2]	✓ *(Off)*	✓ *(Off)*	✓ *(On)*	✓ *(Off)*	–
Enable Desktop/Tablet VoIP Client	–	✓[3] *(On)*	✓[3] *(On)*	–	✓ *(On)*
Enable Mobile VoIP Client	–	–	–	–	✓ *(On)*
Enable MS Teams Client	–	✓ *(On)*	✓ *(On)*	–	✓ *(On)*
Send Mobility Email	–	–	–	✓ *(Off)*	✓ *(Off)*
Web Collaboration • Not supported in IP Office R12.0 and higher.	–	✓ *(Off)*	✓ *(Off)*	–	✓ *(Off)*

Server Edition PLDS Licensed Systems

Option	Basic User	Office Worker	Power User
Enable Softphone	–	–	✓ *(On)*
Enable one-X Portal Services	–	✓ *(On)*	✓ *(On)*
Enable one-X Telecommuter	–	–	✓ *(On)*

Table continues…

Option	Basic User	Office Worker	Power User
Enable Remote Worker [2]	✓ *(Off)*	✓ *(Off)*	✓ *(On)*
Enable Desktop/Tablet VoIP Client	✓[3] *(Off)*	✓ *(On)*	✓ *(On)*
Enable Mobile VoIP Client	–	–	✓ *(On)*
Enable MS Teams Client	–	–	✓ *(On)*
Send Mobility Email	–	–	✓ *(Off)*
Web Collaboration • Not supported in IP Office R12.0 and higher.	–	✓ *(Off)*	✓ *(Off)*

Subscription Mode Systems

Option	Telephony User	Telephony Plus User	UC User
Enable Softphone	–	✓ *(On)*	✓ *(On)*
Enable one-X Portal Services	–	–	✓ *(On)*
Enable one-X Telecommuter	–	–	✓ *(On)*
Enable Remote Worker [2]	✓ *(Off)*	✓ *(Off)*	✓ *(On)*
Enable Desktop/Tablet VoIP Client	–	✓[3] *(Off)*	✓ *(On)*
Enable Mobile VoIP Client	–	–	✓ *(On)*
Enable MS Teams Client	–	–	✓ *(On)*
Send Mobility Email	–	–	✓ *(Off)*
Web Collaboration • Not supported in IP Office R12.0 and higher.	–	–	✓ *(On)*

User Profile Notes:

1. Non-licensed users can be created on both Standard Mode and Server Edition systems.
2. The system supports users using remote H.323 or SIP extensions. On non-Server Edition systems, up to 4 users are supported as remote extensions without needing to be configured and licensed for a user profile. Additional remote users are supported if licensed and configured for either a **Teleworker** or **Power User** user profile. On Server Edition systems, the remote worker is supported for all user profiles.
3. Supports the Avaya Workplace Client in standalone mode only. Simultaneous mode, shared call control mode, and presence are not available and supports local contacts only (not enterprise or IP Office contacts). See the IP Office Avaya Workplace Client Installation Notes manual.
   - On PLDS licensed IP500 V2 systems, Avaya Workplace Client can be used with a **Basic User** with **IP Softphone** license or a **Mobile Worker** with **IP Softphone** license.

Field	Description
Profile	Default = Basic User. A user's profile controls whether they can be configured for a number of features. The different profiles available and the features accessible by each are shown in the tables above. The number of users that can be configured for each profile is controlled by the user licenses or subscription that the system has. • A **Non-licensed User** is allowed dial-in access, can be paged, and can be used as a Music on Hold or Analog paging port. • For non-subscription IP500 V2 systems, a **Preferred Edition** system license is a pre-requisite for any user profile licenses. - In a multi-site network, the **Preferred Edition** license of the central system is automatically shared with other systems in the network, enabling user profile licenses on all IP500 V2 systems. - Each IP500 V2 system supporting a Voicemail Pro server still requires a **Preferred Edition** license for Voicemail Pro operation. • To upgrade an **Office Worker** or **Mobile Worker** to a **Power User**, you must first set the user to **Basic User**. • For an IP500 V2 system configured as an Avaya Aura X for Avaya Cloud Office (ACO) gateway, select the profile **ACO User**. Refer to the Deploying IP Office as an Avaya Aura X for Avaya Cloud Office (ACO) ATA Gateway.
Receptionist	Default = Off. This settings allows the user to use the SoftConsole application. This requires the configuration to have **Receptionist** licenses or subscriptions. • In PLDS licensed systems, a **Receptionist** license is only consumed when a configured user runs the SoftConsole application. • In subscription systems, a **Receptionist** subscription is consumed when a user is configured for SoftConsole use. • Up to 4 users can be licensed for IP500 V2 systems, 10 for Server Edition systems. • The use of SoftConsole is not supported for user's who then hot-desk to other systems in a the multi-site network.
Enable Softphone	Default = Controlled by the user profile, see the tables above. If selected, the user is able to use the IP Office Softphone application.
Enable one-X Portal Services	Default = Controlled by the user profile, see the tables above. If selected, the user is able to use the one-X Portal application, either directly or using one of its plug-in clients.
Enable one-X Telecommuter	Default = Controlled by the user profile, see the tables above. If selected, the user is able to use the telecommuter mode features of the one-X Portal application. Requires **Enable one-X Portal Services** to also be enabled.

Table continues…

Field	Description
Enable Remote Worker	Default = Off Indicates whether the user is allowed to use a remote H.323 or SIP extension. That is, an extension on a different IP network from the extensions registered IP Office system. • **SIP** – This option is not required for SIP extension users phones if an Avaya Session Border Controller for Enterprise (ASBCE) is deployed in the network. • **H323** – If the user's **Extension Number** matches the **Base Extension** setting of an IP extension, the **H.323 Remote Extn Enable** setting of that extension is automatically changed to match the user's **Enable Remote Worker** setting and vice versa. • Up to 4 **Basic User** users can be configured for **Enable Remote Worker**. Other users require licensing to a profile that supports the **Enable Remote Worker** setting.
Enable Desktop/ Tablet VoIP Client	Default = Controlled by the user profile, see the tables above. This option allows users to use Avaya Workplace Client on Windows or macOS operating systems.
Enable Mobile VoIP Client	Default = Controlled by the user profile, see the tables above. This option allows the users to use Avaya Workplace Client on Android and iOS operating systems.
Enable MS Teams Client	Default = Off This option enables IP Office to fetch the Microsoft Teams user data. The system is configured as the telephony service for calls made to and from Microsoft Teams.
Send Mobility Email	Default = Controlled by the user profile, see the tables above. When enabled, the user receives a welcome email with the following information: • A brief introduction of one-X Mobile Preferred for IP Office. • Instructions and links for installing and configuring the one-X Mobile Preferred for IP Office client.
Web Collaboration	Default = Controlled by the user profile, see the tables above. When enabled, allows the user to use the Web Collaboration application. • Not supported in IP Office R12.0 and higher. • In addition to the user profile license, each user requires a **Web Collaboration** license. • Web Collaboration requires Avaya one-X Portal on a Linux–based IP Office server other than a Unified Communications Module.

Hunt Group Membership

This drop-down allows you to quickly select the hunt groups to which the user belongs.

User Rights

Selected user settings can be overridden by those set within a set of User Rights. The same user rights can be applied to multiple users.

In addition, a time profile can be used to control when the user rights are applied to the user, and whether at other times, a different set of user rights are applied or the user's own settings.

Field	Description
User Rights View	This field affects Manager only. It allows you to switch between displaying the user settings as affected by their associated **Working Hours User Rights** or **Out of Hours User Rights**.
Working Hours Time Profile	Default = <None> (Continuous). If set, the selected time profile defines when the user's **Working Hours User Rights** are applied. Outside the time profile, the user's **Out of Hours User Rights** are applied
Working Hours User Rights	Default = Blank (No rights restrictions). This field allows selection of user rights which may set and lock some user settings. If a **Working Hours Time Profile** has been selected, the **Working Hours User Rights** are only applied during the times defined by that time profile, otherwise they are applied at all times.
Out of Hours User Rights	Default = Blank (No rights restrictions). This field allows selection of alternate user rights that are used outside the times defined by the user's Working Hours Time Profile.

Related links

Users on page 157

Voicemail

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Voicemail**

Additional configuration information

The **Enable Gmail API** setting is used to configure Gmail Integration.

For additional information, see Configuring Gmail Integration on page 833.

Configuration settings

If a voicemail server application is being used on your system, each user has use of a voicemail mailbox. You can use this form to enable this facility and various user voicemail settings.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Voicemail Code	Default = Blank. Range = 0 (no code) to 31 digits. A code used by the voicemail server to validate access to this mailbox. If remote access is attempted to a mailbox that has no voicemail code set, the prompt "Remote access is not configured on this mailbox" is played. The mailbox access code can be set through IP Office Manager or through the mailbox telephone user interface (TUI). The minimum password length is: • Voicemail Pro (Manager): 0 • Voicemail Pro (Intuity TUI): 2 • Embedded Voicemail (Manager): 0 • Embedded Voicemail (Intuity TUI): 0 Codes set through the Voicemail Pro telephone user interface are restricted to valid sequences. For example, attempting to enter a code that matches the mailbox extension, repeat the same number (111111) or a sequence of numbers (123456) are not allowed. If these types of code are required they can be entered through Manager. Manager does not enforce any password requirements for the code if one is set through Manager. • **Embedded Voicemail**: For Embedded Voicemail running in IP Office mailbox mode, the voicemail code is used if set. • **IP Office mode**: The voicemail code is required when accessing the mailbox from a location that is not set as a trusted number in the user's Source Numbers list. • **Intuity Emulation mode**: By default the voicemail code is required for all mailbox access. The first time the mailbox is accessed the user will be prompted to change the password. Also if the voicemail code setting is left blank, the caller will be prompted to set a code when they next access the mailbox. The requirement to enter the voicemail code can be removed by adding a customized user or default collect call flow, refer to the Voicemail Pro manuals for full details. • **Trusted Source Access**: The voicemail code is required when accessing the mailbox from a location that is not set as a trusted number in the user's Source Numbers list. • **Call Flow Password Request**: Voicemail Pro call flows containing an action where the action's PIN code set to **$** will prompt the user for their voicemail code. • **Changing the Code**: All of the voicemail interfaces, except IMS and IMAP, provide options for the user to change the voicemail code themselves. In addition, Voicemail Pro running in Intuity emulation mode will request that the user sets a code when they first log in to their mailbox using the phone.

Table continues…

Field	Description
Voicemail On	Default = On. When on, the mailbox is used by the system to answer the user's unanswered calls or calls when the user's extension returns busy. Note that selecting off does not disable use of the user's mailbox. Messages can still be forward to their mailbox and recordings can be placed in it. The mailbox can also still be accessed to collect messages. When a caller is directed to voicemail to leave a message, the system indicates the target user or hunt group mailbox. • The mailbox of the originally targeted user or hunt group is used. This applies even if the call has been forwarded to another destination. It also includes scenarios where a hunt group call overflows or is in fallback to another group. • Voicemail Pro can be used to customize which mailbox is used separately from the mailbox indicated by the system.
Voicemail Help	Default = Off This option controls whether users retrieving messages are automatically given an additional prompt "For help at any time press 8." If switched off, users can still press 8 for help. For voicemail systems running in Intuity emulation mode, this option has no effect. On those systems the default access greeting always includes the prompt "For help at any time, press *4" (*H in the US locale).
Voicemail Ringback	Default = Off When enabled and a new message has been received, the voicemail server calls the user's extension to attempt to deliver the message each time the telephone is put down. Voicemail will not ring the extension more than once every 30 seconds.
Voicemail Email Reading	Default = Off This option can be enabled for users whose Profile is set to **Mobile Worker** or **Power User**. If enabled, when you log into you voicemail box, it will detect your email messages and read them to you. This email text to speech feature is set-up through Voicemail Pro. This option is not currently supported with Linux based Voicemail Pro.
UMS Web Services	Default = On When selected, the user can use any of the Voicemail Pro UMS services to access their voicemail messages (IMAP email client, web browser or Exchange 2007 mailbox). Note that the user must have a voicemail code set in order to use the UMS services. • For subscription systems, this setting is only supported for **UC User**. • For PLDS licensed systems, this setting is only supported for **Teleworker**, **Office Worker** or **Power User** users.

Table continues…

Field	Description
Enable Gmail API	Default = Off. This setting is only supported on Server Edition systems and requires the used to have **UMS Web Services** enabled. When enabled: • The **Voicemail Email** setting is disabled. • The **Voicemail Email Mode** options (**Off**, **Copy**, **Forward**, **Alert**) are available. This feature uses the Gmail address defined in the setting **Call Management** > **Users** > **Add/Edit Users** > **User** > **Unique Identity**.
Voicemail Email	Default = Blank (No voicemail email features) This field is used to set the user or group email address used by the voicemail server for voicemail email operation. When an address is entered, the additional Voicemail Email control below are selectable to configure the type of voicemail email service that should be provided. Use of voicemail email requires the Voicemail Pro server to have been configured to use either a local MAPI email client or an SMTP email server account. For Embedded Voicemail, voicemail email is supported and uses the system's SMTP settings. The use of voicemail email for the sending (automatic or manual) of email messages with wav files attached should be considered with care. A one-minute message creates a 1MB .wav file. Many email systems impose limits on emails and email attachment sizes. For example the default limit on an Exchange server is 5MB. **Note:** Unicode characters are not supported.

Table continues…

Field	Description
Voicemail Email Mode	Default = Off This option is selectable when for users and groups when either: • A **Voicemail Email** email address is set. • The **Enable Gmail API** is set to **On**. These settings control the mode of automatic voicemail email operation provided by the voicemail server whenever the voicemail mailbox receives a new voicemail message. Users can change their voicemail email mode using visual voice. The ability to change the voicemail email mode can also be provided by Voicemail Pro in a call flow using a Play Configuration Menu action or a Generic action. If the voicemail server is set to IP Office mode • Users can change their voicemail email mode through the telephone prompts. • users can manually forward a message to email. The options are: • **Off** If off, none of the options below are used for automatic voicemail email. Users can also select this mode by dialing *03 from their extension. • **Copy** If this mode is selected, each time a new voicemail message is received in the voicemail mailbox, a copy of the message is attached to an email and sent to the email address. There is no mailbox synchronization between the email and voicemail mailboxes. For example reading and deletion of the email message does not affect the message in the voicemail mailbox or the message waiting indication provided for that new message. • **Forward** If this mode is selected, each time a new voicemail message is received in the voicemail mailbox, that message is attached to an email and sent to the email address. No copy of the voicemail message is retained in the voicemail mailbox and their is no message waiting indication. As with Copy, there is no mailbox synchronization between the email and voicemail mailboxes. Users can also select this mode by dialing *01 from their extension. Note that until email forwarding is completed, the message is present in the voicemail server mailbox and so may trigger features such as message waiting indication. • **UMS Exchange 2007** With Voicemail Pro, the system supports voicemail email to an Exchange 2007 server email account. For users and groups also enabled for UMS Web Services this significantly changes their mailbox operation. The Exchange Server inbox is used as their voicemail message store and features such as message waiting indication are set by new messages in that location rather than the voicemail mailbox on the voicemail server. Telephone access to voicemail messages, including Visual Voice access, is redirected to the Exchange 2007 mailbox. • **Alert** If this mode is selected, each time a new voicemail message is received in the voicemail mailbox, a simple email message is sent to the email address. This is an email message announcing details of the voicemail message but with no copy of the voicemail message attached. Users can also select this mode by dialing ***02** from their extension.

Table continues…

Field	Description
DTMF Breakout When a caller is directed to voicemail to leave a message, they can be given the option to be transferred to a different extension. The greeting message needs to be recorded telling the caller the options available. The extension numbers that they can be transferred to are entered in the fields below.System default values can be set for these numbers and are used unless a different number is set within these user settings. The values can be set using User Rights. The Park & Page feature is supported when the system voicemail type is configured as **Embedded Voicemail** or **Voicemail Pro**. Park & Page is also supported on systems where Avaya Aura Messaging, Modular Messaging over SIP, or CallPilot (for Enterprise Branch with CS 1000 deployments) is configured as the central voice mail system and the local Embedded Voicemail or Voicemail Pro provides auto attendant operation. The Park & Page feature allows a call to be parked while a page is made to a hunt group or extension. This feature can be configured for Breakout DTMF 0, Breakout DTMF 2, or Breakout DTMF 3.	
Reception/ Breakout (DTMF 0)	The number to which a caller is transferred if they press `0`while listening to the mailbox greeting rather than leaving a message (***0** on Embedded Voicemail in IP Office mode). For voicemail systems set to Intuity emulation mode, the mailbox owner can also access this option when collecting their messages by dialing ***0**. If the mailbox has been reached through a Voicemail Pro call flow containing a **Leave Mail** action, the option provided when **0** is pressed are: • For IP Office mode, the call follows the **Leave Mail** action's **Failure** or **Success** results connections depending on whether the caller pressed **0** before or after the record tone. • For Intuity mode, pressing **0** always follows the **Reception/Breakout (DTMF 0)** setting. When Park & Page is selected for a DTFM breakout, the following drop-down boxes appear: • **Paging Number –** displays a list of hunt groups and users (extensions). Select a hunt group or extension to configure this option. • **Retries –** the range is 0 to 5. The default setting is 0. • **Retry Timeout –** provided in the format M:SS (minute:seconds). The range can be set in 15-second increments. The minimum setting is 15 seconds and the maximum setting is 5 minutes. The default setting is 15 seconds
Breakout (DTMF 2)	The number to which a caller is transferred if they press `2`while listening to the mailbox greeting rather than leaving a message (***2** on Embedded Voicemail in IP Office mode).
Breakout (DTMF 3)	The number to which a caller is transferred if they press `3`while listening to the mailbox greeting rather than leaving a message (***3** on Embedded Voicemail in IP Office mode).

Related links

Users on page 157

Button Programming

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Button Programming**

Additional configuration information

For additional information on programming button actions, see Button Programming Overview on page 1082.

Configuration settings

Used to assign functions to the programmable keys provided on many Avaya telephones. For full details of button programming refer to the section Button Programming.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Button No.	The number of the DSS key against which the function is being set. To set a function against a button double-click it or select it and then click **Edit**.
Label	This is a text label for display on the phone. If no label is entered, the default label for the selected action is used.
Action	Defines the action taken by the menu item.
Action Data	This is a parameter used by the selected action. The options here will vary according to the selected button action.

Related links

Users on page 157

Telephony

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Telephony**

This page allows you to set telephony related features for the user. These override any matching setting in the Manager System | Telephony tab. The settings are grouped into a number of sub-tabs.

Related links

Users on page 157
Telephony Call Settings on page 175
Supervisor Settings on page 178
Multiline Options on page 181
Telephony Call Log on page 183
Telephony TUI on page 184

Telephony Call Settings

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Settings**

Additional configuration information

For additional information on ring tones, see Ring Tones on page 775.

Configuration settings

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Outside Call Sequence	Default = Default Ring (Use system setting) Applies only to analog phones. Sets the ring pattern used for external calls to the user. The distinctive ring patterns used for other phones are fixed. Note that changing the pattern for users associated with fax and modem device extensions can cause those devices to not recognize and answer calls.
Inside Call Sequence	Default = Default Ring (Use system setting) Applies only to analog phones. Sets the ring pattern used for internal calls to the user. The distinctive ring patterns used for other phones are fixed.
Ring Back Sequence	Default = Default Ring (Use system setting) Applies only to analog phones. Sets the ring pattern used for ringback calls to the user. The distinctive ring patterns used for other phones are fixed.
No Answer Time	Default = Blank (Use system setting). Range = 6 to 99999 seconds. Sets how long a call rings the user before following forwarded on no answer if set or going to voicemail. Leave blank to use the system default setting (**System** > **Telephony** > **Telephony** > **Default No Answer Time**). • For users who are using Avaya Workplace Client on iOS devices, it is recommended to set the time to at least 20 seconds.
Wrap-up Time (secs)	Default = 2 seconds, Range 0 to 99999 seconds. Specifies the amount of time after ending one call during which the user is treated as still being busy. During this time: • Other phones or applications monitoring the user's status indicate the user as still being busy (on a call). • Hunt group calls are not presented to the user. • If the user is using a single line set, direct calls also receive busy treatment. If the user is using a mutli-line set (multiple call appearances), direct calls to them will ring as normal. • It is recommended that this option is not set to less than the default of 2 seconds. 0 is used to allow immediate ringing. • The user's wrap-up time setting is added to the system hold recall time for calls put on hold by the user.

Table continues…

Field	Description
Transfer Return Time (secs)	Default = Blank (Off), Range 1 to 99999 seconds. Sets the delay after which any call transferred by the user, which remains unanswered, should return to the user. A return call will continue ringing and does not follow any forwards or go to voicemail. • Transfer return will occur if the user has an available call appearance button. • Transfer return is not applied if the transfer is to a hunt group that has queuing enabled.
Call Cost Mark-Up	Default = 100. This setting is used for ISDN advice of charge (AOC). The markup is applied to the cost calculations based on the number of units and the line base cost per charging unit. The field is in units of 1/100th, for example an entry of 100 is a markup factor of 1. This value is included in the system SMDR output.
Advertize Callee State To Internal Callers	Default = System Default (Off). The options are: • **System Default (Off)**. The system setting is **System Settings** > **System** > **Telephony** > **Advertize Callee State To Internal Callers**. • **On** • **Off** When enabled, for internal calls, additional status information is communicated to the calling party. Not supported for SIP endpoints except the J100 Series (excluding the J129). • When calling another internal phone and the called phone is set to Do Not Disturb or on another call, the calling phone displays “Do Not Disturb” or “On Another Call” rather than “Number Busy”. • On 9500 Series, 9600 Series and J100 Series phones, if a line appearance is programmed on a button on phone A and that line is in use on phone B, then phone A displays the name of the current user of the line along with the line number. • If a line appearance on a phone is in use elsewhere in the system and another extension unsuccessfully attempts to seize that line, the phone displays “In Use:<name>” where <name> is the name of the user currently using the line.
Call Waiting On	Default = Off For users on phones without appearance buttons, if the user is on a call and a second call arrives for them, an audio tone can be given in the speech path to indicate a waiting call (the call waiting tone varies according to locale). The waiting caller hears ringing rather than receiving busy. There can only be one waiting call, any further calls receive normal busy treatment. If the call waiting is not answered within the no answer time, it follows forward on no answer or goes to voicemail as appropriate. User call waiting is not used for users on phones with multiple call appearance buttons.

Table continues…

Field	Description
Answer Call Waiting on Hold	Default = On Applies to analog and IP DECT extension users only. If the user has a call waiting and places their current call on hold, the waiting call is automatically connected.
Busy on Held	Default = Off for users with call appearance buttons/On for other users. If on, when the user has a call on hold, new calls receive busy treatment. They will follow the user's forward on busy setting or are diverted to voicemail. Otherwise busy tone (ringing for incoming analog calls) is played. This overrides call waiting when the user has a call on hold. The use of **Busy on Held** for users with multiple call appearance buttons is deprecated and Manager will prompt whether it should switch off the feature off for such a user.
Offhook Station	Default = Off Off-hook station allows an analog extension to be left permanently off-hook, with calls being made and answered using an application or TAPI. When enabled, the analog extension user is able to control calls using the application in the following ways: Offhook station does not disable the physical off-hook on the phone. When starting with the phone on-hook, making and answering calls is the same as normal analog extension operation. Additionally however calls can be initiated from the application. After entering the required number and making the call, the on-hook analog extension receives a ringback showing the users own caller ID and when answered the outgoing call leg to the dialed number is started. Calls to a busy destination present busy tone before being cleared. The application can be used to end a call with the analog extension still off-hook. Instead of hearing disconnect tone the user hears silence and can use the application to make another call. Though off-hook the user is indicated as idle on BLF indicators. Without off-hook Station set the user would be indicated as busy when off-hook, whether on a call or not. If off-hook and idle (having cleared a previous call), incoming call alerts by presenting ringing through the audio path. The call can be answered using the application or going on-hook/off-hook or by pressing recall. Note that if the phone normally displays call ID, any caller ID displayed on the phone is not updated in this mode, however the call ID in the application will be that of the current call. If on-hook, an incoming call alerts as normal using the phone's ringer and is answered by going off-hook. The answer call option in the application cannot be used to answer calls to an on-hook analog extension. While off-hook and idle, the analog extension user will receive page calls. If the analog extension handset is replaced with a headset, changing the Manager setting **Extension | Analog | Equipment Classification** to **Quiet Handset** is recommended.

Related links

[Telephony](#) on page 174

Supervisor Settings

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Supervisor Settings**

Additional configuration information

- For additional information on the **Force Authorization Code** setting, see Configuring Authorization Codes on page 823.
- For additional information on the **Inhibit Off-Switch Forward/Transfers** setting see, Off-Switch Transfer Restrictions on page 902.

Configuration settings

These settings relate to user features normally only adjusted by the user's supervisor.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Login Code	Default = Blank. Range = Up to 31 digits. • Login code must be at least 4 digits for DS port users. • Login codes of up to 15 digits are supported with **Extn Login** buttons. • Login codes of up to 31 digits are supported with **Extn Login** short codes. This code is used for logging in on a phone (and for restricting access to features on phones. See Hot Desking on page 876. • Hot desking is not supported for centralized users. Centralized users use the **Login Code** for SIP registration on Session Manager. • Normally users can only log out if they have a **Login Code** set or if they are currently logged in at an extension whose **Base Extension** number no longer matches their own **Extension** setting. • When set, the short code feature **Change Login Code** can be used by users to change their login code. • If the user has a login code set, it is used by the **Outgoing Call Bar Off** short code feature. • If the user has a login code set, access to a range of programmable button features requires entry of the login code. For example, access **Self Admin** and **System Phone** features.
Login Idle Period (secs)	Default = Blank (Off). Range = 0 (Off) to 99999. If the telephone is not used for this period; the user currently logged in is automatically logged out. This option should be used only in conjunction with Force Login (see below).
Monitor Group	Default = <None> Sets the hunt group whose members the user can monitor if silent monitoring is setup. See the Call Listen short code.

Table continues…

Field	Description
Privacy Override Group	Default = <None> The drop-down menu lists the local and network advertised hunt groups. If selected, calls to this user cannot be seen or picked up by other users unless they are a member of the selected group.
Coverage Group	Default = <None>. If a group is selected, then in scenarios where an external call would normally have gone to voicemail, it instead continues ringing and also starts alerting the members of the coverage group. See Coverage Groups on page 893.
Status on No Answer	Default = Logged On. Hunt groups can change the status of call center agents (users with a log in code and set to forced log in) who do not answer a hunt group call presented to them before it is automatically presented to the next agent. Use of this is controlled by the **Agent's Status on No Answer Applies To** setting of the hunt group. This option is not used for calls ringing the agent because the agent is in another group's overflow group. The options are: • **Logged On**: If this option is selected, the user's status is not changed. • **Busy Wrap-Up**: If this option is selected the user's membership status of the hunt group triggering the action is changed to disabled. The user can still make and receive calls and will still continue to receive calls from other hunt groups to which they belong. • **Busy Not Available**: If this option is selected the user's status is changed to do not disturb. This is the equivalent of DND and will affect all calls to the user. • **Logged Off**: If this option is selected the users status is changed to logged out. In that state they cannot make calls or receive calls. Hunt group calls go to the next available agent and personal calls treat the user as being busy.
Reset Longest Idle Time	Default = All Calls. This setting is used in conjunction with hunt groups set to Longest Waiting (also known as Idle and Longest Waiting). It defines what type of calls reset the idle time of users who are members of these hunt groups. Options are **All Calls** and **External Incoming**.
Force Login	Default = Off If checked, the user must log in using their **Login Code** to use any extension including an extension to which they are the default associated user (**Base Extension**). For example: If user B has logged onto user A's phone and now logs off • If user A has **Force Login** enabled, they are not automatically logged back on to their extension. • If user A do not have **Force Login** enabled, they are automatically logged back in.
Force Account Code	Default = Off If checked, the user must enter a valid account code to make an external call.

Table continues…

Field	Description
Force Authorization Code	Default = Off. If checked, the user must enter a valid authorization code to make an external call. That authorization code must be one associated with the user or the user rights to which the user belongs.
Incoming Call Bar	Default = Off When enabled, this setting stops a user from receiving any external calls. On the calling phone, the call is rejected.
Outgoing Call Bar	Default = Off When enabled, this setting stops a user from making any external calls except those that use dial emergency features. On many Avaya display phones, this causes a **B** to be displayed. The following features can be used with outgoing call bar: Outgoing Call Bar On, Outgoing Call Bar Off and Change Login Code.
Inhibit Off-Switch Forward/Transfers	Default = Off. When enabled, this setting stops the user from transferring or forwarding calls externally. This does not stop another user transferring the restricted users calls off-switch on their behalf. Note that a number of other controls may inhibit the transfer operation.
Can Intrude	Default = Off If enabled, the user can perform is allowed to perform a range of action on other user's calls. For example: **Call Intrude**, **Call Listen**, **Call Steal** and **Dial Inclusion**. See Call Intrusion on page 834. • Use of the features is subject to the **Cannot Be Intruded** setting of the target.
Cannot be Intruded	Default = On If checked, this user's calls cannot be interrupted or acquired by users who have **Can Intrude** enabled. This setting also affects whether other users can use their appearance buttons to bridge into a call to which this user has been the longest present user.
Can Trace Calls	Default = Off. This settings controls whether the user is able to make used of ISDN MCID controls.
Can Control After Call Work	Default = Off. If enabled, the agent can extend the currently active After Call Work time indefinitely.
After Call Work Time (Sec)	Default = The value in this field is populated from the **Default After Call Work Time** field located at **System | Contact Center**. The time after a call when an agent is busy and unable to deal with hunt group calls. Change the value if you want to specify ACW time for this user to be different from the system default.
Can Accept Collect Calls	Default = Off [Brazil Only] Determines whether the user is able to receive and accept collect calls.
Deny Auto Intercom Calls	Default = Off. When enabled, any automatic intercom calls to the user's extension are automatically turned into normal calls.

Related links

Telephony on page 174

Multiline Options

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Multi-line Options**

Additional configuration information

- For additional configuration information, see Appearance Button Operation on page 1198.
- For the **Reserve Last CA** setting, 1400, 1600, 9500 and 9600 Series telephone users can put a call on hold pending transfer if they already have held calls even if they have no free call appearance button available. For additional information, see Context Sensitive Transfer on page 903.

Configuration settings

Multi-line options are applied to a user's phone when the user is using an Avaya phones which supports appearance buttons (call appearance, line appearance, bridged and call coverage).

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Individual Coverage Time (secs)	Default = 10 seconds, Range 1 to 99999 seconds. This function sets how long the phone will ring at your extension before also alerting at any call coverage users. This time setting should not be equal to or greater than the **No Answer Time** applicable for the user.
Ring Delay	Default = Blank (Use system setting). Range = 0 (use system setting) to 98 seconds. This setting is used when any of the user's programmed appearance buttons is set to Delayed ringing. Calls received on that button will initially only alert visually. Audible alerting will only occur after the ring delay has expired.

Table continues…

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Coverage Ring</td><td>Default = Ring.

This field selects the type of ringing that should be used for calls alerting on any the user's call coverage and bridged appearance buttons. Ring selects normal ringing. Abbreviated Ring selects a single non-repeated ring. No Ring disables audible ringing. Note that each button's own ring settings (Immediate, Delayed Ring or No Ring) are still applied.

The ring used for a call alerting on a call coverage or bridged appearance button will vary according to whether the user is currently connected to a call or not.

• If not currently on a call, the Coverage Ring setting is used.
• If currently on a call, the quieter of the Coverage Ring and Attention Ring settings is used.

<table>
<tr><th rowspan="2">Attention Ring Setting</th><th colspan="3">Coverage Ring Setting</th></tr>
<tr><th>Ring</th><th>Abbreviated</th><th>Off</th></tr>
<tr><td>Ring</td><td>Ring</td><td>Abbreviated</td><td>Off</td></tr>
<tr><td>Abbreviated</td><td>Abbreviated</td><td>Abbreviated</td><td>Off</td></tr>
</table>
</td></tr>
<tr><td>Attention Ring</td><td>Default = Abbreviated Ring.

This field selects the type of ringing that should be used for calls alerting on appearance buttons when the user already has a connected call on one of their appearance buttons.

• Ring selects normal ringing.
• Abbreviated Ring selects a single ring.
• Note that each buttons own ring settings (Immediate, Delayed Ring or No Ring) are still applied.</td></tr>
<tr><td>Ringing Line Preference</td><td>Default = On.

For users with multiple appearance buttons. When the user is free and has several calls alerting, ringing line preference assigns currently selected button status to the appearance button of the longest waiting call. Ringing Line Preference overrides Idle Line Preference.</td></tr>
<tr><td>Idle Line Preference</td><td>Default = On.

For users with multiple appearance buttons. When the user is free and has no alerting calls, idle line preference assigns the currently selected button status to the first available appearance button.</td></tr>
<tr><td>Delayed Ring Preference</td><td>Default = Off.

This setting is used in conjunction with appearance buttons set to delayed or no ring. It sets whether ringing line preference should use or ignore the delayed ring settings applied to the user's appearance buttons.

• When on, ringing line preference is only applied to alerting buttons on which the ring delay has expired.
• When off, ringing line preference can be applied to an alerting button even if it has delayed ring applied.</td></tr>
</table>

Table continues…

Field	Description
Answer Pre-Select	Default = Off. Normally when a user has multiple alerting calls, only the details and functions for the call on currently selected button are shown. Pressing any of the alerting buttons will answer the call on that button, going off-hook will answer the currently selected button. Enabling **Answer Pre-Select** allows the user to press any alerting button to make it the current selected button and displaying its call details without answering that call until the user either presses that button again or goes off-hook. Note that when both **Answer Pre-Select** and **Ringing Line Preference** are enabled, once current selected status is assigned to a button through ringing line preference, it is not automatically moved to any other button.
Reserve Last CA	Default = Off. When selected, this option stops the user's last call appearance button from being used to receive incoming calls. This ensures that the user always has a call appearance button available to make an outgoing call and to initiate actions such as transfers and conferences. • 1400, 1600, 9500 and 9600 Series telephone users can put a call on hold pending transfer if they already have held calls even if they have no free call appearance button available.

Related links

Telephony on page 174

Telephony Call Log

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Log**

The IP Office stores a centralized call log for each user:

- The user's centralized call log is stored by the IP Office system on which the user is configured. If the user is logged in on another system, new call log records are sent to the user's home IP Office system, but using the time and date on the IP Office system where the user is logged in.
- Each user's centralized call log can contain 30 (IP500 V2) or 60 (Server Edition) call records. Each new call record replaces the oldest previous record when it reaches the limit.
- By default, the centralized call log is displayed on Avaya phones with a fixed **Call Log** or **History** button (1400, 1600, 9500, 9600, J100 Series) and in the one-X Portal, Avaya Workplace Client, and IP Office User Portal applications.
- The centralized call log moves with the user as they log onto different phones and IP Office applications.
- The missed call count is updated per unique caller, not per call.

These settings are using in conjunction with the system wide call log settings (**System** > **Telephony** > **Call Log**).

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Centralized Call Log	Default = System Default (On) This setting allows the use of centralized call logging to be enabled or disabled on a per user basis. The default is to match the system setting **System Settings** > **System** > **Telephony** > **Call Log** > **Default Centralized Call Log On**. The other options are **On** or **Off** for the individual user. If set to **Off**, the user receives the message “Call Log Disabled” when the Call Log button is pressed.
Delete records after (hours:minutes)	Default = 00:00 (Never). If a time period is set, records in the user's call log are automatically deleted after this period.
Groups	Default = System Default (On). This section contains a list of hunt groups on the system. If **System Settings** > **System** > **Telephony** > **Call Log** > **Log Missed Hunt Group Calls** is enabled, then the selected groups are shown as part of the users centralized call log. The missed hunt group calls are any missed calls for the whole hunt group, not just group calls presented to the user and not answered by them.

Related links

[Telephony](#) on page 174

Telephony TUI

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **TUI**

Used to configure system wide telephony user interface (TUI) options for 1400, 1600, 9500, 9600 and J100 Series phones (except the J129).

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Features Menu Controls	
User Setting	Default = Same as System When set to **Same as System**, matches the system-wide settings of the System | Telephony | TUI menu options. When set to **Custom**, uses the **Features Menu** settings below.

Table continues…

Field	Description
Features Menu	Default = On When set to off, TUI feature menus are not available. When set to on, you can select to turn individual feature menus off or on. The following feature menus are listed: • **Basic Call Functions:** If selected, users can access menu options for call pickup, park, unpark and transfer to mobile functions. • **Advanced Call Functions:** If selected, users can access the menu options for do not disturb, account code, withhold number and internal auto-answer functions. Note, the **Account Code** menu is only shown if the system has been configured with accounts codes. • **Forwarding**: If selected, users can access the phone's menus for forwarding and follow me functions. • **Hot Desk Functions:** If selected, users can access the menu options for logging in and out. • **Passcode Change:** If selected, users can change their login code (security credentials) through the phone menus.. • **Phone Lock:** If selected, users can access the menu options for locking the phone and for setting it to automatically lock. • **Self Administration:** If selected, users can access the phone's **Self-Administration** menu options. • **Voicemail Controls**: If set, users can access the **Visual Voice** option through the phone's **Features** menu.

Related links

Telephony on page 174

Short Codes

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Short Codes**

Additional configuration information

For additional configuration information on short codes, see Short Code Overview on page 973.

Configuration settings

Short codes entered in this list can only be dialed by the user. They will override any matching user rights or system short code.

User and User Rights short codes are only applied to numbers dialed by that user. For example they are not applied to calls forwarded via the user.

Warning:

User dialing of emergency numbers must not be blocked by the addition of short codes. If short codes are added, the users ability to dial emergency numbers must be tested and maintained.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Short codes can be added and edited using the **Add**, **Remove** and **Edit** buttons. Alternatively you can right-click on the list of existing short code to add and edit short codes.

Code	Description
`*FWD`	Short codes of this form are inserted by the system. They are used in conjunction with the **User | Forwarding** settings to remember previously used forwarding numbers. They can be accessed on that tab by using the drop-down selector on the forwarding fields.
`*DCP`	Short codes of this form are often inserted by the system. They are used by some phone types to contain settings relating to functions such as ring volume and auto answer. Deleting such short codes will cause related phone settings to return to their defaults.
`*DCP/Dial/ 8xxxxxxx,0,1,1,0/0`	For systems with TCM phone ports, when a phone is first connected to the port, the button programming of the associated user is overwritten with the default button programming appropriate for the phone model. Adding the above short code prevents that behavior if not required, for example if a pre-built configuration including user button programming is added to the system before the connection of phones.

Related links

Users on page 157

Forwarding

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Forwarding**

Use this page to check and adjust a user's call forwarding and follow me settings. For additional configuration information, see DND, Follow Me, and Forwarding on page 862.

Follow Me is intended for use when the user is present to answer calls but for some reason is working at another extension. For example; temporarily sitting at a colleague's desk or in another office or meeting room. As a user, you would use Follow Me instead of Hot-Desking if you do not have a log in code or you do not want to interrupt you colleague also receiving their own calls. Multiple users can use follow me to the same phone.

Forwarding is intended for use when, for some reason, the user is unable to answer a call. They may be busy on other calls, unavailable or simply do not answer. Calls may be forwarded to internal or, subject to the user's call barring controls, external numbers.

- **To bar a user from forwarding calls to an external number:** Select **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Supervisor Settings** > **Inhibit Off-Switch Forward/Transfers**.
- **To bar all users from forwarding calls to external numbers:** Select **System Settings** > **System** > **Telephony** > **Inhibit Off-Switch Forward/Transfers**.

Note that analog lines doe not provide call progress signalling. Therefore, calls forwarded off-switch via an analog line are treated as answered and are not recalled.

Once a call has been forwarded to an internal target, it will ignore the target's **Forward No Answer** or **Forward on Busy** settings but may use its **Forward Unconditional** settings unless they create a loop.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

General Settings

Field	Description
Block Forwarding	Default = Off. When enabled, call forwarding is blocked for this user. The following actions are blocked: Follow me, Forward unconditional, Forward on busy, Forward on no answer and Hot Desking.
Follow Me Number	Default = Blank. Range = Internal extension number. Redirects the user's calls to the internal extension number entered. If the redirected call receives busy or is not answered, it follows the user's forwarding and or voicemail settings as if it had been presented to their normal extension. When a user has follow me in use, their normal extension will give alternate dialtone when off hook. Using **Follow Me** overrides **Forward Unconditional**. Calls targeting longest waiting type hunt groups ignore Follow Me. Calls triggered by actions at the user's original extension, for example voicemail ringback, ignore Follow Me. Park, hold and transfer return calls will go to the extension at which the user initiated the park, hold or transfer action.

Forward Unconditional

Field	Description
Forward Unconditional	Default = Off This option, when checked and a **Forward Number** also set, forwards all external calls immediately. Additional options allow this forwarding to also be applied to internal calls and to hunt group calls if required. When a user has forward unconditional in use, their normal extension will give alternate dialtone when off hook. If the destination is an internal user on the same system, they are able to transfer calls back to the user, overriding the Forward Unconditional. After being forwarded for the user's no answer time, if still unanswered, the system can apply additional options. It does this if the user has forward on no answer set for the call type or if the user has voicemail enabled. • If the user has forward on no answer set for the call type, the call is recalled and then forwarded to the forward on no answer destination. • If the user has voicemail enabled, the call is redirected to voicemail. • If the user has both options set, the call is recalled and then forwarded to the forward on no answer destination for their no answer time and then if still unanswered, redirected to voicemail. • If the user has neither option set, the call remains redirected by the forward unconditional settings. Note that for calls redirected via external trunks, detecting if the call is still unanswered requires call progress indication. For example, analog lines do not provide call progress signalling and therefore calls forwarded via an analog lines are treated as answered and not recalled.
To Voicemail	Default = Off. If selected and forward unconditional is enabled, calls are forwarded to the user's voicemail mailbox. The **Forward Number** and **Forward Hunt Group Calls** settings are not used. This option is not available if the system's **Voicemail Type** is set to **None**. 1400, 1600, 9500 and 9600 Series phone users can select this setting through the phone menu. Note that if the user disables forward unconditional the **To Voicemail** setting is cleared.
Forward Number	Default = Blank. Range = Internal or External number. Up to 33 characters. This option sets the destination number to which calls are forwarded when **Forward Unconditional** is checked. The number can be an internal or external number. This option is also used for **Forward on Busy** and **Forward on No Answer** if no separate **Forward Number** is set for those features. If a user forwards a call to a hunt group of which they are a member, the group call is not presented to them but is presented to other members of the hunt group.

Table continues…

Field	Description
Forward Hunt Group Calls	Default = Off Hunt group calls (internal and external) are not normally presented to a user who has forward unconditional active. Instead they are presented to the next available member of the hunt group. This option, when checked, sets that hunt group calls (internal and external) are also forwarded when forward unconditional is active. The group's **Ring Type** must be **Sequential** or **Rotary**, not **Collective** or **Longest Waiting**. The call is forwarded for the period defined by the hunt group's **No Answer Time** after which it returns to the hunt group if unanswered. Note also that hunt group calls cannot be forwarded to another hunt group.
Forward Internal Calls	Default = On. This option, when checked, sets that internal calls should be also be forwarded immediately when forward unconditional is active.

Forward on Busy/No Answer

Field	Description
Forward On Busy	Default = Off When checked and a forward number is set, external calls are forwarded when the user's extension is busy. The number used is either the **Forward Number** set for **Forward Unconditional** or if set, the separate **Forward Number** set under **Forward On Busy**. Having **Forward Unconditional** active overrides **Forward on Busy**. If the user has **Busy on Held** selected, if forward on busy is active it is applied when the user is free to receive calls but already has a call on hold. If the user's phone has multiple call appearance buttons, the system will not treat them as busy until all the call appearance buttons are in use unless the last appearance button has been reserved for outgoing calls only.
Forward On No Answer	Default = Off When checked and a forward number is set, calls are forwarded when the user does not answer within their set No Answer Time (User | Telephony | Call Settings).
Forward Number	Default = Blank. Range = Internal or External number. Up to 33 characters. If set, this number is used as the destination for **Forward On Busy** and **Forward On No Answer** when on. If not set, the **Forward Number** set for **Forward Unconditional** is used. If a user forwards a call to a hunt group of which they are a member, the group call is not presented to them but is presented to other members of the hunt group.
Forward Internal Calls	Default = On. When checked, this option sets that internal calls should be also be forwarded when forward on no answer or forward on busy is active.

Related links

Users on page 157

Mobility

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Mobility**

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Configuration settings

Twinning allows the IP Office to present a user's calls to both their main phone and another extension or number. The IP Office system supports two modes of twinning:

	Internal	Mobile
Twinning Destination	Internal extensions on the same IP Office.	External numbers only.
Supported in	All locales.	All locales.
License Required	The primary phone user must be a licensed user.	Yes

Using both internal and mobile twinning

For IP Office R11.1.3 and higher, you can configure both **Internal Twinning** and **Mobile Twinning** for Avaya Workplace Client users:

- The Avaya Workplace Client users can switch between internal and mobile twinning using the client's **Incoming Call Features** menu.
- When the Avaya Workplace Client user selects mobile twinning, the internal twinning extension temporarily reverts to its original extension number. Therefore, Avaya recommend restricting the internal twin extension to internal calls when not twinned.

Simultaneous

These settings apply to the operation of simultaneous clients.

Field	Description
Coverage Delay (secs)	Default = 0 seconds. Range= minimum 0 seconds to maximum 15 seconds. Sets the delay between calls alerting on the user's main telephony device/client and then also alerting their MS Teams client.
MS Teams URI	The user's telephony URI for MS Teams. The maximum length of the URI is 161 characters. For more details, see the Deploying MS Teams Direct Routing with IP Office manual. This field is read-only if the **Auto Populate MS Teams Data** setting (**System** > **Telephony** > **MS Teams**) is enabled.

Internal Twinning

Select this option to enable internal twinning for a user. Internal twinning is not supported during resilience.

Field	Description
Twinned Handset	Default = Blank. This drop-down list is used to select twinned phone. Supported internal twining destinations must: • Be on the same IP Office system • Not be using simultaneous mode. • Be a physical deskphone or DECT extension. Softphones are not supported. If the list is grayed out, the user is a twinning destination and the main phone to which it is twinned is displayed. All **Call Management** > **Users** > **Add/Edit Users** > **Mobility** fields are grayed out for unlicensed users.
Maximum Number of Calls	Default = 1. Sets the number of calls the user can have internally twinned at the same time: • If set to one, when either the main or twinned phone are in use, any additional incoming call receives busy treatment. • If set to two, when either phone is in use, it receives call waiting indication for the second call. Any further calls above two receive busy treatment.
Twin Bridge Appearances	Default = Off. Set whether calls alerting on bridged appearance buttons on the main phone also alert on the twinned phone.
Twin Coverage Appearances	Default = Off. Set whether calls alerting on coverage appearance buttons on the main phone also alert on the twinned phone.
Twin Line Appearances	Default = Off. Set whether calls alerting on line appearance buttons on the main phone also alert on the twinned phone.

Mobility Features

If enabled, this option allows any of the mobility features to be enabled for the user.

Field	Description
Mobile Twinning	If selected, the user is enable for mobile twinning. The user can control this option through a **Twinning** programmable button on their a phone.
Fallback Twinning	Default = Disabled When enabled, if the user's main extension is unreachable, the IP Office redirects their calls to the **Twinned Mobile Number** even if **Mobile Twinning** is disabled. **Fallback Twinning** does not use the **Mobile Dial Delay**.

Table continues…

Field	Description
Twinned Mobile Number	Default = Blank. This field sets the external destination number for mobile twinned calls. • When used to make a call from the IP Office system, the number is subject to short code processing and must include any external dialing prefix necessary. • The IP Office also uses this number to control access to mobile call control and FNE functions. The IP Office allows access only if the caller ID matches the **Twinned Mobile Number** of an IP Office user. If matched, the user settings control operation of the mobile call control/FNE features.
Twinning Time Profile	Default = <None> (Any time) This field allows selection of a time profile during which mobile twinning is used.
Mobile Dial Delay	Default = 2 seconds This setting controls how long calls alert at the user's main extension before also alerting at the twinned number. You can use this setting at the user's request, however you may also need to use it in some scenarios. For example: • If the twinning number is a switched off mobile device, the mobile service provider may immediately answer the call using their voicemail service. That creates a scenario where the user's main extension does not ring or rings briefly.
Mobile Answer Guard	Default = 0 (Off). Range = 0 to 99 seconds. This control can be used in situations where calls sent to the twinned destination are automatically answered by a voicemail service or automatic message if the twinned device is not available. If a twinned call is answered before the **Mobile Answer Guard** expires, the system will drop the call to the twin.
Hunt group calls eligible for mobile twinning	Default = Off This setting controls whether hunt group calls ringing the user's primary extension should also be presented to the mobile twinning number.
Forwarded calls eligible for mobile twinning	Default = Off This setting controls whether calls forwarded to the user's primary extension should also be presented to the mobile twinning number.

Table continues…

Field	Description
Twin When Logged Out	Default = Off. If enabled, if the user logs off their main extension, calls to that extension will still alert at their twinned number rather than immediately going to voicemail or busy. When logged out but twinned: • **Mobile Dial Delay** is not applied. • Hunt group calls (all types) are twinned if **Hunt group calls eligible for mobile twinning** is enabled. The user's idle time is reset for each externally twinned call answered. Note the IP Office automatically treats calls twinned over analog and analog emulation trunks as answered. • When the user's **Mobile Time Profile** is not active, calls are treated the same as the user was logged out user with no twinning. • Callback calls initiated by the user will ring the twinned number. Other users can set automatic callback to the user. The twinned user's busy/free state is tracked for all calls through the IP Office system. • The user's bridged appearance buttons do not alert. Their coverage appearance buttons will continue to operate. • The BLF/user button status shown for the user is: - For calls alerting or in progress through the IP Office system to the twin, the user status shows alerting or in-use. The user shows as busy/in-use if they such a call on hold and they have **Busy on Held** enabled. - If the user enables DND through Mobile Call Control, their status shows as DND/busy. - Calls from the IP Office system dialed direct to the user's twinned destination rather than redirected by twinning do not change the user's status.
one-X Mobile Client	Default = Off. Not supported with R11.1 and higher.
Mobile Call Control	Default = Off. This feature allows a user receiving a call on their twinned device to access system dial tone and then perform dialing action including making calls and activating short codes. See Mobile Call Control on page 894.
Mobile Callback	Default = Off. Mobile callback allows the user to make calls from the twinned number using the IP Office to route the calls. See Mobile Call Control on page 894. When used: • The user calls the IP Office system and then hangs up. • The IP Office system calls the user's caller ID number. • When answered, the IP Office provide dial tone for the user to make a call.

Related links

Users on page 157

Group Membership

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Group Membership**

This tab displays the groups of which the user has been made a member.

Related links

Users on page 157

Voice Recording

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Voicemail Recording**

These settings are used to control manual and automatic recording of user's calls.

- Call recording requires Voicemail Pro to be installed and running. Call recording also requires available conference resources similar to a 3-way conference.
- Call recording starts when the call is answered.
- Call recording is paused when the call is parked or held. It restarts when the call is unparked or taken off hold. This does not apply to SIP terminals.
- Calls to and from IP devices, including those using Direct media, can be recorded.
- Recording continues for the duration of the call or up to the maximum recording time configured on the voicemail server.
- Recording is stopped when the call ends or if:
  - User call recording stops if the call is transferred to another user.
  - Account code call recording stops if the call is transferred to another user.
  - Hunt group call recording stops if the call is transferred to another user who is not a member of the hunt group.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Auto Recording

Field	Description
Inbound	Default = None. Select whether automatic recording of incoming calls is enabled as below The adjacent field sets whether **External**, **Internal**, or **External & Internal** calls are included. • **None**: Do not automatically record calls. • **On**: Record the call if possible. Otherwise, allow the call to continue without recording. • **Mandatory**: Record the call if possible. Otherwise, block the call and return busy tone. • **Percentages of calls**: Record a selected percentages of the calls.
Outbound	Default = None. Select whether automatic recording of outgoing calls is enabled. The options are the same as for incoming calls above.
Destination	Default = User's mailbox. Sets the destination for automatically triggered recordings. The options are: • **Mailbox** This option sets the destination for the recording to be a selected user or hunt group mailbox. The adjacent drop down list is used to select the mailbox. • **Voice Recording Library**: This option set the destination for the recording to be a VRL folder on the voicemail server. The VRL application polls that folder and collects waiting recordings which it then places in its archive. Recording is still done by Voicemail Pro. • **Voice Recording Library Authenticated**: This option is similar to the above but instructs the voicemail server to create an authenticated recording. If the file contents are changed, the file is invalidated though it can still be played. - For systems recording to `.opus` format (the default), both settings create authenticated recordings.
Time Profile	Default = None. (Any time). Used to select a time profile during which automatic call recording of incoming calls is applied. If no profile is selected, automatic recording is always active.

Manual Recording

Field	Description
Destination	Default = User's mailbox. Sets the destination for automatically triggered recordings. The options are: • **Mailbox** This option sets the destination for the recording to be a selected user or hunt group mailbox. The adjacent drop down list is used to select the mailbox. • **Voice Recording Library**: This option set the destination for the recording to be a VRL folder on the voicemail server. The VRL application polls that folder and collects waiting recordings which it then places in its archive. Recording is still done by Voicemail Pro. • **Voice Recording Library Authenticated**: This option is similar to the above but instructs the voicemail server to create an authenticated recording. If the file contents are changed, the file is invalidated though it can still be played. - For systems recording to `.opus` format (the default), both settings create authenticated recordings.

Related links

Users on page 157

Do Not Disturb

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Do Not Disturb**

Additional configuration information

For additional configuration information, see DND, Follow Me, and Forwarding on page 862.

See Do Not Disturb in the Telephone Features section for full details of Do Not Disturb operation.

Do not disturb prevents the user from receiving hunt group and page calls. Direct callers hear busy tone or are diverted to voicemail if available. It overrides any call forwarding, follow me and call coverage settings. A set of exception numbers can be added to list numbers from which the user still wants to be able to receive calls when they have do not disturb in use.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Do Not Disturb	Default = Off When checked the user's extension is considered busy, except for calls coming from sources listed in their Do Not Disturb Exception List. When a user has do not disturb in use, their normal extension will give alternate dialtone when off hook. Users with DND on are indicated as 'busy' on any BLF indicators set to that user.

Table continues…

Field	Description
Do Not Disturb Exception List	Default = Blank This is the list of telephone numbers that are still allowed through when Do Not Disturb is set. For example this could be an assistant or an expected phone call. Internal extension numbers or external telephone numbers can be entered. If you wish to add a range of numbers, you can either enter each number separately or make use of the wildcards "N" and "X" in the number. For example, to allow all numbers from 7325551000 to 7325551099, the DND Exception number can be entered as either 73255510XX or 73255510N. Note that this list is only applied to direct calls to the user. Calls to a hunt group of which the user is a member do not use the Do Not Disturb Exceptions list.

Related links

Users on page 157

Announcements

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Announcements**

Announcements are played to callers waiting to be answered. This includes callers being presented to hunt group members, ie. ringing, and callers queued for presentation.

- The system supports announcements using Voicemail Pro or Embedded Voicemail.
- If no voicemail channel is available for an announcement, the announcement is not played.
- In conjunction with Voicemail Pro, the system allows a number of voicemail channels to be reserved for announcements. See **System Settings** > **System** > **Voicemail**.
- With Voicemail Pro, the announcement can be replaced by the action specified in a Queued (1st announcement) or Still Queued (2nd announcement) start point call flow. Refer to the Voicemail Pro Installation and Maintenance documentation for details.
- Calls can be answered during the announcement. If it is a mandatory requirement that announcements should be heard before a call is answered, then a Voicemail Pro call flow should be used before the call is presented.

  Note:

  Call Billing and Logging

  A call becomes connected when the first announcement is played to it. That connected state is signaled to the call provider who may start billing at that point. The call will also be recorded as answered within the SMDR output once the first announcement is played.
- If a call is rerouted, for example forwarded, the announcement plan of the original user is still applied until the call is answered. The exception is calls rerouted to a hunt group at which point the hunt group announcement settings are applied.
- For announcements to be used effectively, either the user's no answer time must be extended beyond the default 15 seconds or Voicemail On should be deselected.

Recording Announcements

Voicemail Pro:

There is no mechanism within the telephony user interfaces (TUI) to record user announcements. To provide custom announcements, user queued and still queued start points must be configured with Voicemail Pro with the required prompts played by a generic action.

Embedded Voicemail:

Embedded Voicemail does not include any default announcement or method for recording an announcement. The Record Message short code feature is provided to allow the recording of announcements. The telephone number field of short codes using this feature requires the extension number followed by either ".1" for announcement 1 or ".2" for announcement 2. For example, for extension number 300, the short codes ***91N# | Record Message | N".1"** and ***92N# | Record Message | N".2"** could be used to allow recording of the announcements by dialing ***91300#** and ***92300#**.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Announcements On	Default = Off. This setting enables or disables announcements.
Wait before 1st announcement:	Default = 10 seconds. Range = 0 to 255 seconds. This setting sets the time delay from the calls presentation, after which the first announcement should be played to the caller.
Flag call as answered	Default = Off. This setting is used by the CCC and CBC applications. By default they do not regarded a call as answered until it has been answered by a person or by a Voicemail Pro action with **Flag call as answered** selected. This setting allows calls to be marked as answered once the caller has heard the first announcement.
Post announcement tone	Default = Music on hold. Following the first announcement, you can select whether the caller should hear Music on Hold, **Ringing** or **Silence** until answered or played another announcement.
2nd Announcement	Default = On. If selected, a second announcement can be played to the caller if they have still not been answered.
Wait before 2nd announcement	Default = 20 seconds. Range = 0 to 255 seconds. This setting sets the wait between the 1st and the 2nd announcement.
Repeat last announcement	Default = On. If selected, the last announcement played to the caller is repeated until they are answered or hang-up.
Wait before repeat	Default = 20 seconds. Range = 0 to 255 seconds. If **Repeat last announcement** is selected, this setting sets is applied between each repeat of the last announcement.

Related links

Users on page 157

Personal Directory

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Personal Directory**

Each user is able to have up to 250 personal directory records up to the overall system limit. Those records are used as follows:

- When using M-Series, T-Series, 1400, 1600, 9500, 9600 or J100 Series phones, the user is able to view and call their personal directory numbers.
- When using a 1400, 1600, 9500, 9600 or J100 Series phone, the user is also able to edit and add personal directory records.
- On phones that support hot desking on the same system or to another system in a multi-site network, the user can still access their personal directory.

Users are able to view and edit their personal directory through their phone. Directory records are used for dialing and caller name matching.

Directory Dialing

Directory numbers are displayed by user applications such as SoftConsole. Directory numbers are viewable through the Dir function on many Avaya phones (**Contacts** or **History**). They allow the user to select the number to dial by name. The directory will also contain the names and numbers of users and hunt groups on the system.

The **Dir** function groups directory records shown to the phone user into the following categories. Depending on the phone, the user may be able to select the category currently displayed. In some scenarios, the categories displayed may be limited to those supported for the function being performed by the user:

- **External** - Directory records from the system configuration. This includes HTTP and LDAP imported records.
- **Groups** - Groups on the system. If the system is in a multi-site network, it will also include groups on other systems in the network.
- **Users** or **Index** - Users on the system. If the system is in a multi-site network it will also include users on other systems in the network.
- **Personal** - Available on 1400, 1600, 9500, 9600 and J100 Series phones. These are the user's personal directory records stored within the system configuration.

Speed Dialing

On M-Series and T-Series phones, a Speed Dial button or dialing **Feature 0** can be used to access personal directory records with an index number.

- **Personal**: Dial **Feature 0** followed by ***** and the 2-digit index number in the range 01 to 99.
- **System**: Dial **Feature 0** followed by 3-digit index number in the range 001 to 999.

- The Speed Dial short code feature can also be used to access a directory speed dial using its index number from any type of phone.

Caller Name Matching

Directory records are also used to associate a name with the dialed number on outgoing calls or the received CLI on incoming calls. When name matching is being done, a match in the user's personal directory overrides any match in the system directory. Note that some user applications also have their own user directory.

SoftConsole applications have their own user directories which are also used by the applications name matching. Matches in the application directory may lead to the application displaying a different name from that shown on the phone.

Name matching is not performed when a name is supplied with the incoming call, for example QSIG trunks. On SIP trunks the use of the name matching or the name supplied by the trunk can be selected using the setting **System Settings** > **System** > **Telephony** > **Default Name Priority**. This setting can also be adjusted on individual SIP lines to override the system setting.

Directory name matching is not supported for DECT handsets. For information on directory integration, see Deploying Avaya Wireless DECT with IP Office.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Index	Range = 00 to 99 or None. This value is used with personal speed dials set and dialed from M and T-Series phones. The value can be changed but each value can only be applied to one directory record at any time. Setting the value to **None** makes the speed dial inaccessible from M and T-Series phones, however it may still be accessible from the directory functions of other phones and applications. The Speed Dial short code feature can be used to create short codes to dial the number stored with a specific index value. Release 10.0 allows users to have up to 250 personal directory entries. However, only 100 of those can be assigned index numbers.
Name	Range = Up to 31 characters. Enter the text to be used to identify the number.
Number	Range = Up to 31 digits plus * and #. Enter the number, without spaces, to be dialed. Wildcards are not supported in user personal directory records. Note that if the system has been configured to use an external dialing prefix, that prefix should be added to directory numbers.

Related links

Users on page 157

SIP

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **SIP**

This tab is available when either of the following has been added to the configuration:

- an **IP Office Line**
- a SIP trunk with a SIP URI record containing a field that has been set to **Use Internal Data**.

Various fields within the URI settings used by SIP trunks can be set to **Use Internal Data**. When that is the case, the values from this tab are used into the URI when the user makes or receives SIP calls. Within a multi-site network, that includes calls which break out using a SIP trunk on another system within the network.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
SIP Name	Default = Blank on Voicemail tab/Extension number on other tabs. This value is used for fields, other the `Contact` header, where the SIP URI entry being used has its **Contact** field set to **Use Internal Data**. • On incoming calls, if the **Local URI** is set to **Use Internal Data**, the system can potentially match the received `R-URI` or `From` header value to a user and/or group **SIP Name**. This requires the SIP URIs **Incoming Group** to match a Incoming Call Route with the same **Line Group ID** and a **.** (period) destination.
SIP Display Name (Alias)	Default = Blank on Voicemail tab/Name on other tabs. The value from this field is used when the **Display** field of the SIP URI being used is set to **Use Internal Data**.
Contact	Default = Blank on Voicemail tab/Extension number on other tabs. The value is used for the `Contact` header when the **Contact** field of the SIP URI being used for a SIP call is set to **Use Internal Data**.
Anonymous	Default = On on Voicemail tab/Off on other tabs. If the `From` field in the SIP URI is set to **Use Internal Data**, selecting this option inserts `Anonymous` into that field rather than the **SIP Name** set above. See Anonymous SIP Calls on page 935.

Related links

Users on page 157

Menu Programming

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Menu Programming**

This tab is used to set and lock the user's programmable button set.

When **Apply User Rights value** is selected, the tab operates in the same manner as the User | Menu Programming tab.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Related links

Users on page 157
Menu Programming — T3 Telephony on page 202
Menu Programming — Hunt Group on page 202
Menu Programming — 4400/6400 on page 203

Menu Programming — T3 Telephony

Navigation: **Call Management** > **Users** > **Edit** > **Advanced** > **Menu Programming** > **T3 Telephony**

These settings are applied to the user when they are using a T3 phone.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Configuration Settings

Third Party Forwarding Avaya T3 phone users can be given menu options to change the forwarding settings of other users. In addition to the following controls, this functionality is protected by the forwarding user's log in code.

- **Allow Third Party Forwarding**: Default = Off Sets whether this user can change the forwarding settings of other users.
- **Protect from Third Party Forwarding**: Default = Off Sets whether this user's forwarding settings can be changed by other users.

Advice of Charge

Display Charges: Default = On. This setting is used to control whether the user sees ISDN AOC information when using a T3 phone.

Allow Self Administer: Default = Off. If selected, this option allows the user to self-administer button programming.

Related links

Menu Programming on page 201

Menu Programming — Hunt Group

Navigation: **Call Management** > **Users** > **Edit** > **Advanced** > **Menu Programming** > **Hunt Group**

Avaya T3, 1400, 1600, 9500 and 9600 Series phone users can control various settings for selected hunt groups. These settings are also used for one-X Portal for IP Office.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Configuration Settings

Can Change Membership: Default = Off This list shows the hunt groups of which the user is a member. Up to 10 of these groups can be checked; those group and the users current membership status are then displayed on the phone. The user can change their membership status through the phone's menus.

T3 Series Phones: The selected hunt groups and the user's current membership status are displayed on the T3 phones status display. That display can be used to change the status.

Can Change Service Status: Default = Off This list shows all the hunt groups on the system. Up to 10 of these groups can be checked.

T3 Series Phones:

The user is then able to view and change the service status of the checked groups through their T3 phones menus (**Menu | Group State**).

In addition to changing the status of the individual hunt groups displayed via **Menu | Group State**, the menu also displays option to change the status of all the groups; **All in service**, **All night service** and **All out service**.

Can Change Night Service Group: Default = Off. If selected, the user can change the fallback group used when the hunt group is in Night Service mode.

Can Change Out of Service Group: Default = Off. If selected, the user can change the fallback group used when the hunt group is in Out of Service mode.

Related links

Menu Programming on page 201

Menu Programming — 4400/6400

Navigation: **Call Management** > **Users** > **Edit** > **Advanced** > **Menu Programming** > **4400/6400**

4412, 4424, 4612, 4624, 6408, 6416 and 6424 phones have a **Menu** key, sometimes marked with an icon. When **Menu** is pressed, a number of default functions are displayed. The < and > keys can be used to scroll through the functions while the keys below the display can be used to select the required function.

The default functions can be overwritten by selections made within this tab.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Configuration Settings

Menu No. The menu position which the function is being set.

Label This is a text label for display on the phone. If no label is entered, the default label for the selected action is used. Labels can also be changed through the menu on some phones, refer to the appropriate telephone user guide.

Action Defines the action taken by the menu button.

Action Data This is a parameter used by the selected action. The options here will vary according to the selected button action.

Related links

Menu Programming on page 201

Dial In

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Dial In**

Use this dialogue box to enable dial in access for a remote user. An Incoming Call Route and RAS service must also be configured.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Dial In On	Default = Off When enabled, dial in access into the system is available via this user.
Dial In Time Profile	Default = <None> Select the Time Profile applicable to this User account. A **Time Profile** can be used to set time restrictions on dial in access via this User account. Dial In is allowed during the times set in the Time Profile form. If left blank, then there are no restrictions.
Dial In Firewall Profile	Default = <None> Select the Firewall Profile to restrict access to the system via this User account. If blank, there are no Dial In restrictions.

Related links

Users on page 157

Source Numbers

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Source Numbers**

Source numbers are used to configure features which do not have specific controls within the IP Office Manager or IP Office Web Manager interfaces. For more details, see User Source Numbers on page 913.

Sources numbers are divided into two types:

- User source numbers are used to apply settings to individual users.
- NoUser source numbers are used to apply settings to the IP Office system or to all users on the system.

Related links

Users on page 157

User Portal

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **User Portal**

Use this menu to enable user portal for a user. You can configure whether they can use user portal and what features they can access within the user portal menus. For a user guide, refer to the Using the IP Office User Portal.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Name	Description
Enable User Portal	Default = Off When enabled, the user can log into user portal by entering the address of the system in the format `http://<address>` and then selecting **IP Office User Portal**. The login uses the user's **User Name** and **Password**.
Run Enduser Wizard	Default = Off If enabled, the user is walked through a series of menus when they login for the first time.

Table continues…

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Allowed Call Operations</td><td>Default = Both

Set whether and how the user can use their user portal to make and answer calls.

The user can change the current mode through their portal's Profile menu. The 'user choice' column in the table below indicates the options that the user can select and the default option used when they log in to the portal.

Note that modes other than None are only supported by users with the following licensed/subscribed profiles:

• On subscription systems, Telephony Plus User and UC User users.

• On non-subscription systems, Power User users.

All systems support the following modes:

<table>
<tr><th>Admin Setting</th><th>Description</th><th>User Choice</th></tr>
<tr><td>None</td><td>Do not use the portal to control current calls.</td><td>None</td></tr>
<tr><td>Call Control</td><td>Use the user portal to control calls using the user's deskphone.</td><td>None
Call Control[1]</td></tr>
</table>

Linux-based IP Office systems also support the following additional modes:

<table>
<tr><th>Admin Setting</th><th>Description</th><th>User Choice</th></tr>
<tr><td>Softphone[2]</td><td>Use the user's portal as a WebRTC softphone. Call audio uses the browser's speaker and microphone settings.</td><td>None
Softphone[1][2]</td></tr>
<tr><td>Both</td><td>Support any of the call operation modes.</td><td>None
Call Control[1]
Softphone[2]</td></tr>
</table>

1. This is the default mode the client will start in.

2. Softphone mode uses WebRTC provided by the IP Office system. For remote portal users, additional configuration of STUN or TURN is also required. See the notes at the bottom of the page.</td></tr>
</table>

User Settings Access

These options control the options that the user can access within self-administration and the type of access they have. For each set of options, the user can be given the following access:

- **No Access** - The user cannot access the related menu and its settings.
- **Read Access** - The user can view the settings on the menu but cannot change them.
- **Write Access** - The user can both view and change the settings on the menu.

Name	Description
Profile	This menu provides the access to details such as full name, voicemail and login code and email address.
Call Handling	This menu provides access to call controls such as forwarding, do not disturb and twinning.
Personal Directory	This menu provides access to the user's personal directory entries.
Button Programming	This option allows the user to assign features to programmable buttons on their phone and to change button labels. They still cannot override the settings of appearance buttons and buttons set by user rights.
Download Applications	This option display a menu of links for user applications that work with IP Office. Note that the user may require further configuration to use a specific application.

Media Manager Replay Self-Administration

These settings control the users rights to play call recordings stored by Media Manager or Centralized Media Manager.

Name	Description
Enable Media Manager Replay	Default = Off. When enabled, the user can replay call recordings through web self-administration. • Note: For users where Media Manager is provided by a separate application server, recordings are viewed and accessed using the address of the application server rather than that of the IP Office system.
Replay All Recordings	If selected, the user can view and replay all recordings.
Replay Own Recordings	If selected, the user can view and replay their own call recordings. When enabled, the **Replay Recordings For Group** and **Replay Recordings For Others** options are also available.
Replay Recordings For Group	These menus allows the selection of groups for which the user is able to view and replay recordings.
Replay Recordings For Others	The field can be used to enter a list of numbers, separated by semi-colons, for which the user can view and playback recordings. Those numbers can be accounts codes, line numbers, user extensions and group extension numbers. The list can be 127 characters in length.
Download Recordings	If selected, the user is able to download recordings as a separate file. • Downloaded files are outside of the control of the system. Therefore, if you allow users to download files, it is your responsibility to ensure that they comply with local privacy and data protection laws regarding the use of those files.

Historical Call Reporting

Call reporting allows the user to view a summary of recent calls by all users. This is currently a trial feature. It is only supported with subscription mode systems. The system must have its **System** > **SMDR** set to **Hosted Only**.

Name	Description
Enable Historical Call Reporting	Default = Off. When enabled, the user can access the call reporting menus through their user portal. For details, refer to the Using the IP Office Embedded Call Reporter manual.

User Portal Softphone Remote Access Notes

Non-IP500 V2 IP Officesystems can support the user portal as a WebRTC softphone. When operating as a remote extension, this may require the following:

- The IP Office and user portal to use STUN.
- Connection using an SBC configured for TURN.

For details, see the **System** > **LAN1** > **Network Topology** > **WebRTC** settings.

Related links

Users on page 157

Chapter 15: Extension

Navigation: **Call Management** > **Extensions**

Main content pane

The **Extensions** main content pane lists provisioned extensions. The contents of the list depends on the filter option selected. Click the icons beside a record to edit or delete.

Bulk delete: You can delete multiple records. Select the check box to the right of each record you want to delete and click **Delete**. You receive a prompt to confirm the deletion.

Click **Actions** for extension template management.

Click **Add/Edit Extension** to select an extension type to add. When you click **Add/Edit Extension**, you are prompted to specify the system where the extension will be added.

Extension Filters

Filter	Description
Show All	List all provisioned extensions on all systems.
Systems	List all provisioned extensions on specific systems.
Extension Type	List a specific provisioned extension type on all systems.

Related links

Extension Template Management on page 209
Add Extension on page 211
Extension Common Fields on page 211
Analog on page 214
H323 Extension VoIP on page 217
SIP Extension VOIP on page 220
T38 Fax on page 225
IP DECT Extension on page 227

Extension Template Management

Navigation: **Call Management** > **Extensions** > **Actions** > **Template Management**

Select the **Template Management** action to open the Extension Templates page. Click **Add** to define an extension template.

Related links

Extension on page 209
Create From Template on page 210
Provision Extensions on page 210

Create From Template

Navigation: **Call Management** > **Extensions** > **Actions** > **Create From Template**

Use this page to add extensions using a template. You can define extension templates by selecting **Call Management** > **Extensions** > **Actions** > **Template Management**.

When you click **Create From Template** and then select a server, the Select Template window opens.

Once you have defined the settings below and click **OK**, the Provision Extensions page opens.

Field	Description
Enter number of records	Enter the number of records you want to create.
Enter starting extension	Enter the extension number of the first record.
Select Template	Select a template from the list.

Related links

Extension Template Management on page 209

Provision Extensions

Navigation: **Call Management** > **Extensions** > **Actions** > **Create From Template** > **Select Template** > **Provision Extensions**

This page displays the extension records that will be created based on the values entered in the Select Template window.

At the top of the page, the **Preview Extensions Data** area indicates the server on which the users will be created, the number of records (**Total Records Read**) and the **Records with Error**.

The table lists the user records that will be created and the values that have been populated based on the template. You can remove records from the list using **Delete Selected Records**. You can modify the display by turning **Show Error Records** on or off.

When you are ready to create the new extension records, click **Create**.

Related links

Extension Template Management on page 209

Add Extension

Navigation: **Call Management** > **Extensions** > **Add/Edit Extension**

Extension Type	Description
H323 **SIP**	IP extensions are either added manually or by the automatic detection of the phone being connected. IP extensions can also be added manually to support a third-party IP phone device.
IP DECT **SIP DECT**	An extension port manually added to match extensions within an Avaya IP DECT system connected to the system via an IP DECT line.

Related links

Extension on page 209

Extension Common Fields

Navigation: **Call Management** > **Extensions** > **Edit Extension** > **Common**

Additional configuration information

The Caller Display Type setting controls the presentation of caller display information. For additional configuration information, see Caller Display on page 739.

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 806.

Configuration Settings

These settings can be edited online except **Base Extension** and **Caller Display Type**. Changes to those settings require a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Extension ID	The physical ID of the extension port. Except for IP extensions, this settings is allocated by the system and is not configurable.

Table continues…

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Base Extension</td><td>Range = 2 to 15 digits.

This is the directory number of the extension's default associated user if one is required.

• The field can be left blank for digital and analog extensions, creating and extension where users are forced to login but the extension has no default associated user. This option is not supported for IP and CTI extensions.

• Following a restart, the system attempts to log in the user with the same extension number if they are not already logged in elsewhere in the multi-site network. This does not occur if that user is set to Force Login.

• If another user logs onto an extension, when they log out, the extension returns to its default associated user unless they have logged in elsewhere or are set to Force Login.</td></tr>
<tr><td>Phone Password</td><td>Default = Blank. Range = 9 to 13 digits.

H.323 and SIP extensions only. This password is entered as part of phone registration with the IP Office system.</td></tr>
<tr><td>Caller Display Type</td><td>Default = On.

Controls the presentation of caller display information for analog extensions. For digital and IP extensions, this value is fixed as On. The table below lists the supported options, all others are currently not used and default to matching UK.

<table><tr><th>Type</th><th>Description</th></tr><tr><td>Off</td><td>Disables caller display.</td></tr><tr><td>On</td><td>Enables caller display using the caller display type appropriate to the System Locale, see Avaya IP Office Locale Settings. If a different setting is required it can be selected from the list of supported options. For an analog extension connected to a fax server or other device that requires the pass through of DTMF tones, select DTMFF.</td></tr><tr><td>UK</td><td>FSK before the first ring conforming to BT SIN 227. Name and number.</td></tr><tr><td>UK20</td><td>As per UK but with a maximum length of 20 characters. Name and number.</td></tr><tr><td>DTMFA</td><td>Caller ID in the DTMF pattern A<caller ID>C. Number only.</td></tr><tr><td>DTMFB</td><td>Caller ID in DTMF after call connection. Number only.</td></tr><tr><td>DTMFC</td><td>Caller ID in the DTMF pattern A<caller ID>#. Number only.</td></tr><tr><td>DTMFF</td><td>Sends the called number in DTMF after call connection. Number only. Used for fax servers. When calls are delivered via a hunt group it is recommended that hunt group queuing is not used. If hunt group queuing is being used, set the Queue Type to Assign Call on Agent Alert.</td></tr><tr><td>DTMFD</td><td>Caller ID in the DTMF pattern D<caller ID>C. Number only.</td></tr><tr><td>FSKA</td><td>Variant of UK used for BT Relate 1100 phones. Name and number.</td></tr><tr><td>FSKB</td><td>ETSI specification with 0.25 second leading ring. Name and number.</td></tr><tr><td>FSKC</td><td>ETSI specification with 1.2 second leading ring. Name and number.</td></tr><tr><td>FSKD</td><td>Conforms to Belcore specification. Name and number.</td></tr></table></td></tr>
</table>

Table continues…

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Reset Volume after Calls</td><td>Default = Off.

Resets the phone's handset volume after each call. This option is supported on Avaya 1400, 1600, 2400, 4400, 4600, 5400, 5600, 6400, 9500 and 9600 Series phones.</td></tr>
<tr><td>Device Type</td><td>This field indicates, the last known type of phone connected to the extension port.

• Analog extension ports always report as Analog Handset since the presence or absence of actual analog phone cannot be detected.

• Digital extension ports report the type of digital phone connected or Unknown digital handset if no phone is detected.

• H.323 extensions report the type of IP phone registered or Unknown H.323 handset if no phone is currently registered as that extension.

• SIP extensions report the type of SIP phone registered or Unknown SIP device if no SIP device is currently registered as that extension. Applications such as Avaya Workplace Client and one-X Mobile Preferred that do not use extension records also display Device type as Unknown SIP device.

For some types of phone, the phone can only report its general type to the system but not the specific model. When that is the case, the field acts as a drop-drown to select a specific model. The value selected is also reported in other applications such as the System Status Application, SNMP, etc.
<table>
<tr><th>Default Type</th><th>Possible Phone Models</th></tr>
<tr><td>T7100</td><td>M7100, M7100N, T7100, Audio Conferencing Unit.</td></tr>
<tr><td>T7208</td><td>M7208, M7208N, T7208.</td></tr>
<tr><td>M7310</td><td>M7310, M7310N, T7406, T7406E.</td></tr>
<tr><td>M7310BLF</td><td>M7310BLF, T7316.</td></tr>
<tr><td>M7324</td><td>M7324, M7324N.</td></tr>
</table>
</td></tr>
<tr><td>Location</td><td>The drop down list contains all locations that have been defined on the system: System Settings > Locations. See Using Locations on page 739.

Associating an extension with a location:

• Allows emergency call routing using settings specific to that location.

• Allows the display of location based time. Supported on 1100, 1200, 1600, 9600 and J100 Series phones and D100, E129 and B179 telephones.

• For Avaya Wireless DECT extensions, the extension location can be overridden on a call-by-call basis using the location name specified in the base station configuration. Supported with R11.1 FP2 SP2 and higher. This requires you to set Call based Location Information on the IP DECT line and to configure each base station with a location name that matches one in the IP Office configuration.</td></tr>
</table>

Table continues…

Field	Description
Fallback as Remote Worker	Default = Auto. Determines what fallback address is used for Remote Worker phone resiliency. The options are: • **Auto**: Use the fallback address configured on the IP Office Line providing the service. • **No**: Use the alternate gateway private address. • **Yes**: Use the alternate gateway public address.
Module	This field indicates the external expansion module on which the port is located. **BP** indicates an analog phone extension port on the base or control unit. **BD** indicates a digital station (DS) port on the control unit. For an IP500 V2 control unit, **BD** and **BP** is also followed by the slot number. VoIP extensions report as **0**.
Port	This field indicates the port number on the **Module** indicated above. VoIP extensions report as **0**.
Disable Speakerphone	Default = Off (Speakerphone enabled). When selected, disables the fixed **SPEAKER** button if present on the phone using this extension port. Only supported on Avaya DS, TCM and H.323 IP phones. An audible beep is sounded when a disabled **SPEAKER** button is pressed. Incoming calls such as pages and intercom calls are still connected but the speech path is not audible until the user goes off-hook using the handset or headset. Similarly calls made or answered using other buttons on the phone are not audible unless the user goes off-hook using the handset or headset. Currently connected calls are not affected by changes to this setting.

Related links

Extension on page 209

Analog

Navigation: **Call Management** > **Extensions** > **Edit Extension** > **Analog**

This tab contains settings that are applicable to analog extensions. These extensions are provided by ports marked as **POT** or **PHONE** on control units and expansion modules.

These settings are not mergeable. Changes to these settings will require a reboot of the system.

Equipment Classification:

Field	Description
Default = Standard Telephone. Only available for analog extension ports. Note that changes to this setting are mergeable.	

Table continues…

Field	Description
Quiet Headset	On extensions set to **Quiet Headset**, the audio path is disabled when the extension is idle. Ringing is presented in the audio path. Caller ID is not supported on the phone. This option can be used with analog extensions where the handset is replaced by a headset and all audio, including ringing should be through the headset. Since the audio path is disabled when idle, the **Quiet Headset** extension cannot dial digits to make calls. Therefore, to make and answer calls this option is typically used with the user **Offhook Station** (**User** > **Telephony** > **Call Settings** setting which allows the extension user to make and answer calls using applications.
Paging Speaker	Used for analog ports connected to a paging amplifier. This extension will present busy and cannot be called or be used to make calls. It can only be accessed using Dial Paging features. When using a UPAM connected to an analog extension port, the extension's **Equipment Classification** should be set to **IVR Port** rather than **Paging Speaker**.
Standard Telephone	Use for normal analog phones.
Door Phone 1/Door Phone 2	These two options are currently not used and so are grayed out.
IVR Port	Used for analog ports connected to devices that require a disconnect clear signal (a break in the loop current) at the end of each call. When selected the **Disconnect Pulse Width** is used.
FAX Machine	If fax Relay is being used, this setting should be selected on any analog extension connected to an analog fax machine. This setting can also be used with SIP trunks.
MOH Source	If selected, the port can be used as a music on hold source in the **System** > **Telephony** > **Tones and Music** settings. An extension set as a music on hold source cannot make or receive calls. The audio input can be monitored through the extension music on hold controls. A suitable interface device is required to provide the audio input to the extension port. It must look to the system like an off-hook analog phone. For example, a transformer with a 600 Ohm winding (such as a Bogen WMT1A) or a dedicated MoH device with a 600 Ohm output designed for connection to a PBX extension port which is providing loop current can be used.

Flash Hook Pulse Width

The following options are only available for analog extension ports. They define the length of loop break that will be considered a time break recall (TBR) signal.

Field	Description
Use System Defaults	Default = On Use the default values appropriate to the system's locale. Refer to Avaya IP Office Locale Settings.

Table continues…

Field	Description
Minimum Width	Range = 20 to 2540 milliseconds. Minimum hook flash length used if **Use System Defaults** is not selected. Shorter breaks are ignored a glitches.
Maximum Width	Range = 30 to 2550 milliseconds. Maximum hook flash length used if **Use System Defaults** is not selected. Longer breaks are treated as clearing.
Disconnect Pulse Width	Default = 0ms. Range = 0 to 2550ms This setting is used with analog extensions where the **Equipment Classification** above has been set to **IVR Port**. It sets the length of loop current break used to indicate call clearing.

Message Waiting Lamp Indication Type

Field	Description
Message Waiting Lamp Indication Type	Default = None Allows the selection of the message waiting indication (MWI) mode for analog and IP DECT extensions. The options are: **On** *(See below)*, **51V Stepped**, **81V**, **101V** *(Phone V2 and IP500 Phone base cards)*, **Bellcore FSK**, **Line Reversal A**, **Line Reversal B**.

If the option **Restrict Analog Extension Ringer Voltage** is selected (**System | Telephony | Telephony**), the MWI options are restricted to: **Line Reversal A**, **Line Reversal B** or **None** with the default **Line Reversal A**.

On defaults the message waiting indication setting as follows based on the system locale:

Setting	Locale
51V Stepped	Argentina, Australia, Brazil, Canada, Chile, China, Colombia, Japan, Korea, Mexico, New Zealand, Peru, Russia, Saudi Arabia, South Africa, Spain, United States, Venezuela
101V on Phone V2 modules and IP500 Phone cards, otherwise **81V**.	Bahrain, Belgium, Denmark, Egypt, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, Italy, India, Kuwait, Morocco, Netherlands, Norway, Oman, Pakistan, Poland, Portugal, Qatar, Singapore, Sweden, Switzerland, Taiwan, Turkey, United Arab Emirates, United Kingdom

Hook Persistency

Field	Description
Hook Persistency	Default = 100ms. Range = 50 to 255ms. Sets the minimum time the extension needs to be off-hook before the system treats it as off-hook and applies any off-hook features. For example dialing timers or hot-dial short codes. Shorter periods of off-hook time are ignored.

Related links

Extension on page 209

H323 Extension VoIP

Navigation: **Call Management** > **Extensions** > **Edit Extension** > **H323 VoIP**

These settings are shown for a H.323 IP extension.

These settings can only be edited offline. Changes to these settings require a reboot of the system.

Field	Description
IP Address	Default = 0.0.0.0 (Accept any address) If an address is entered here, the IP Office will only accept registration from a device with that address.
MAC Address	Default = 0000000000000 (Grayed out) This field is grayed out and not used.
Codec Selection	Default = System Default Set the supported codecs. Where possible, Avaya recommend that you use the same set of codecs for all IP Office systems, lines, and extensions. The options are: • **System Default** - Use the codec list set in the system settings. • **Custom** - Configure a list of codec preferences for the line. - You can move codecs between the **Unused** and **Selected** sets and change the order of the codecs. - The codecs available are set by **System Settings** > **System** > **VoIP**. The possible codecs are: • **OPUS** - Supported on Linux-based IP Office systems only. • **G.711 ALAW/G.711 ULAW** • **G.729** • **G.723.1** - Supported on IP500 V2 systems only. • **G.722 64K** - Supported by Linux-based IP Office systems and on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards.
TDM | IP Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the system TDM interface to the IP connection. This field is not shown on Linux based platforms.
IP | TDM Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the IP connection to the system TDM interface. This field is not shown on Linux based platforms.

Table continues…

Field	Description
Supplementary Services	Default = H450. Selects the supplementary service signaling method for use with non-Avaya IP devices. Options are **None**, **QSIG** and **H450**. For H450, hold and transfer are supported. Note that the selected method must be supported by the remote end.
Media Security	Default = Same as System. These settings control whether SRTP is used for this extension and the settings used for the SRTP. The options are: • **Same as System**: Matches the system setting at **System Settings** > **System** > **VoIP Security**. • **Disabled**: Use RTP. • **Preferred**: Attempt to use SRTP. If SRTP call setup is unsuccessful, fall back to RTP. • **Enforced**: Use SRTP. If SRTP call setup is unsuccessful, the call fails. - For calls using **Dial Emergency**, the IP Office will switch to RTP if SRTP call setup fails.
Advanced Media Security Options	Default = Same as System. Sets the requirements for SRTP when enabled. • **Same as System**: Use the same settings as configured on **System Settings** > **System** > **VoIP Security**. • **Encryptions**: Default = RTP Sets which parts of a session SRTP protects using encryption. • **Authentication**: Default = RTP and RTCP Sets which parts of the session SRTP protects using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Not adjustable. The IP Office will accept authenticated packets that have a sequence number that is higher than or within 64 packets of the highest-numbered packet already received. • **Crypto Suites**: Default = *SRTP_AES_CM_128_SHA1_80*. Set the crypto suites SRTP uses for encryption. The options are *SRTP_AES_CM_128_SHA1_32* and *SRTP_AES_CM_128_SHA1_80*.
VoIP Silence Suppression	Default = Off When enabled, when the IP Office detects silence during an IP call, it does not send any audio data. • Lines between IP Office systems using G.711 ignore this feature. • On trunks between networked IP Office systems, you must enable the setting at both ends.

Table continues…

Field	Description
Enable FastStart for non-Avaya IP Phones	Default = Off A fast connection procedure. Reduces the number of messages that need to be exchanged before an audio channel is created.
Out of Band DTMF	Default = On When on, DTMF is sent as a separate signal ("Out of Band") rather than as part of the encoded voice stream ("In Band"). The "Out of Band" signaling is inserted back into the audio by the remote end. This is recommended for low bit-rate compression modes such as G.729 and G.723 where DTMF in the voice stream can become distorted. For Avaya 1600, 4600, 5600 and 9600 Series phones, the system will enforce the appropriate setting for the phone type.
Requires DTMF	Default = Off. This field is displayed when **Ignore DTMF Mismatch for Phones** (**System** > > **VoIP** is enabled. • If disabled, during the checks for direct media on calls between two VoIP phones, the system ignores the DTMF checks. - Direct media may still not be possible if other settings, such as codecs, NAT settings, or security settings, do not match. • If enabled, the extension needs to receive DTMF signals. - When enabled, the extension setting is ignored for contact center applications. Contact center application SIP extensions are always treated as requiring DTMF.
Local Tones	Default = Off When selected, the H.323 phones generate their own tones.
Allow Direct Media Path	Default = On This settings controls whether calls between IP endpoints and/or lines must go through the IP Office. • If disabled, calls go through the IP Office and use its resources. RTP relay allows calls between devices using the same audio codec to not require a voice compression channel. • If enabled, calls can take routes other than through the IP Office system. Both ends must support direct media and have matching VoIP settings. For example, both ends must use the same protocol (SIP or H.323), same addressing (IPv4 or IPv6), and so on. Otherwise, the call goes through the IP Office system. - For extensions, disabling **Requires DTMF** allows the extension to attempt direct media even if the other end has differing DTMF settings.

Table continues…

Field	Description
Reserve License	Default = None. By default, the IP Office issues phone licenses in the order that devices register. Using this setting, you can license an extension before the device registers. The options are: • **Reserve Avaya IP Endpoint License** • **Reserve 3rd Party IP Endpoint License** • **Both** • **None** Note: • Avaya IP phones supported by IP Office require an Avaya IP Endpoint license. • Other IP phones require a Third-Party IP Endpoint license. • When WebLM licensing is enabled, this field is automatically set to **Reserve Avaya IP Endpoint License.** The **Both** and **None** options are not available. • When the **Profile** of the corresponding user is set to **Centralized User**, this field is automatically set to **Centralized Endpoint License**.

Related links

Extension on page 209

SIP Extension VOIP

Navigation: **Call Management** > **Extensions** > **Edit Extension** > **SIP VoIP**

The IP Office uses these settings for SIP extensions. For example, for J100 Series phones.

Field	Description
IP Address	Default = 0.0.0.0 (Accept any IPv4 address) If set, the IP Office will only accept registration from a device with the same address.

Table continues…

Field	Description
IP Address (IPv6)	Default = Blank (Accept any IPv6 address) If set, the IP Office will only accept registration from a device with the same address. • Supported on Linux-based IP Office R12.1 systems only. To enable IPv6 support, select **LAN1** > **LAN Setting (IPv6)** > **IPv6** and/or **LAN2** > **LAN Setting (IPv6)** > **IPv6**. • The IP Office supports IPv6 addresses in the following formats: - Full address: For example, `2001:0000:040F:0000:0000:0000:805B:001B`. - Replace one series of `:0000:` parts with `::`. For example, `2001:0000:040F::805B:001B`. - Replace any individual `:0000:` parts with `:0:`. For example, `2001:0:040F::805B:001B`. - Remove leading `0` zeros after any `:` colon. For example, `2001:0:40F::805B:1B`.
Codec Selection	Default = System Default Set the supported codecs. Where possible, Avaya recommend that you use the same set of codecs for all IP Office systems, lines, and extensions. The options are: • **System Default** - Use the codec list set in the system settings. • **Custom** - Configure a list of codec preferences for the line. - You can move codecs between the **Unused** and **Selected** sets and change the order of the codecs. - The codecs available are set by **System Settings** > **System** > **VoIP**. The possible codecs are: • **OPUS** - Supported on Linux-based IP Office systems only. • **G.711 ALAW/G.711 ULAW** • **G.729** • **G.723.1** - Supported on IP500 V2 systems only. • **G.722 64K** - Supported by Linux-based IP Office systems and on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards.

Table continues…

Field	Description
Reserve License	Default = None. By default, the IP Office issues phone licenses in the order that devices register. Using this setting, you can license an extension before the device registers. The options are: • **Reserve Avaya IP Endpoint License** • **Reserve 3rd Party IP Endpoint License** • **Both** • **None** Note: • Avaya IP phones supported by IP Office require an Avaya IP Endpoint license. • Other IP phones require a Third-Party IP Endpoint license. • When WebLM licensing is enabled, this field is automatically set to **Reserve Avaya IP Endpoint License.** The **Both** and **None** options are not available. • When the **Profile** of the corresponding user is set to **Centralized User**, this field is automatically set to **Centralized Endpoint License**.
VoIP Silence Suppression	Default = Off When enabled, when the IP Office detects silence during an IP call, it does not send any audio data. • Lines between IP Office systems using G.711 ignore this feature. • On trunks between networked IP Office systems, you must enable the setting at both ends.

Table continues…

Field	Description
Fax Transport Support	Default = None. If enabled, when the IP Office detects fax tone, it will renegotiate the call codec as configured below. • This option requires **Re-Invite Supported**. • IP Office systems in a network support fax relay for fax calls between systems. • IP500 V2 systems can terminate T38 fax calls. • Linux-based IP Office systems can route the calls between trunks/terminals with compatible fax types. The supported options are: • **None** - Do not support fax. • **G.711** - Use G.711 to send and receive faxes. • **T38** - Use T38 to send and receive faxes. • **T38 Fallback** - Use T38 to send and receive faxes. If the call destination does not support T38, the IP Office will send a re-invite to change the transport method to **G.711**.
DTMF Transport	Default = RFC2833. Set how the IP Office signals DTMF key presses to the remote end. The supported options are **In Band**, **RFC2833**, or **Info**.
Requires DTMF	Default = Off. You can use this setting to attempt direct media between devices with differing DTMF setting. This requires you to enable **Ignore DTMF Mismatch for Phones** (**System Settings** > **System** > **VoIP**). • If disabled, during direct media check the IP Office ignores the DTMF checks if the call is between two VoIP phones. - Direct media is still not be possible if other settings differ, for example; codecs, NAT, or security settings. • You must enable **Requires DTMF** if the extension needs to receive DTMF signals. The IP Office treats SIP soft-phone that do not have an extension record in the IP Office configuration as not requiring DTMF.
Local Hold Music	Default = Off. When enabled, the extension plays local music when on HOLD. • For calls using a SIP line, if the SIP line **Local Hold Music** setting is enabled (**System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Advanced**), you must disable the extension **Local Hold Music** setting to play far end music to the extension.

Table continues…

Field	Description
Allow Direct Media Path	Default = On This settings controls whether calls between IP endpoints and/or lines must go through the IP Office. • If disabled, calls go through the IP Office and use its resources. RTP relay allows calls between devices using the same audio codec to not require a voice compression channel. • If enabled, calls can take routes other than through the IP Office system. Both ends must support direct media and have matching VoIP settings. For example, both ends must use the same protocol (SIP or H.323), same addressing (IPv4 or IPv6), and so on. Otherwise, the call goes through the IP Office system. - For extensions, disabling **Requires DTMF** allows the extension to attempt direct media even if the other end has differing DTMF settings.
VoIP Silence Suppression	Default = Off When enabled, when the IP Office detects silence during an IP call, it does not send any audio data. • Lines between IP Office systems using G.711 ignore this feature. • On trunks between networked IP Office systems, you must enable the setting at both ends.
Codec Lockdown	Default = Off. After making a SIP offer with a list of codecs, the IP Office expects an answer with a single codec selected from the list. User agents that send an answer with multiple codecs expect to switch to any of those codecs during the call without further negotiation, which the IP Office does not support. Instead, loss of speech occurs if the user agent changes codec without renegotiating. • If enabled, when the IP Office receives an answer with multiple codecs, the IP Office sends a `re-INVITE` and a SIP offer with just one codec. • This option requires **Re-Invite Supported** enabled.
3rd Party Auto Answer	Default = None. This setting applies to 3rd party standard SIP extensions. The options are: • **RFC 5373**: Add an RFC 5373 auto answer header to the INVITE. • **answer-after**: Add answer-after header. • **device auto answers**: IP Office relies on the phone to auto answer calls.

Table continues…

Field	Description
Media Security	Default = Same as System. These settings control how the extension uses SRTP. The options are: • **Same as System**: Matches the system setting at **System Settings** > **System** > **VoIP Security**. • **Disabled**: Use RTP. • **Preferred**: Attempt to use SRTP. If SRTP call setup is unsuccessful, fall back to RTP. • **Enforced**: Use SRTP. If SRTP call setup is unsuccessful, the call fails. - For calls using **Dial Emergency**, the IP Office will switch to RTP if SRTP call setup fails.
Advanced Media Security Options	Default = Same as System. Sets the requirements for SRTP when enabled. • **Same as System**: Use the same settings as configured on **System Settings** > **System** > **VoIP Security**. • **Encryptions**: Default = RTP Sets which parts of a session SRTP protects using encryption. • **Authentication**: Default = RTP and RTCP Sets which parts of the session SRTP protects using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Not adjustable. The IP Office will accept authenticated packets that have a sequence number that is higher than or within 64 packets of the highest-numbered packet already received. • **Crypto Suites**: Default = *SRTP_AES_CM_128_SHA1_80*. Set the crypto suites SRTP uses for encryption. The options are *SRTP_AES_CM_128_SHA1_32* and *SRTP_AES_CM_128_SHA1_80*.

Related links

Extension on page 209

T38 Fax

Navigation: **Call Management** > **Extensions** > **Edit Extension** > **SIP T38 Fax**

The settings are available only on IP500 V2 since it can terminate T38 fax. On the **VoIP** settings for the line type, **Fax Transport Support** must be set to **T38** or **T38 Fallback**.

These settings are mergeable.

Field	Description
Use Default Values	Default = On. If selected, all the fields are set to their default values and greyed out.
T38 Fax Version	Default = 3. During fax relay, the two gateways will negotiate to use the highest version which they both support. The options are: **0**, **1**, **2**, **3**.
Transport	Default = UDPTL (fixed). Only **UDPTL** is supported. **TCP** and **RTP** transport are not supported. For **UDPTL**, redundancy error correction is supported. Forward Error Correction (FEC) is not supported.
Redundancy Redundancy sends additional fax packets in order to increase the reliability. However increased redundancy increases the bandwidth required for the fax transport.	
Low Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for low speed V.21 T.30 fax transmissions.
High Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for V.17, V.27 and V.28 fax transmissions.
TCF Method	Default = Trans TCF. TCF = Training Check Frame.
Max Bit Rate (bps)	Default = 14400. Lower rates can be selected if the current rate is not supported by the fax equipment or is found to not be reliable.
EFlag Start Timer (msecs)	Default = 2600.
EFlag Stop Timer (msecs)	Default = 2300.
Tx Network Timeout (secs)	Default = 150.
Scan Line Fix-up	Default = On.
TFOP Enhancement	Default = On.
Disable T30 ECM	Default = Off. When selected, disabled the T.30 Error Correction Mode used for fax transmission.
Disable EFlags For First DIS	Default = Off.
Disable T30 MR Compression	Default = Off.

Table continues…

Field	Description
NSF Override	Default = Off. If selected, the NSF (Non-Standard Facility) information sent by the T38 device can be overridden using the values in the fields below. **Country Code**: Default = 0. **Vendor Code**: Default = 0.

Related links

Extension on page 209

IP DECT Extension

Navigation: **Call Management** > **Extensions** > **Edit Extension** > **IP DECT**

IP DECT extensions are created manually after an IP DECT line has been added to the configuration or added automatically as DECT handsets subscribe to the DECT system.

These settings can be edited online with the exception of the **Reserve License** setting. The **Reserve License** setting must be edited offline and requires a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
DECT Line ID	Use the drop-down list to select the IP DECT line from the system to the Avaya Wireless DECT system.
Message Waiting Lamp Indication Type	Default = On Allows selection of the message waiting indication to use with the IP DECT extension. The options are: • None • On

Table continues…

Field	Description
Reserve License	Default = None. By default, the IP Office issues phone licenses in the order that devices register. Using this setting, you can license an extension before the device registers. The options are: • **Reserve Avaya IP Endpoint License** • **Reserve 3rd Party IP Endpoint License** • **Both** • **None** Note: • Avaya IP phones supported by IP Office require an Avaya IP Endpoint license. • Other IP phones require a Third-Party IP Endpoint license. • When WebLM licensing is enabled, this field is automatically set to **Reserve Avaya IP Endpoint License.** The **Both** and **None** options are not available. • When the **Profile** of the corresponding user is set to **Centralized User**, this field is automatically set to **Centralized Endpoint License**.

The additional fields below depend on whether the IP DECT line has **Enable Provisioning** selected.

Enable Provisioning Not Selected

Field	Description
Handset Type	Default = Unknown Correct selection of the handset type allows application of appropriate settings for the handset display and buttons. Selectable handset types are supported 3700 Series phones or **Unknown**.

Enable Provisioning Selected

Field	Description
IPEI	Default = 0 (Any IPEI) If set to a value other than 0, sets the IPEI number of the handset that is able to subscribe to the Avaya Wireless DECT system using this extension number. The IPEI for each DECT handset is unique.
Use Handset Configuration	Default = Off. If **Use Handset Configuration**. is selected, the handset user is able to set the phone language and date/time format. If not selected, those settings will be driven by the system or user locale settings in the system configuration.

Related links

Extension on page 209

Chapter 16: Groups

Navigation: **Call Management** > **Group**

Additional configuration information

This section provides the Group field descriptions.

For additional configuration information, see Group Operation on page 883.

Main content pane

The **Group** main content pane lists provisioned groups. The contents of the list depends on the filter option selected. Click the icons beside a record to edit or delete.

Bulk delete: You can delete multiple records. Select the check box to the right of each record you want to delete and click **Delete**. You receive a prompt to confirm the deletion.

Click **Add/Edit Group** to open the Add Groups window where you can provision a user. When you click **Add/Edit Group**, you are prompted to specify the server on which the group will be provisioned.

Group Filters

Filter	Description
Show All	List all provisioned groups on all systems.
Systems	List the groups provisioned on a specific system.
Ring Modes	List groups provisioned with specific ring modes on all systems.
Profiles	
Queuing	List groups with queuing enabled.

Related links

Add Groups on page 230
Group settings on page 230
Queuing on page 234
Overflow on page 237
Fallback on page 239
Voicemail on page 242
Voice Recording on page 248
Announcements on page 249
SIP on page 252

Add Groups

Navigation: **Call Management** > **Group** > **Add/Edit Group**

Related links

Groups on page 229

Group settings

Navigation: **Call Management** > **Group** > **Add/Edit Group** > **Group**

Additional configuration information

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 806.

Configuration settings

The Group settings are used to define the name, extension number and basic operation of the group. It is also used to select the group members.

You can edit these settings online without needing to reboot the IP Office.

Field	Description
Name	Range = Up to 15 characters The name to identify this group. This field is case sensitive and must be unique. • Do not start names with a space. Do not use punctuation characters such as #, ?, /, ^, > and ,. • Voicemail uses the name to match a group and its mailbox. Changing the name will route voicemail calls to a new mailbox. Note that Voicemail Pro is not case-sensitive. For example it will treat "Sales", "sales" and "SALES" as being the same.

Table continues…

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Profile</td><td>Default = Standard Hunt Group

Defines the group type. The options are:

<table>
<tr><th>Profile</th><th>Description</th></tr>
<tr><td>Standard Hunt Group</td><td>The default group type and the standard method for creating IP Office user groups.</td></tr>
<tr><td>XMPP Group</td><td>Extensible Messaging and Presence Protocol (XMPP) is a communications protocol for presence status and Instant Messaging (IM). Select XMPP to enable presence information and instant messaging within a defined group of XMPP enabled one-X clients. Two users can see each other's presence and exchange instant messages only if they are members of the same XMPP group. A user can be a member of zero or more groups.

Important:

Before adding a user to an XMPP group, the user must be added to the configuration and the configuration saved. If the user is added to the group before the directory is synchronized, the user will not be visible in one-X Portal.</td></tr>
<tr><td>Centralized Group</td><td>Used for centralized extensions that are normally handled by the core feature server (Avaya Aura®) and are handled by the IP Office only when in survival mode due to loss of connection to the Avaya Aura®.

Calls arriving to a centralized hunt group number when the Avaya Aura® line is in-service are sent by the IP Office to Avaya Aura®. Calls arriving to a centralized hunt group number when the Avaya Aura Session Manager line is out-of-service are processed by the IP Office and targeted to the hunt group members as configured on the IP Office.</td></tr>
</table>
</td></tr>
<tr><td>Extension</td><td>Range = 1 to 15 digits.

This sets the directory number for calls to the hunt group.

• Groups for CBC and CCC should only use up to 4 digit extension numbers.
• Extension numbers in the range 8897 to 9999 are reserved for use by the IP Office Delta Server.</td></tr>
<tr><td>Exclude From Directory</td><td>Default = Off

When on, the user does not appear in the directory list shown by the user applications and on phones with a directory function.</td></tr>
</table>

Table continues…

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Ring Mode</td><td>Default = Sequential

Sets how the system determines which hunt group member to ring first and the next hunt group member to ring if unanswered. This is used in conjunction with the User List which list the order of group membership. The options are:

<table>
<tr><th>Ring Mode</th><th>Description</th></tr>
<tr><td>Collective</td><td>All available phones in the User List phones ring simultaneously.</td></tr>
<tr><td>Collective Call Waiting</td><td>This is a Collective hunt group as above but with hunt group call waiting also enabled. When an additional call to the hunt group call is waiting to be answered, users in the group who are already on a call will receive call waiting indication.

• On phones with call appearance buttons, the call waiting indication takes the form of an alert on the next available call appearance button. The user's own Call Waiting On setting is overridden when they are using a phone with call appearances.

• On other phones, call waiting indication is given by a tone in the speech path (the tone is locale specific). The user's Call Waiting On setting is used in conjunction with the hunt group setting.</td></tr>
<tr><td>Sequential</td><td>Each extension is rung in order, one after the other, starting from the first extension in the list each time.</td></tr>
<tr><td>Rotary</td><td>Each extension is rung in order, one after the other. However, the last extension used is remembered. The next call received rings the next extension in the list.</td></tr>
<tr><td>Longest Waiting</td><td>The extension that has been unused for the longest period rings first, then the extension that has been idle second longest rings, etc. For extensions with equal idle time, 'sequential' mode is used.

Where hunt group calls are being presented to a twinned extension, the longest waiting status of the user can be reset by calls answered at either their master or twinned extension.</td></tr>
</table>
</td></tr>
<tr><td>No Answer Time (secs)</td><td>Default = System Default. Range = System Default or 6 to 99999 seconds.

The number of seconds an extension rings before the call is passed to another extension in the list. This applies to all telephones in this group and also any Overflow Group List groups it uses. Leave blank to use the system default setting (System > Telephony > Telephony > Default No Answer Time).

• This does not apply for collective hunt groups, where calls will continue ringing until either the Overflow Time or Group No Answer Time applies.

• If the group contains users who are using Avaya Workplace Client on iOS devices, Avaya recommends the time is set to at least 20 seconds.</td></tr>
</table>

Table continues…

Field	Description
Hold Music Source	Default = No Change. The system can support multiple music on hold sources; the **System Source** (either an internal file or the external source port or tones) plus a number of additional internal sources (3 on IP500 V2 systems, 31 on Linux systems), see **System** > **Telephony** > **Tones & Music**. Before reaching a hunt group, the source used is set by the system wide setting or by the **Incoming Call Route** that routed the call. If the system has several hold music sources available, this field allows selection of the source to associate with calls presented to this hunt group or to leave it unchanged. The new source selection will then apply even if the call is forwarded or transferred out of the hunt group unless changed again by another hunt group. If the call is routed to another system in a multi-site network, the matching source on that system is used if available. Hunt group calls overflowing ignore the settings of the **Overflow Group List** groups. Calls going to night service or out of service fallback group use the hold music source setting of the original hunt group and then, if different, the setting of the fallback group. The setting of further fallback groups from the first are ignored.
Ring Tone Override	Default = Blank If ring tones have been configured in the **System | Telephony | Ring Tones** tab, they are available in this list. Setting a ring tone override applies a unique ring tone for the hunt group. Ring tone override features are only supported on 1400 Series, 9500 Series and J100 Series (except J129) phones.
Agent's Status on No-Answer Applies To	Default = None (No status change). For hunt group members with a login code set and **Force Log** enabled, the system can change their status if they do not answer a hunt group call presented to them within the group's **No Answer Time**. • This setting defines what type of hunt group calls can trigger use of the agent's **Status on No Answer** setting. The options are **None**, **Any Call** and **External Inbound Calls Only**. • The new status is set by the agent's **Status on No Answer** setting (**User** > **Telephony** > **Supervisor Settings**). • The **Status on No Answer** action does not apply if the call is presented and then answered elsewhere or the caller disconnects. • This option is not used for calls ringing the agent because the group is in another group's **Overflow Group List**.

Table continues…

Field	Description
User List	This is an ordered list of the users who are members of the hunt group. For **Sequential** and **Rotary** groups it also sets the order in which group members are used for call presentation. • Repeated numbers can be used, for example 201, 202, 201, 203, etc. Each extension will ring for the number of seconds defined by the **No Answer Time** before moving to the next extension in the list, dependent on the Hunt Type chosen. • The check box next to each member indicates the status of their membership. Group calls are not presented to members who have their membership currently disabled. However, those users are still able to perform group functions such as group call pickup. • The order of the users can be changed by dragging the existing records to the required position. • To add records select **Edit**. A new menu is displayed that shows available users on the left and current group members of the right. The lists can be sorted and filtered. • Users on remote systems in a multi-site network can also be included. Groups containing remote members are automatically advertised within the network. • Before adding a user to an XMPP group, the user must be added to the configuration and the configuration saved. If the user is added to the group before the directory is synchronized, the user will not be visible in one-X Portal.

Related links

Groups on page 229

Queuing

Navigation: **Call Management** > **Group** > **Add/Edit Group** > **Queuing**

Any calls waiting to be answered at a hunt group are regarded as being queued. The **Normalise Queue Length** control allows selection of whether features that are triggered by the queue length should include or exclude ringing calls. Once one call is queued, any further calls are also queued. When an available hunt group member becomes idle, the first call in the queue is presented. Calls are added to the queue until the hunt group's Queue Limit, if set, is reached.

- When the queue limit is reached, any further calls are redirected to the hunt group's voicemail if available.
- If voicemail is not available excess calls receive busy tone. An exception to this are analog trunk and T1 CAS trunk calls which will remain queued regardless of the queue limit if no alternate destination is available.
- If an existing queued call is displaced by a higher priority call, the displaced call will remain queued even if it now exceeds the queue limit.

Hunt group announcements are separate from queuing. Announcements can be used even if queuing is turned off and are applied to ringing and queued calls. See Hunt Group | Announcements.

There are several methods of displaying a hunt group queue.

- **Group Button**: On phones, with programmable buttons, the **Group** function can be assigned to monitor a specified group. The button indicates when there are calls ringing within the group and also when there are calls queued. The button can be used to answer the longest waiting call.
- **SoftConsole**: The SoftConsole applications can display queue monitors for up to 7 selected hunt groups. This requires the hunt group to have queuing enabled. These queues can be used by the SoftConsole user to answer calls.

When a hunt group member becomes available, the first call in the queue is presented to that member. If several members become available, the first call in the queue is simultaneously presented to all the free members.

Overflow Calls Calls that overflow are counted in the queue of the original hunt group from which they overflow and not that of the hunt group to which they overflow. This affects the **Queue Limit** and **Calls in Queue Threshold**.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Queuing On	Default = On If enabled, calls to the hunt group are queued.
Queue Length	Default = No Limit. Range = No Limit, 1 to 99 calls. This setting can be used to limit the number of calls that can be queued. Calls exceeding this limit are passed to voicemail if available or otherwise receive busy tone. This value is affected by Normalize Queue Length setting. • If voicemail is not available excess calls receive busy tone. An exception to this is analog trunk and T1 CAS trunk calls which will remain queued regardless of the queue limit if no alternate destination is available. This is due to the limited call status signalling supported by those trunks which would otherwise create scenarios where the caller has received ringing from the local line provider and then suddenly gets busy from the system, creating the impression that the call was answered and then hung up. • If priority is being used with incoming call routes, high priority calls are place ahead of lower priority calls. If this would exceed the queue limit the limit is temporarily increased by 1. • If an existing queued call is displaced by a higher priority call, the displaced call will remain queued even if it now exceeds the queue limit.

Table continues…

Field	Description
Normalize Queue Length	Default = On. Calls both waiting to ring and ringing are regarded as being queued. This therefore affects the use of the **Queue Limit** and **Calls in Queue Alarm** thresholds. If **Normalize Queue Length** is enabled, the number of hunt group members logged in and not on DND is added to those thresholds. For example, a customer has two products that it is selling through a call center with 10 available agents; one product with a $10 margin and one with a $100 margin. Separate hunt groups with the same 10 members are created for each product. • The $100 product has a Queue Limit of 5 and Normalize Queue Length is on. The maximum number of $100 calls that can be waiting to be answered will be 15 (10 ringing/connected + 5 waiting to ring). • The $10 product has a Queue Limit of 5 and Normalize Queue Length is off. The maximum number of $10 calls that can be waiting to be answered is 5 (5 ringing/connected).
Queue Type	Default = Assign Call On Agent Answer. When queuing is being used, the call that the agent receives when they answer can be assigned in one of two ways: • **Assign Call On Agent Answer** In this mode the call answered by the hunt group member will always be the longest waiting call of the highest priority. The same call will be shown on all ringing phones in the group. At the moment of answering that may not necessarily be the same call as was shown by the call details at the start of ringing. • **Assign Call on Agent Alert** In this mode, once a call has been presented to a hunt group member, that is the call they will answer if they go off hook. This mode should be used when calls are being presented to applications which use the call details such as a fax server, CTI or TAPI.
Calls In Queue Alarm	The system can be set to send an alert to a analog specified extension when the number of calls queued for the hunt group reaches the specified threshold.
Calls In Queue Threshold	Default = Off. Range = 1 to 99. Alerting is triggered when the number of queued calls reaches this threshold. Alerting will stop only when the number of queued calls drops back below this threshold. This value is affected by **Normalize Queue Length** setting above.
Analog Extension to Notify	Default = <None>. This should be set to the extension number of a user associated with an analog extension. The intention is that this analog extension port should be connected to a loud ringer or other alerting device and so is not used for making or receiving calls. The list will only shown analog extensions that are not members of any hunt group or the queuing alarm target for any other hunt group queue. The alert does not follow user settings such as forwarding, follow me, DND, call coverage, etc or receive ICLID information.

Group Queue Controls

Group Queue Settings	
Manager	Hunt group queuing is enabled using the Queuing On option on the **Hunt Group | Queuing** tab.
Controls	The following short code features/button programming actions can be used:
SoftConsole	SoftConsole can display up to 7 hunt group queues (an eighth queue is reserved for recall calls). They are configured by clicking and selecting the **Queue Mode** tab. • Within the displayed queues, the number of queued calls is indicated and the time of the longest queued call is shown. Exceeding an alarm threshold is indicated by the queue icons changing from white to red. The longest waiting call in a queue can be answered by clicking on the adjacent button. • For each queue, an alarm threshold can be set based on number of queued calls and longest queued call time. Actions can then be selected for when a queue exceeds its alarm threshold; **Automatically Restore SoftConsole**, **Ask me whether to restore SoftConsole** or **Ignore the Alarm**.

Related links

Groups on page 229

Overflow

Navigation: **Call Management** > **Group** > **Add/Edit Group** > **Overflow**

Overflow can be used to expand the list of group members who can be used to answer a call. This is done by defining an overflow group or groups. The call is still targeted to the original group and subject to that group's settings, but is now presented to available members in the overflow groups in addition to its own available members.

Overflow calls still use the settings of the original target group. The only settings of the overflow group that is used is it's **Ring Mode**. For example:

- Calls that overflow use the announcement settings of the group from which they are overflowing.
- Calls that overflow use the **Voicemail Answer Time** of the original group from which are are overflowing.
- Calls that are overflowing are included in the overflowing group's **Queue Length** and **Calls In Queue Threshold**. They are not included in those values for the hunt group to which they overflow.
- The queuing and overflow settings of the overflow groups are not used, ie. calls cannot cascade through a series of multiple overflows.

A call will overflow in the following scenarios:

- If **Queuing** is off and all members of the hunt group are busy, a call presented to the group will overflow immediately, irrespective of the **Overflow Time**.

- If **Queuing** is on and all members of the hunt group are busy, a call presented to the group will queue for up to the **Overflow Time** before overflowing.
- If **Queuing** is on but there are no members logged in or enabled, calls can be set to overflow immediately by setting the **Overflow Immediate** setting to **No Active Members**. Otherwise calls will queue until the **Overflow Time** expires.
- If no **Overflow Time** is set, a call will overflow when it has rung each available hunt group member without being answered.
- Once one call is in overflow mode, any additional calls will also overflow if the **Overflow Mode** is set to **Group** (the default).

An overflow call is presented to available group members as follows:

- Once a call overflows, it is presented to the first available member of the first overflow group listed. The **Ring Mode** of the overflow group is used to determine its first available member. However the **No Answer Time** of the original targeted group is used to determine how long the call is presented.
- When the **No Answer Time** expires, the call is presented to the next available member in the overflow group. If all available members in the overflow group have been tried, the first member in the next listed overflow group is tried.
- When the call has been presented to all available members in the overflow groups, it is presented back to the first available member in the original target group.
- While the call is being presented to members in an overflow group, the announcement and voicemail settings of the original targeted group are still applied.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Overflow Time	Default = Blank. Range = Off or 1 to 3600 seconds. For a group using queuing, the **Overflow Time** sets how long a call queues before being presented to available agents in the group's **Overflow Group List**. Note that if the call is currently ringing an agent when the timer expires, it will complete ringing for the group's **No Answer Time** before overflowing.
Overflow Mode	Default = Group. This option allows selection of whether the overflow of queued calls is determined on an individual call by call basis or is applied to all calls once any one call overflows. The options are: • **Group**: In this mode, once one call overflows all additional queued calls also overflow. • **Call**: In this mode, each individual call will follow the group's overflow settings before it overflows.

Table continues…

Field	Description
Immediate Overflow:	Default = Off. For groups which are using queueing, this setting can be used to control whether calls should overflow immediately when there are no available or active agents. The options are: • **Off**: Do not overflow immediately. Use the **Overflow Time** setting as normal. • **No Active Agents**: Overflow immediately if there are no available or active agents as defined above, regardless of the **Overflow Time** setting. - An active agent is an agent who is either busy on a call or in after call work. An available agent is one who is logged in and enabled in the hunt group but is otherwise idle. - A hunt group is automatically treated as having no available or active agents if: - The group's extension list is empty. - The group's extension list contains no enabled users. - The group's extension list contains no extensions that resolve to a logged in agent (or mobile twin in the case of a user logged out mobile twinning).
Overflow Group List	This list is used to set the group or groups that are used for overflow. Each group is used in turn, in order from the top of the list. The call is presented to each overflow group member once, using the **Ring Mode** of the overflow group. If the call remains unanswered, the next overflow group in the list is used. If the call remains unanswered at the end of the list of overflow groups, it is presented to available members of the original targeted group again and then to those in its overflow list in a repeating loop. A group can be included in the overflow list more than once if required and the same agent can be in multiple groups.

Related links

Groups on page 229

Fallback

Navigation: **Call Management** > **Group** > **Add/Edit Group** > **Fallback**

Fallback settings can be used to make a hunt group unavailable and to set where the hunt group's calls should be redirected at such times. Hunt groups can be manually placed In Service, Out of Service or in Night Service. Additionally using a time profile, a group can be automatically placed in Night Service when outside the Time Profile settings.

Fallback redirects a hunt group's calls when the hunt group is not available, for example outside normal working hours. It can be triggered either manually or using an associated time profile.

Group Service States:

A hunt group can be in one of three states; **In Service**, **Out of Service** or **Night Service**. When **In Service**, calls are presented as normal. In any other state, calls are redirected as below.

Call Redirection:

The following options are possible when a hunt group is either **Out of Service** or in **Night Service**.

- **Destination**: When in **Out of Service**, if an **Out of Service Destination** has been set, calls are redirected to that destination. When in **Night Service**, if a **Night Service Destination** has been set, calls are redirected to that destination.
- **Voicemail**: If no fallback destination has been set but voicemail is enabled for the group, calls are redirected to voicemail.
- **Busy Tone**: If no fallback destination has been set and voicemail is not available, busy tone is returned to calls.

Manually Controlling the Service State:

Manager and or short codes can be used to change the service state of a hunt group. The short code actions can also be assigned to programmable buttons on phones.

- The icon is used for a hunt group manually set to **Night Service** mode.
- The icon is used for a hunt group manually set to **Out of Service** mode.

Setting and clearing hunt group night service can be done using either manual controls or using a system time profile. The use of both methods to control the night service status of a particular hunt group is not supported. You can manually override a time profile.

Time Profile:

A **Day Service Time Profile** can be associated with the hunt group. A time profile if required, is set through **System Settings** > **Time Profiles** > **Add/Edit Time Profile**.

When outside the time profile, the hunt group is automatically placed into night service. When inside the time profile, the hunt group uses manually selected mode.

- When outside the time profile and therefore in night service, manual night service controls cannot be used to override the night service. However the hunt group can be put into out of service.
- When a hunt group is in Night Service due to a time profile, this is not indicated within Manager.
- Time profile operation does not affect hunt groups set to Out of Service.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Day Service Time Profile	Default = <None> (No automatic night service) This field allows selection of a previously created Time Profile. That profile then specifies the times at which it should use the manually selected Service Mode settings. Outside the period defined in the time profile, the hunt group behaves as if set to Night Service mode. Note that when a hunt group is in Night Service due to it associated time profile, this is not reflected by the Service Mode on this tab. Note also that the manual controls for changing a hunt group's service mode cannot be used to take a hunt group out of time profile night service.
Night Service Destination	Default = <None> (Voicemail or Busy Tone) This field sets the alternate destination for calls when this hunt group is in Night Service mode. The destination can be a group, a user, a short code, or an Auto Attendant. Select a group or user from the drop down list. Manually enter a short code or an Auto Attendant name. If left blank, calls are redirected to voicemail if available or otherwise receive busy tone.
Out of Service Fallback Group	Default = <None> (Voicemail or Busy Tone) This field sets the alternate destination for calls when this hunt group is in Out of Service mode. The destination can be a group, a user, a short code, or an Auto Attendant. Select a group or user from the drop down list. Manually enter a short code or an Auto Attendant name. For Auto Attendant names, use the format **AA:Name**. If left blank, calls are redirected to voicemail if available or otherwise receive busy tone.
Mode	Default = In Service This field is used to select the current service mode for the hunt group manually. The options are: • **In Service**: When selected, the hunt group is enabled. This is the default mode. • **Night Service**: When selected, calls are redirected using the **Night Service Fallback Group** setting. This setting can also be manually controlled using the short code, and button programming features Set Hunt Group Night Service and Clear Hunt Group Night Service. • **Out of Service**: When selected, calls are redirected using the **Out of Service Fallback Group** setting. This setting can also be manually controlled using the short code, and button programming features Set Hunt Group Out of Service and Clear Hunt Group Out of Service.
Group No Answer Time	Default = 45 seconds, Range = 1 to 3600 seconds. This setting sets the time duration on presting a call to a hunt group and its overflow groups if set before going to the group's **Group No Answer Destination**. Exceeding the time duration redirects the call regardless of any announcements, overflow, or queue. If **Group No Answer Time** is set to **Off**, the no answer destination is used, and once each available member of the hunt group is alerted for the group's **No Answer Time**.

Table continues…

Field	Description
Group No Answer Destination	When an unanswered call to a hunt group reaches the **Group No Answer Time**, you can configure the following options: • **<NONE>** - The destination is not used. Instead, calls continue ringing against the hunt group. • **Voicemail** - The call is redirected to a voicemail to leave a message and uses the call original destination mailbox. Set to **Voicemail** for default configurations. • The drop-down list includes all other group and user extensions and redirects the call to that extension. • You can enter a number manually to match against system short codes.

Hunt Group Fallback Controls

The following short code features and button programming actions can be used.

Feature/Action	Short Code	Default	Button
Set Hunt Group Night Service	Yes	*20*N#	Yes-Toggles
Clear Hunt Group Night Service	Yes	*21*N#	Yes
Set Hunt Group Out of Service	No	No	Yes-Toggles
Clear Hunt Group Out of Service	No	No	Yes

Note that for a hunt group using a time profile, these controls only are only applied when the hunt group is within the specified time profile period. When outside its time profile, the hunt group is in night service mode and cannot be overridden.

Related links

Groups on page 229

Voicemail

Navigation: **Call Management** > **Group** > **Add/Edit Group** > **Voicemail**

The system supports voicemail for hunt groups in addition to individual user voicemail mailboxes.

If voicemail is available and enabled for a hunt group, it is used in the following scenarios.

Scenario	Description
Group No Answer Time	For 11.1 FP1 and higher, the use of voicemail to answer calls during normal operation is controlled by the group's Fallback settings.

Table continues…

Scenario	Description
Voicemail Answer Time	This option is only used for pre-11.1 FP1 systems. A call goes to voicemail when this timeout is reached, regardless of any announcement, overflow, queuing or other settings. The default timeout is 45 seconds.
Unanswered Calls	A call goes to voicemail when it has been presented to all the available hunt group members without being answered. If overflow is being used, this includes be presented to all the available overflow group members.
Night Service	A call goes to voicemail if the hunt group is in night service with no **Night Service Fallback Group** set.
Out of Service	A call goes to voicemail if the hunt group is out of service with no **Out of Service Fallback Group** set.
Queue Limit Reached	If queuing is being used, it overrides use of voicemail prior to expiry of the **Voicemail Answer Time**, unless the number of queued callers exceeds the set **Queue Limit**. By default there is no set limit.
Automatic Call Recording	Incoming calls to a hunt group can be automatically recorded using the settings on the **Hunt Group** > **Voice Recording tab**.

When a caller is directed to voicemail to leave a message, the system indicates the target user or hunt group mailbox.

The mailbox of the originally targeted user or hunt group is used. This applies even if the call has been forwarded to another destination. It also includes scenarios where a hunt group call overflows or is in fallback to another group.

Voicemail Pro can be used to customize which mailbox is used separately from the mailbox indicated by the system.

By default no user is configured to receive message waiting indication when a hunt group voicemail mailbox contains new messages. Message waiting indication is configured by adding a **H groupname** record to a user's **SourceNumbers** tab (**User** > **Source Numbers**).

By default, no mechanism is provided for access to specific hunt group mailboxes. Access needs to be configured using either a short code, programmable button or source number.

- **Intuity Emulation Mailbox Mode**:For systems using Intuity emulation mode mailboxes, the hunt group extension number and voicemail code can be used during normal mailbox access.
- **Avaya Branch Gateway Mailbox Mode** or **IP Office Mailbox Mode**: For this mode of mailbox access, short codes or a Voicemail Collect button are required to access the mailbox directly.

The voicemail system (Voicemail Pro only) can be instructed to automatically forward messages to the individual mailboxes of the hunt group members. The messages are not stored in the hunt group mailbox.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Voicemail On	**Note:** From 11.1 FP1 IP Office system onwards, you can configure **Voicemail On** through **Group No Answer Destination** under **Group | Fallback** tab. Default = On When on, the mailbox is used by the system to answer the any calls to the group that reaches the **Voicemail Answer Time**. Note that selecting off does not disable the use of the group mailbox. Messages can still be forward to the mailbox, and recordings can be placed in it. The mailbox can also still be accessed to collect messages. When a caller is directed to the voicemail to leave a message, the system indicates the target user or hunt group mailbox. • The mailbox of the originally targeted user or hunt group is used. This applies even if the call was forwarded to another destination. It also includes scenarios where a hunt group call overflows or is in fallback to another group. • Voicemail Pro can be used to customize which mailbox is used separately from the mailbox indicated by the system.
Voicemail Answer Time	**Note:** From 11.1 FP1 IP Office system onwards, you can configure **Voicemail Answer Time** through **Group No Answer Time** under **Group | Fallback** tab. Default = 45 seconds. Range = Off, 1 to 99999 seconds. This setting sets how long a call should be presented to a hunt group, and its overflow groups if set, before going to the voicemail. When exceeded, the call goes to voicemail (if available) regardless of any announcements, overflow, queuing, or any other actions. If set to **Off**, voicemail is used when all available members of the hunt group have been alerted for the no answer time.

Table continues…

Field	Description
Voicemail Code	Default = Blank. Range = 0 (no code) to 15 digits. A code used by the voicemail server to validate access to this mailbox. If remote access is attempted to a mailbox that has no voicemail code set, the prompt "Remote access is not configured on this mailbox" is played. The mailbox access code can be set through IP Office Manager or through the mailbox telephone user interface (TUI). The minimum password length is: • Voicemail Pro (Manager) - 0 • Voicemail Pro (Intuity TUI) - 2 • Embedded Voicemail (Manager) - 0 • Embedded Voicemail (Intuity TUI) - 0 Codes set through the Voicemail Pro telephone user interface are restricted to valid sequences. For example, attempting to enter a code that matches the mailbox extension, repeat the same number (1111) or a sequence of numbers (1234) are not allowed. If these types of code are required they can be entered through Manager. Manager does not enforce any password requirements for the code if one is set through Manager. • **Embedded Voicemail** For Embedded Voicemail running in IP Office mailbox mode, the voicemail code is used if set. • **IP Office mode** The voicemail code is required when accessing the mailbox from a location that is not set as a trusted number in the user's Source Numbers list. • **Intuity Emulation mode** By default the voicemail code is required for all mailbox access. The first time the mailbox is accessed the user will be prompted to change the password. Also if the voicemail code setting is left blank, the caller will be prompted to set a code when they next access the mailbox. The requirement to enter the voicemail code can be removed by adding a customized user or default collect call flow, refer to the Voicemail Pro manuals for full details. • **Trusted Source Access** The voicemail code is required when accessing the mailbox from a location that is not set as a trusted number in the user's Source Numbers list. • **Call Flow Password Request** Voicemail Pro call flows containing an action where the action's PIN code set to **$** will prompt the user for their voicemail code.
Voicemail Help	Default = Off This option controls whether users retrieving messages are automatically given an additional prompt "For help at any time press 8." If switched off, users can still press 8 for help. For voicemail systems running in Intuity emulation mode, this option has no effect. On those systems the default access greeting always includes the prompt "For help at any time, press *4" (*H in the US locale).

Table continues…

Field	Description
Broadcast	Default = Off. (Voicemail Pro only). When enabled, if a voicemail message is left for the hunt group, copies of the message are forwarded to the mailboxes of the individual group members. The original message in the hunt group mailbox is deleted unless it occurred as the result of call recording. This feature is not applied to recordings created by **Voice Question** actions.
UMS Web Services	Default = Off. This option is used with Voicemail Pro. If enabled, the hunt group mailbox can be accessed using either an IMAP email client or a web browser. Note that the mailbox must have a voicemail code set in order to use either of the UMS interfaces. **UMS Web Service** licenses are required for the number of groups configured. In the License section, double-clicking on the **UMS Web Services** license display a menu that allows you to add and remove users and groups from the list of those enabled for UMS Web Services without having to open the settings of each individual user or group.
Voicemail Email:	Default = Blank (No voicemail email features) This field is used to set the user or group email address used by the voicemail server for voicemail email operation. When an address is entered, the additional Voicemail Email control below are selectable to configure the type of voicemail email service that should be provided. Use of voicemail email requires the Voicemail Pro server to have been configured to use either a local MAPI email client or an SMTP email server account. For Embedded Voicemail, voicemail email is supportedand uses the system's SMTP settings. The use of voicemail email for the sending (automatic or manual) of email messages with wav files attached should be considered with care. A one-minute message creates a 1MB .wav file. Many email systems impose limits on emails and email attachment sizes. For example the default limit on an Exchange server is 5MB.

Table continues…

Field	Description
Voicemail Email	Default = Off If an email address is entered for the user or group, the following options become selectable. These control the mode of automatic voicemail email operation provided by the voicemail server whenever the voicemail mailbox receives a new voicemail message. Users can change their voicemail email mode using visual voice. If the voicemail server is set to IP Office mode, user can also change their voicemail email mode through the telephone prompts. The ability to change the voicemail email mode can also be provided by Voicemail Pro in a call flow using a Play Configuration Menu action or a Generic action. If the voicemail server is set to IP Office mode, users can manually forward a message to email. The options are: • **Off** If off, none of the options below are used for automatic voicemail email. Users can also select this mode by dialing *03 from their extension. • **Copy** If this mode is selected, each time a new voicemail message is received in the voicemail mailbox, a copy of the message is attached to an email and sent to the email address. There is no mailbox synchronization between the email and voicemail mailboxes. For example reading and deletion of the email message does not affect the message in the voicemail mailbox or the message waiting indication provided for that new message. • **Forward** If this mode is selected, each time a new voicemail message is received in the voicemail mailbox, that message is attached to an email and sent to the email address. No copy of the voicemail message is retained in the voicemail mailbox and their is no message waiting indication. As with Copy, there is no mailbox synchronization between the email and voicemail mailboxes. Users can also select this mode by dialing *01 from their extension. Note that until email forwarding is completed, the message is present in the voicemail server mailbox and so may trigger features such as message waiting indication. • **UMS Exchange 2007** With Voicemail Pro, the system supports voicemail email to an Exchange 2007 server email account. For users and groups also enabled for UMS Web Services this significantly changes their mailbox operation. The Exchange Server inbox is used as their voicemail message store and features such as message waiting indication are set by new messages in that location rather than the voicemail mailbox on the voicemail server. Telephone access to voicemail messages, including Visual Voice access, is redirected to the Exchange 2007 mailbox. • **Alert** If this mode is selected, each time a new voicemail message is received in the voicemail mailbox, a simple email message is sent to the email address. This is an email message announcing details of the voicemail message but with no copy of the voicemail message attached. Users can also select this mode by dialing ***02** from their extension.

Related links

Groups on page 229

Voice Recording

Navigation: **Call Management** > **Group** > **Add/Edit Group** > **Voicemail Recording**

This tab is used to configure automatic recording of calls handled by hunt group members.

- Call recording requires Voicemail Pro to be installed and running. Call recording also requires available conference resources similar to a 3-way conference.
- Call recording starts when the call is answered.
- Call recording is paused when the call is parked or held. It restarts when the call is unparked or taken off hold. This does not apply to SIP terminals.
- Calls to and from IP devices, including those using Direct media, can be recorded.
- Recording continues for the duration of the call or up to the maximum recording time configured on the voicemail server.
- Recording is stopped when the call ends or if:
  - User call recording stops if the call is transferred to another user.
  - Account code call recording stops if the call is transferred to another user.
  - Hunt group call recording stops if the call is transferred to another user who is not a member of the hunt group.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Record Inbound	Default = None Select whether automatic recording of incoming calls is enabled. The options are: • **None**: Do not automatically record calls. • **On**: Record the call if possible. Otherwise, allow the call to continue without recording. • **Mandatory**: Record the call if possible. Otherwise, block the call and return busy tone. • **Percentages of calls**: Record a selected percentages of the calls.
Record Time Profile	Default = <None> (Any time) Used to select a time profile during which automatic call recording of incoming calls is applied. If no profile is selected, automatic recording is always active.

Table continues…

Field	Description
Recording (Auto)	Default = Mailbox Sets the destination for automatically triggered recordings. The options are: • **Mailbox** This option sets the destination for the recording to be a selected user or hunt group mailbox. The adjacent drop down list is used to select the mailbox. • **Voice Recording Library**: This option set the destination for the recording to be a VRL folder on the voicemail server. The VRL application polls that folder and collects waiting recordings which it then places in its archive. Recording is still done by Voicemail Pro. • **Voice Recording Library Authenticated**: This option is similar to the above but instructs the voicemail server to create an authenticated recording. If the file contents are changed, the file is invalidated though it can still be played. - For systems recording to `.opus` format (the default), both settings create authenticated recordings.
Auto Record Calls	Default = External. This setting allows selection of which calls are recorded. The options are **External** or **External & Internal**.

Related links

Groups on page 229

Announcements

Navigation: **Call Management** > **Group** > **Add/Edit Group** > **Announcements**

Announcements are played to callers waiting to be answered. This includes callers being presented to hunt group members, ie. ringing, and callers queued for presentation.

- The system supports announcements using Voicemail Pro or Embedded Voicemail.
- If no voicemail channel is available for an announcement, the announcement is not played.
- In conjunction with Voicemail Pro, the system allows a number of voicemail channels to be reserved for announcements. See **System Settings** > **System** > **Voicemail**.
- With Voicemail Pro, the announcement can be replaced by the action specified in a Queued (1st announcement) or Still Queued (2nd announcement) start point call flow. Refer to the *Voicemail Pro Installation and Maintenance* documentation for details.
- Calls can be answered during the announcement. If it is a mandatory requirement that announcements should be heard before a call is answered, then a Voicemail Pro call flow should be used before the call is presented.
- A call becomes connected when the first announcement is played to it. That connected state is signaled to the call provider who may start billing at that point. The call will also be recorded as answered within the SMDR output once the first announcement is played.
- If a call is rerouted to a hunt group's Night Service Group or Out of Service Fallback Group, the announcements of the new group are applied.

- If a call overflows, the announcements of the original group are still applied, not those of the overflow group.
- For announcements to be used effectively, the hunt group's **Voicemail Answer Time** must be extended or **Voicemail On** must be unselected.

Recording the Group Announcement

Voicemail Pro provides a default announcement "I'm afraid all the operators are busy but please hold and you will be transferred when somebody becomes available". This default is used for announcement 1 and announcement 2 if no specific hunt group announcement has been recorded. Embedded Voicemail does not provide any default announcement. Voicemail Lite also provides the default announcements.

The maximum length for announcements is 10 minutes. New announcements can be recorded using the following methods.

Voicemail Pro	The method of recording announcements depends on the mailbox mode being used by the voicemail server. • **IP Office Mailbox Mode:** Access the hunt group mailbox and press 3. Then press either 3 to record the 1st announcement for the hunt group or 4 to record the 2nd announcement for the hunt group. • **Intuity Emulation Mailbox Mode:** There is no mechanism within the Intuity telephony user interface (TUI) to record hunt group announcements. To provide custom announcements, hunt group queued and still queued start points must be configured with Voicemail Pro with the required prompts played by a generic action.
Embedded Voicemail	Embedded Voicemail does not include any default announcement or method for recording announcements. The **Record Message** short code feature is provided to allow the recording of announcements. The telephone number field of short codes using this feature requires the extension number followed by either ".1" for announcement 1 or ".2" for announcement 2. For example, for extension number 300, the short codes ***91N# | Record Message | N".1"** and ***92N# | Record Message | N".2"** could be used to allow recording of the announcements by dialing ***91300#** and ***92300#**.

Settings

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Announcements On	Default = Off. This setting enables or disables announcements.

Table continues…

Field	Description
Wait before 1st announcement:	Default = 10 seconds. Range = 0 to 255 seconds. This setting sets the time delay from the calls presentation, after which the first announcement should be played to the caller. If **Synchronize Calls** is selected, the actual wait may differ, see below.
Flag call as answered	Default = Off. This setting is used by the CCC and CBC applications. By default they do not regarded a call as answered until it has been answered by a person or by a Voicemail Pro action with **Flag call as answered** selected. This setting allows calls to be marked as answered once the caller has heard the first announcement.
Post announcement tone	Default = Music on hold. Following the first announcement, you can select whether the caller should hear Music on Hold, **Ringing** or **Silence** until answered or played another announcement.
2nd Announcement	Default = On. If selected, a second announcement can be played to the caller if they have still not been answered.
Wait before 2nd announcement	Default = 20 seconds. Range = 0 to 255 seconds. This setting sets the wait between the 1st and the 2nd announcement. If **Synchronize Calls** is selected, the actual wait may differ, see below.
Repeat last announcement	Default = On. If selected, the last announcement played to the caller is repeated until they are answered or hang-up.
Wait before repeat	Default = 20 seconds. Range = 0 to 255 seconds. If **Repeat last announcement** is selected, this setting sets is applied between each repeat of the last announcement. If **Synchronize Calls** is selected, this value is grayed out and set to match the **Wait before 2nd announcement** setting.

Table continues…

Field	Description
Synchronize calls	Default = Off This option can be used to reduce the number of voicemail channels required to provide the announcements. Using this setting, the maximum number of voicemail channels needed is 1 or 2 depending on the number of selected announcements. • When on: - If the required prompt is already being played to another caller, further callers wait until the prompt has completed and can be restarted. - If the required prompt is not being played and there are multiple waiting callers, once one caller has waited for the set wait period, the prompt is played to all the currently waiting callers. - If Voicemail Pro custom **Queued** or **Still Queued** start point call flows are used for the announcements, when **Synchronize Calls** is enabled the call flows support the playing of prompts only. • When off: - Announcements are played individually for each call. This requires a separate voicemail channel each time an announcement is played to each caller. While this accurately follows the wait settings, it does not use voicemail channels efficiently.

Related links

Groups on page 229

SIP

Navigation: **Call Management** > **Group** > **Add/Edit Group** > **SIP**

Each hunt group can be configured with its own SIP URI information. For calls received on a SIP line where any of the line's SIP URI fields are set to **Use Internal Data**, if the call is presented to the hunt group that data is taken from these settings.

This form is hidden if there are no system multi-site network lines in the configuration or no SIP lines with a URI set to **Use Internal Data**.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
SIP Name	Default = Blank on Voicemail tab/Extension number on other tabs. This value is used for fields, other the `Contact` header, where the SIP URI entry being used has its **Contact** field set to **Use Internal Data**. • On incoming calls, if the **Local URI** is set to **Use Internal Data**, the system can potentially match the received `R-URI` or `From` header value to a user and/or group **SIP Name**. This requires the SIP URIs **Incoming Group** to match a Incoming Call Route with the same **Line Group ID** and a **.** (period) destination.
SIP Display Name (Alias)	Default = Blank on Voicemail tab/Name on other tabs. The value from this field is used when the **Display** field of the SIP URI being used is set to **Use Internal Data**.
Contact	Default = Blank on Voicemail tab/Extension number on other tabs. The value is used for the `Contact` header when the **Contact** field of the SIP URI being used for a SIP call is set to **Use Internal Data**.
Anonymous	Default = On on Voicemail tab/Off on other tabs. If the `From` field in the SIP URI is set to **Use Internal Data**, selecting this option inserts `Anonymous` into that field rather than the **SIP Name** set above. See Anonymous SIP Calls on page 935.

Related links

Groups on page 229

Chapter 17: Conferences

Call Management > **Conferences**

Systems support system meet-me conferences in addition to the normal ad-hoc and personal conferences.

For full details, see System Conferences on page 700.

Field	Description
Conference ID	Range = Up to 15 digits. This ID is shown in the destination list for auto-attendant actions and incoming call routes. The ID can also be used with short code and programmable button features in order to access the conference. • Do not enter a number that matches a user's extension number. Doing so will override that user's personal meet-me conference facility. • It is advisable not to use conference ID's that are near the range that may be in use for ad-hoc conferences as above (100 plus). Once a conference ID is in use by an ad-hoc conference, it is no longer possible to join the conference using the various conference meet me features.
Name	This is a short name to help indicate the system conferences intended use. For example, "Sales Team".
Moderator List	Optional. Default = No moderators. List the internal users who are moderators for this system conference, up to a maximum of 8 moderators. When set: • The conference **Hold Music** is played to other participants when there is no moderator in the conference. • These user's do not need to enter a PIN in order to access the conference. • Listed users using the User Portal application can view the conference PIN details. In addition: • Other participants, including external participants, can become moderators by entering the **Moderator Pin** when they join the conference. • Conferences with no defined moderators (blank **Moderator List** and no **Moderator Pin**) start immediately any caller joins and can have recording started/stopped by any internal user.

Table continues…

Field	Description
Delegate Pin	Optional. Range = Up to 30 digits. If set, the system will prompt callers, other than those in the **Moderator List** list, to enter a PIN before it allows them to join the conference. The system allows 3 PIN entry attempts before disconnecting the caller.
Moderator Pin	Optional. Range = Up to 30 digits. If set, callers who enter this PIN rather than the **Delegate Pin** are added to the conference as a moderator. This allows moderators who are not in the **Moderator List** including external callers. Note however that external callers will not be able to access moderator controls other than starting/stopping the conference by their presence.
Hold Music	Default = **Tone** If the conference has been configured with moderators, this music is played to other participants who join the conference when no moderator is present. The music is also played if any present moderators leave the conference. • **Tone** – Play repeated system tones to participants whilst waiting for a conference moderator. • **System** – Use the system's default music-on-hold. This option is only shown in a music-on-hold file has been uploaded. • If other music sources have been configured, they can also be selected from the drop-down list. Before the hold music is played, participants will hear a prompt informing them of the reason for hearing the music.
Speech AI	Default = Same as system On subscription systems, this and other text-to-speech options are available if the **System | Voicemail** setting for **Google Speech AI** is enabled. • If set to **Same as System**, the settings of the **System | Voicemail** form are used for TTS prompts. • If set to **Custom**, the **Language** and **Voice** fields below can be used.
Language	Default = Matches the system locale. Set the language used for prompts provided by the system for the system conference.
Voice	Sets the voice to be used with the speech language. The number of voices available varies depending on the speech language selected.
Recording Type	Default = **Manual** Sets the method by which recording of the system conference is controlled: • **Manual** – Recording can be started/stopped by moderators. • **Private** – No recording allowed. • **Automatic** – Automatically start recording the conference when started. The recording can be stopped/restarted by moderators.

Table continues…

Field	Description
Recording Destination	Default = **Conference Mailbox** Sets the destination for system conference recordings. Note that the selected option may also affect the maximum recording length: • **Conference Mailbox** - Place calls into a standard group mailbox, using the conference ID as the mailbox number. Maximum recording length 60 minutes. Message waiting indication and visual voice access can be configured by adding **C**<*conference ID*> to a user's source numbers. • **Conference VRL** - Transfer the conference recordings to the systems VRL application (on subscription systems, set by the **System** > **System** > **Media Archival Solution** setting). Maximum recording length 5 hours.
Meeting Arrival Announcement	Default = Off If enabled, the system plays this prompt to callers before they join the conference. If conference PIN codes have been defined, it is played before the request to the caller to enter their PIN code. • **Audio Output** – Use an uploaded audio file. See .The file must be a .wav file in Mono PCM 16-bit format, either 8, 16 or 22KHz. Maximum length 10 minutes. To upload a file click on **Upload** and select the required file. Alternatively, click and drag the file onto the download box. • **Text-to-Speech** – Use a prompt generated using TTS. Up to 200 characters.

Chapter 18: Auto Attendant (EVM)

Call Management > **Auto Attendants**

These settings cover auto-attendants provided by embedded voicemail on IP500 V2 systems.

For auto-attendants provided by Voicemail Pro, see Voicemail Pro Auto-Attendant Settings on page 659.

For full details on configuration and operation of Embedded Voicemail auto-attendants, refer to the IP Office Embedded Voicemail Installation.

Up to 40 auto-attendant services can be configured. Embedded voicemail services include auto-attendant, callers accessing mailboxes to leave or collect messages and announcements to callers waiting to be answered.

The IP500 V2 supports 2 simultaneous Embedded Voicemail calls by default but can be licensed for up to 6. The licensed limit applies to total number of callers leaving messages, collecting messages and or using an auto attendant.

In addition to basic mailbox functionality, embedded voicemail can also provide auto-attendant operation. Each auto attendant can use existing time profiles to select the greeting given to callers and then provide follow on actions relating to the key presses 0 to 9, * and #.

Time Profiles

Each auto attendant can use up to three existing time profiles, on each for Morning, Afternoon and Evening. These are used to decide which greeting is played to callers. They do not change the actions selectable by callers within the auto attendant. If the time profiles overlap or create gaps, then the order of precedence used is morning, afternoon, evening.

Greetings

Four different greetings are used for each auto attendant. One for each time profile period. This is then always followed by the greeting for the auto-attendant actions. By default a number of system short codes are automatically created to allow the recording of these greetings from a system extension. See below.

Actions

Separate actions can be defined for the DTMF keys 0 to 9, * and #. Actions include transfer to a specified destination, transfer to another auto-attendant transfer to a user extension specified by the caller (dial by number) and replaying the greetings.

- The **Fax** action can be used to reroute fax calls when fax tone is detected by the auto-attendant.
- The **Dial by Name** action can be used to let callers specify the transfer destination.

Short Codes

Adding an auto attendant automatically adds a number of system short codes to assist in recording the auto-attendant prompt. These use the **Auto Attendant** short code feature.

- System short codes (`*81XX`, `*82XX`, `*83XX` and `*84XX`) are automatically added for use with all auto-attendants. These are used for morning, afternoon, evening and menu options greetings respectively. These short codes use a **Telephone Number** of the form `"AA:"N".Y"` where `N` is the replaced with the auto attendant number dialed and `Y` is 1, 2, 3 or 4 for the morning, afternoon, evening or menu option greeting.
- To add a short code to call an auto-attendant, omit the `XX` part. For example, add the short code `*80XX/Auto Attendant/"AA:"N` if internal dialed access to auto-attendants is required.
- System short codes `*800XX`, `*801XX`, ..., `*809XX`, `*850XX`, and `*851XX` are also automatically added for recording prompts for any **Page and Page** actions. The codes correspond to the key to which the action has been assigned; 0 to 9, * and # respectively. These short codes use a **Telephone Number** of the form `"AA:"N".00"`, ..., `"AA:"N".01"`, `"AA:"N".10"` and `"AA:"N".11"` respectively.

Routing Calls to the Auto Attendant

The telephone number format `AA:Name` can be used to route callers to an auto attendant. It can be used in the destination field of incoming call routes and telephone number field of short codes set to the **Auto Attend** feature. Note however that when used with a short code it should be enclosed in quotation marks, that is `"AA:Name"`.

Related links

Auto Attendant settings (EVM) on page 258
Auto Attendant (EVM) on page 259
Actions (EVM) on page 260

Auto Attendant settings (EVM)

Call Management > **Auto Attendant** > **Add Auto Attendant**

Auto-attendants are provided in 2 forms.

- These settings cover auto-attendants provided by embedded voicemail on IP500 V2 systems.
- For auto-attendants provided by Voicemail Pro, see Voicemail Pro Auto-Attendant Settings on page 659.

Related links

Auto Attendant (EVM) on page 257

Auto Attendant (EVM)

Navigation: **Call Management** > **Auto Attendant** > **Add Auto Attendant** > **Auto Attendant**

These settings cover auto-attendants provided by embedded voicemail on IP500 V2 systems. For auto-attendants provided by Voicemail Pro, see Voicemail Pro Auto-Attendant Settings on page 659.

These settings are used to define the name of the auto attendant service and the time profiles that should control which auto attendant greetings are played.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Name	Range = Up to 12 characters, no spaces. This field sets the name for the auto-attendant service. External calls can be routed to the auto attendant by entering AA:Name in the destination field of an Incoming Call Route.
Maximum Inactivity	Default = 8 seconds; Range = 1 to 20 seconds. This field sets how long after playing the prompts the Auto Attendant should wait for a valid key press. If exceeded, the caller is either transferred to the **Fallback Extension** set within the **Incoming Call Route** used for their call or else the caller is disconnected.
Enable Local Recording	Default = On. When off, use of short codes to record auto-attendant prompts is blocked. The short codes can still be used to playback the greetings.
Direct Dial-By-Number	Default = Off. This setting affects the operation of any key presses in the auto attendant menu set to use the **Dial By Number** action. • If selected, the key press for the action is included in any following digits dialed by the caller for system extension matching. For example: If 2 is set in the actions to **Dial by Number**, a caller can dial 201 for extension 201. • If not selected, the key press for the action is not included in any following digits dialed by the caller for system extension matching. For example: If 2 is set in the actions to **Dial by Number**, a caller must dial 2 and then 201 for extension 201.
Dial by Name Match Order	Default = First Name/Last Name. Determines the name order used for the Embedded Voicemail Dial by Name function. The options are: • **First then Last** • **Last then First**
AA Number	This number is assigned by the system and cannot be changed. It is used in conjunction with short codes to access the auto attendant service or to record auto attendant greetings.

Table continues…

Field	Description
Morning/ Afternoon/ Evening/Menu Options	Each auto-attendant can consist of three distinct time periods, defined by associated time profiles. A greeting can be recorded for each period. The appropriate greeting is played to callers and followed by the Menu Options greeting which should list the available actions. The options are: • **Time Profile** The time profile that defines each period of auto-attendant operation. When there are overlaps or gaps between time profiles, precedence is given in the order morning, afternoon and then evening. • **Short code** These fields indicate the system short codes automatically created to allow recording of the time profile greetings and the menu options prompt. • **Recording Name**: Default = Blank. Range = Up to 31 characters. No spaces. This field appears next to the short code used for manually recording auto-attendant prompts. It is only used is using pre-recorded wav files as greeting rather than manually recording greetings using the indicated short codes. If used, note that the field is case sensitive and uses the name embedded within the wav file header rather than the actual file name. This field can be used with all systems supporting Embedded Voicemail. The utility for converting .wav files to the correct format is provided with Manager and can be launched via **File** > **Advanced** > **LVM Greeting Utility**. Files then need to be manually transferred to the Embedded Voicemail memory card. For full details, see the IP Office Embedded Voicemail Installation.

Related links

Auto Attendant (EVM) on page 257

Actions (EVM)

Navigation: **Call Management** > **Auto Attendant** > **Add Auto Attendant** > **Actions**

These settings cover auto-attendants provided by embedded voicemail on IP500 V2 systems. For auto-attendants provided by Voicemail Pro, see Voicemail Pro Auto-Attendant Settings on page 659.

This tab defines the actions available to callers dependent on which DTMF key they press. To change an action, select the appropriate row and click **Edit**. When the key is configured as required click **OK**.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Key	The standard telephone dial pad keys, 0 to 9 plus * and #. The option **Fax** can be used for a transfer to the required fax destination and will then be triggered by fax tone detection. If left as **Not Defined**, fax calls will follow the incoming call routes fallback settings once the auto-attendant Maximum Inactivity Time set on the Auto Attendant | Auto Attendant tab is reached.
Action The following actions can be assigned to each key.	
Centrex Transfer	Used to transfer the incoming call to an external telephone number defined in the **Transfer Number** field. Only supported for calls on Centrex analog trunks. This option is only supported with Embedded Voicemail.
Dial by Name	Callers are asked to dial the name of the user they require and then press #. The recorded name prompts of matching users are then played back for the caller to make a selection. The name order used is set by the **Dial by Name Match Order** setting on the Auto Attendant tab. Note the name used is the user's **Full Name** if set, otherwise their **User Name** is used. Users without a recorded name prompt or set to **Exclude From Directory** are not included. For Embedded Voicemail in IP Office mode, users can record their name by accessing their mailbox and dialing *05. For Embedded Voicemail in Intuity mode, users are prompted to record their name when they access their mailbox.
Dial By Number	This option allows callers with DTMF phones to dial the extension number of the user they require. No destination is set for this option. The prompt for using this option should be included in the auto attendant Menu Options greeting. A uniform length of extension number is required for all users and hunt group numbers. The operation of this action is affected by the auto attendant's Direct Dial-by-Number setting.
Normal Transfer	Can be used with or without a **Destination** set. When the **Destination** is not set, this action behaves as a **Dial By Number** action. With the **Destination** is set, this action waits for a connection before transferring the call. Callers can hear Music on Hold. Announcements are not heard.
Not Defined	The corresponding key takes no action.

Table continues…

Field	Description
Park & Page	The Park & Page feature is supported when the system **Voicemail Type** is designated as **Embedded Voicemail** or **Voicemail Pro**. Park & Page is also supported on systems where **Modular Messaging over SIP** is configured as the central voicemail system and the local **Embedded Voicemail** provides auto attendant operation. The Park & Page feature is an option in user mailboxes where a key is configured with the Park & Page feature. When an incoming call is answered by the voicemail system and the caller dials the DTMF digit for which Park & Page is configured, the caller hears the Park & Page prompt. IP Office parks the call and sends a page to the designated extension or hunt group. When Park & Page is selected in the **Action** drop-down box, the following fields appear: • **Park Slot Prefix –** the desired Park Slot prefix number. Maximum is 8 digits. A 0-9 will be added to this prefix to form a complete Park Slot. • **Retry count –** number of page retries; the range is 0 to 5. • **Retry timeout –** provided in the format M:SS (minute:seconds). The range can be set in 15-second increments. The minimum setting is 15 seconds and the maximum setting is 5 minutes. The default setting is 15 seconds. • **Page prompt –** short code to record the page prompt or upload the recorded prompt. (Prompt can be uploaded to the SD card in the same way the AA prompts are).
Replay Menu Greeting	Replay the auto-attendant greetings again.
Transfer	Transfer the call to the selected destination. This is an unsupervised transfer, if the caller is not answered they will be handled as per a direct call to that number.
Transfer to Attendant	This action can be used to transfer calls to another existing auto attendant.
Destination	Sets the destination for the action. Destination can be a user, a hunt group or a short code. If the destination field is left blank, callers can dial the user extension number that they require. Note however that no prompt is provided for this option so it should be included in the auto attendant Menu Options greeting.
Consent Directive	This field is used to control the addition of a consent value to the system's SMDR output and CTI call logging outputs. The intention is to allow the creation of auto-attendants where having been prompts for consent to some issue, the caller's response is included in the system call logs. It can be set to the following: • Not applicable: Set the consent value in the logging outputs to 0. • Consent Denied: Set the consent value in the logging outputs to 6. • Consent Given: Set the consent value in the logging outputs to 1.

Related links

[Auto Attendant (EVM)](#) on page 257

Chapter 19: Auto Attendants (Voicemail Pro)

Call Management > **Auto Attendants** > /**+Add**

This section describes the auto–attendant settings used by systems using Voicemail Pro. For full details of auto-attendant operation, see Voicemail Pro Auto-Attendants on page 649.

For details of auto-attendants provided by embedded voicemail on IP500 V2 systems, see Auto Attendant (EVM) on page 257.

The auto-attendant settings are split into two tabs.

Tab	Description
Auto Attendants	This tab defines the general settings of the auto-attendant and its greetings and announcements.
Action	This tab defines the functions provided by the individual telephone keys.

Related links

Auto Attendants on page 263
Action on page 267

Auto Attendants

Call Management > **Auto Attendants** > /**+Add** > **Auto Attendants**

These settings are used to define the operation of the auto–attendant service whilst it waits for the caller to select an option from the configured actions.

For a visual summary of how these settings interact, see Auto-Attendant Callflow on page 652.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Auto-Attendant Settings

Field	Description
Name	Range = Up to 12 characters The name for the auto-attendant. Set a name that acts as a reminder of the auto-attendants role. The name is then also shown in other menus used to route calls to the auto-attendant.
AA Number	This number is automatically assigned by the system and cannot be changed. It is used in conjunction with short codes to access the auto–attendant service or to record greetings. See Recording Auto-Attendant Prompts Using Short Codes on page 679. • IP500 V2 systems support up to 40 auto-attendants. • IP Office Server Edition and Select systems support up to 100 auto-attendants.
Maximum Inactivity	Default = 8 seconds; Range = 1 to 20 seconds. This value sets how long the attendant should wait for a response from the caller after playing any current prompts. • If the caller responds, their response is checked for a match to a configured action without any further wait. • Note that the caller can respond whilst the prompts are playing. • If the timeout expires, the **Menu Loop Count** is checked to determine the next steps.
Name Match Order	Default = Last then First This setting sets the name order used for the **Dial By Name** action if used.
Direct By Number	Default = No This setting affects the operation keys set to the **Dial By Number** action. • **If enabled:** The caller's key press to select the action is included in the digits they dial for a extension match. For example, if menu key 2 is used for the action, a caller can dial 2 and then 01 for extension 201. • **If not enabled:** The caller's key press to select the action is not included in the digits they dial for extension match. For example, if menu key 2 is used for the action, a caller must dial 2 and then 201 for extension 201.
Direct By Conference	Default = No This setting affects the operation keys set to the **Dial By Conference** action. • **If enabled:** The caller's key press to select the action is included in the digits they dial for a conference match. For example, if menu key 3 is used for the action, a caller can dial 3 and then 01 for conference 301. • **If not enabled:** The caller's key press to select the action is not included in the digits they dial for a conference match. For example, if menu key 3is used for the action, a caller must dial 3 and then 301 for conference 301.

Table continues…

Field	Description
Enable Local Recording	Default = Yes When off, use of short codes to record auto-attendant prompts is blocked. The short codes can still be used to playback the greetings. See Recording Auto-Attendant Prompts Using Short Codes on page 679.
Speech AI	Default = Off This option is only available on subscription mode systems. It sets whether the auto-attendant supports text-to-speech and automatic speech recognition features. • When off, the auto-attendant does not support any text-to-speech and speech recognition features. - The language used for any prompts provided by the system is determined from the call settings. See Google TTS Prompt Language on page 650. • When set to a specific language, the auto-attendant supports text-to-speech and speech recognition features in that language. - It also uses that language for all system prompts it provides regardless of the locale call settings the system has associated with the call.
Speech Voice	This setting is available when **Speech AI** is set to a specific language. It allows selection of a particular voice used for any text-to-speech features. See Text-to-Speech (TTS) Prompts on page 650.

Greeting and Announcement Settings

When a caller reaches an auto-attendant, they first hear the attendant's current greeting (if any) and then the attendant's menu announcement.

- The greeting used is the first one (from up to 3 defined greetings) for which the greeting's associated time profile is currently active. This allows you to define greetings for different times of day (for example *"Good Morning"*, *"Good Afternoon"* and *"Sorry, we are currently closed"*) or different greetings for business and non-business days.
- The menu announcement should contain the instructions for the caller regarding the keys they can press and other actions.
- Each time a caller goes round the auto-attendant loop, they can respond (with key presses or speech) whilst any greeting and announcement menu prompt is being played.

Field	Description
Optional Greeting 1 **Optional Greeting 2**	Up to 3 greetings can be defined using the **Add Greeting** button. • Each greeting requires an associated time profile. - **Time Profile:** Default = Off *(Greeting not used)*. • If **Off**, the greeting is not used. • The greeting is only used when defined by its associated time profile. • When multiple greetings are defined, the first one that has an active time profile, in the order 1 to 3, is used as the current greeting.

Table continues…

Field	Description
Optional Greeting 3	• If no greetings is currently active according to its time profile, then no greeting is played. • If a greeting is no longer required, it can be deleted by clicking on the adjacent icon. • After playing any greeting, the system always then plays the menu announcement.
Menu Announcement	The menu announcement should contain the instructions for callers about the actions they can perform. For example; "*Press 1 for reception. Press 2 for sales, ...*" It is used as follows: • When a call first reaches the auto-attendant, it is played to the caller after whichever greeting is currently active. • If the **Menu Loop Count** is not zero, it is played again at the start of each repeat loop. • The caller can respond by pressing a key whilst the announcement is being played. On subscription mode systems, if **Speech AI** is enabled they can also respond by speaking whilst the announcement is played. • After the announcement is played, the auto-attendant waits for a response for the time set by the **Maximum Inactivity** setting.
Menu Loop Count	Default = 0 *(No Repeat)* This setting sets the number of times the auto-attendant will repeat the **Menu Announcement** and then wait for a valid response. If the caller does not respond or their response is not matched to an action: • If 0, the default, they hear the **No Match Prompt** prompt and the **Fallback Action** setting is used. • If non-zero but the number of repeat loops has not been reached, they hear the **No Match Prompt** and then the **Menu Announcement** again and the auto-attendant waits for a response again. • If non-zero and the number of repeat loops has been reached, they hear the **No Match Prompt** prompt and the **Fallback Action** setting is used.
No Match Prompt	This prompt is heard when the caller does not respond in time or if their response does not match a configured action. For example; "*Sorry, no response was recognized.*" • Note that this prompt is also heard by callers who are about to be redirected to the **Fallback Action**. Therefore a prompt like "*"Please try again"*" would not be appropriate.

The following settings are common to the menu announcement, greetings and error message. The greetings and announcements can be recorded from the phone, use an uploaded file or be provided by text-to-speech. Whichever method was last used or configured overrides any previous prompt.

Field	Description
Dial To Record Greeting	Default = Automatically assigned. Not changeable. This field indicates the short code that can be dialed in order to record the greeting from an internal extension. See Recording Auto-Attendant Prompts Using Short Codes on page 679.

Table continues…

Field	Description
Audio Output	Default = Audio File The field sets the current method used to provide the prompt used for the greeting or announcement. Clicking on the current value allows you to see its current settings and to change them or to change the recording method. • **Audio File (wav)** – Provide the prompt using a pre-recorded audio file. See Using Pre-Recorded Prompt Files on page 680. • **Text To Speech** – Provide the prompt using the text-to-speech service. This option is only available on subscription mode systems with **Speech AI** enabled and set to a specific language. See Recording Auto-Attendant Prompts Using Text-to-Speech on page 681.

Related links

Auto Attendants (Voicemail Pro) on page 263

Action

Call Management > Auto Attendants > /+Add > Action

This tab defines the actions available to callers dependent on which DTMF key they press or, on subscription mode systems, based on automatic speech recognition of keywords. To change an action, click on the appropriate button.

The **Fallback Action** action applied is the user does not make a recognized choice is configured separately through the **No Match Prompt** prompt settings.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Settings: Keys/Events

The following actions can be assigned to the selected keys.

Action	Description
0 to **9**, *, #	These keys correspond to the standard telephone dial pad key. Clicking on a key allows configuration of its settings.
Fax	If configured, the **Fax** option is used when the system detects fax tone.

Table continues…

Action	Description
Fallback Action	Default = Drop Call This option is used when the number of times the auto-attendant has waited for a valid response from the caller has exceeded the **Menu Loop Count**. It is preceded by the **No Match Prompt** and then the configured action is performed. All actions are supported except **Park & Page**, **Replay Menu Greeting**, **Speak By Name** and **Speak By Number** You can choose whether to mention this option in the **Menu Announcement**. For example, if set to transfer to your receptionist, add "... or wait to for our operator."
Menu Announcement	The menu announcement should contain the instructions for callers about the actions they can perform. For example; "*Press 1 for reception. Press 2 for sales, ...*" It is used as follows: • When a call first reaches the auto-attendant, it is played to the caller after whichever greeting is currently active. • If the **Menu Loop Count** is not zero, it is played again at the start of each repeat loop. • The caller can respond by pressing a key whilst the announcement is being played. On subscription mode systems, if **Speech AI** is enabled they can also respond by speaking whilst the announcement is played. • After the announcement is played, the auto-attendant waits for a response for the time set by the **Maximum Inactivity** setting.

Settings: Key Actions

Action	Description
Not configured	Perform no action.
Dial By Conference	Allow the caller to dial the conference ID they require. See Dial By Conference on page 666.
Dial By Name	Prompt the caller to dial the name of the user they require. See Dial By Name on page 667.
Dial By Number	Allow the caller to dial the extension number they require. See Dial By Number on page 669.
Leave Message	Redirect the caller a specified mailbox to leave a message. See Leave Message on page 670.
Supervised Transfer	Transfer the caller to the specified extension number. See Supervised Transfer on page 671.
Park & Page	Park the call and make an announcement to the a specified group. See Park & Page on page 672.

Table continues…

Action	Description
Replay Menu Greeting	Replay the auto-attendant's menu announcement. See Replay Menu on page 674.
Unsupervised Transfer	Transfers the caller to the specified extension number. See Unsupervised Transfer on page 677.
Transfer To Auto Attendant	Transfers the caller to another auto–attendant. See Transfer to Auto Attendant on page 678.
Speak By Name	Allow the caller to select from listed names using speech. See Speak By Name on page 675.
Speak By Number	Allow the caller to speak the extension number required. See Speak By Number on page 676.
Destination	The destination depends on the action: • **Leave Message**, **Supervised Transfer** and **Unsupervised Transfer** – Use the drop-down to select the target extension. • **Transfer To Auto Attendant** – Use the drop-down to select another existing auto-attendant.
Speech Recognition Keywords	This option is only available on subscription mode systems and when **Speech AI** is set to a specific language. It allows the action to be triggered by speech recognition of keywords. • The keywords must be unique. The same word cannot be used for another key. • Up to 3 keywords are supported per key, separated by commas. Note that using more keywords in total reduces the chances of a match. • Avoid using proper names. These are less likely to be matched as they may not match existing words in the speech recognition dictionaries used by Google. • Encourage matches by ensuring that the keywords are part of the announcements played to callers. For example, "Say whether you want Sales or Support" rather than "Say what department you want".
Consent Directive	When a caller selects a particular action, the actions **Consent Directive** value is included in the system logs. These options allow you record whether the caller has indicated their consent to some action, for example call recording. See Auto-Attendant Consent Example on page 653. • **Consent Not Applicable** – Indicates that the caller has not been prompted to select whether they consent to call recording. • **Consent Given** – Indicates that the caller has been prompted for their consent and has consented. • **Consent Denied** – Indicates that the caller has been prompted for their consent and has not consented.

Related links

Auto Attendants (Voicemail Pro) on page 263

Part 4: The System Settings Menu

System Settings

System Settings

This drop-down provides access to the menus for configuring the features supported by the IP Office telephony service.

- The menus for configuring auto-attendants, conferences, users, groups and extensions are accessed via the **Call Management** menu.

The menu provides access to the configuration records of users, extensions, group, system conferences and auto-attendants. The lists can be used to add, edit and delete those records.

Menu/Sub-Menu	Description
Account Code	Account codes can be used to track calls. Users can either voluntarily enter an account code during a call, or for certain numbers, be forced to enter a valid account code in order to make a call.
Alternate Route Selection	Alternate Route Selection (ARS) records are used to control the routing of outgoing calls. Short codes within the ARS record are matched against the number to dial to see which line to uses or whether it is barred and to change the number actually dialed from the system if necessary.
Authorization Code	Each authorization code is associated with a particular user. That code allows the user to temporarily override the settings of another users phone and make a call from it using their own settings.
Firewall Profile	Configure firewall profiles which can then be applied to IP connections.
Incoming Call Route	Incoming call routes records are used to control the routing of incoming calls. Various aspects of the incoming call (for example the line it is on and the caller ID) are compared for matches to the available ICR records. The destination settings in the ICR record that is the best match are then used to route the call.
IP Route	This menu is used to configure static IP routes to control the routing of matching IP addresses and address ranges.
Licenses	This menu is used to configure the license source settings on non-subscription systems.
Line	Lines are used for external calls, both incoming and outgoing.

Table continues…

Menu/Sub-Menu	Description
Locations	Location records can be used to identify where particular extensions are physically located and to apply settings that need to differ from that location.
RAS	A Remote Access Server (RAS) is a piece of computer hardware which sits on a corporate LAN and into which employees dial on the public switched telephone network to get access to their email and to software and data on the corporate LAN.
Services	Services are used to configure the settings required when a user or device on the LAN needs to connect to a another network. Services can be used when making data connections via trunk or WAN interfaces. Once a service is created, it can be used as the destination for an IP Route record.
Short Codes	Dialing by users on the system can be compared to short codes. When a match occurs, the matching short code sets what should happen. This may be the triggering of some feature, changing a system setting, or changing the dialed number.
Subscription	On subscription mode systems, display the subscriptions obtained and the settings used.
System Directory	The system directory contains records for external contacts, that is their names and numbers. These can be displayed on phones in order to make outgoing calls. They can also be used to match a name to the number on incoming calls.
System	This menu gives access to a set of sub-menus for settings that control system-wide behavior.
Time Profiles	Time profiles contains time, date and weekly schedule settings. Using those each time profile is currently either ‘true’ or ‘false’. That value is used to change the behavior of other types of record that can be linked to the time profile such as incoming call routes.
Tunnel	These menus can be used to create L2TP and IPSec tunnels to other servers and services. Supported on IP Office IP500 V2 systems only.
User Rights	User rights can be used to override some of the individual settings of some users. Changes to the user rights are then automatically applied to all those users rather than having to individually edit each user.
WAN Port	Use these menus to configure physical and virtual WAN ports.

Chapter 20: Account Code

System Settings > **Account Code**

Additional configuration information

This section provides the **Account Code** field descriptions. For additional configuration information, see Configuring Account Codes on page 840.

Account codes are commonly used to control cost allocation and out-going call restriction. The IP Office can use account codes in a number of ways.

- When making calls, users can voluntarily enter an account code.
  - On phones that support programmable buttons, users can do this using an **Account Code Entry** button.
  - A short code set to **Set Account Code** can also be used to enter an account code before making a call.
- If the number dialed for an outgoing call matches a short code set to **Forced Account Code**, the user is required to enter a valid account code in order to continue the call.
- Individual users can be set to **Forced Account Code** (**User** > **Telephony** > **Supervisor Settings**). They then need to enter an account code for any outgoing external calls.
- Incoming calls can also be associated with an account code by matching the Caller ID stored with the account code settings. That account code is then included in the call's SMDR call log.

When an account code is entered during a call:

- The IP Office checks the code entered for a match against those account codes set in its configuration. For **Forced Account Code** calls, the call is not allowed until a valid code is entered.
- If the code is valid, it is included in the information output by the system's SMDR call log.
- The account code used on a call is not included in the user's personal call log. This means that re-dial functions will not re-enter the account code.
- If more than one account code is entered during a call, only the last code entered is included in the SMDR call log.

An IP Office system can support up to 1500 configured account codes.

- Wildcards can be used in the account codes configured to expand the supported range. For example, a single account code entry `9??` allows dialing any number between 900 and 999 to be treated as a valid account code.
- By default, in Server Edition/Select networks, account codes are configured at the network level and automatically replicated in the configuration of all systems in the network. That is, the 1500 account code limit applies to the whole network. They can only be seen and edited

at the individual system configuration level if record consolidation is switched off. See Record Consolidation on page 51.

Bulk delete: You can delete multiple records. Select the check box to the right of each record you want to delete and click **Delete**. You receive a prompt to confirm the deletion.

Related links

Account Code on page 273
Voicemail Recording on page 273

Account Code

Navigation: **System Settings** > **Account Code** > **Add/Edit Account Code** > **Account Code**

These settings can be edited online. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Descriptions
Account Code	Enter the account code required. It can also include wildcards; **?** matches a single digit and ***** matches any digits.
Caller ID	A caller ID can be entered and used to automatically assign an account code to calls made to or received from caller ID.

Related links

Account Code on page 272

Voicemail Recording

Navigation: **System Settings** > **Account Code** > **Add/Edit Account Code** > **Voicemail Recording**

These settings are used to activate the automatic recording of external calls when the account code is entered at the start of the call.

- Call recording requires Voicemail Pro to be installed and running. Call recording also requires available conference resources similar to a 3-way conference.
- Call recording starts when the call is answered.
- Call recording is paused when the call is parked or held. It restarts when the call is unparked or taken off hold. This does not apply to SIP terminals.
- Calls to and from IP devices, including those using Direct media, can be recorded.

- Recording continues for the duration of the call or up to the maximum recording time configured on the voicemail server.
- Recording is stopped when the call ends or if:
  - User call recording stops if the call is transferred to another user.
  - Account code call recording stops if the call is transferred to another user.
  - Hunt group call recording stops if the call is transferred to another user who is not a member of the hunt group.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Description
Record Outbound	Default = None Select whether automatic recording of outgoing calls is enabled. The Auto Record Calls option sets whether just external calls or external and internal calls are included. The options are: • **None**: Do not automatically record calls. • **On**: Record the call if possible. Otherwise, allow the call to continue without recording. • **Mandatory**: Record the call if possible. Otherwise, block the call and return busy tone. • **Percentages of calls**: Record a selected percentages of the calls.
Record Time Profile	Default = <None> (Any time) Used to select a time profile during which automatic call recording of incoming calls is applied. If no profile is selected, automatic recording is always active.
Recording (Auto)	Default = Mailbox Sets the destination for automatically triggered recordings. The options are: • **Mailbox** This option sets the destination for the recording to be a selected user or hunt group mailbox. The adjacent drop down list is used to select the mailbox. • **Voice Recording Library**: This option set the destination for the recording to be a VRL folder on the voicemail server. The VRL application polls that folder and collects waiting recordings which it then places in its archive. Recording is still done by Voicemail Pro. • **Voice Recording Library Authenticated**: This option is similar to the above but instructs the voicemail server to create an authenticated recording. If the file contents are changed, the file is invalidated though it can still be played. - For systems recording to `.opus` format (the default), both settings create authenticated recordings.

Related links

Account Code on page 272

Chapter 21: Alternate Route Selection

System Settings > **Alternate Route Selection**

Alternate Route Selection (ARS) records are used to control the routing of outgoing calls. Short codes within the ARS record are matched against the number to dial to see which line to uses or whether it is barred and to change the number actually dialed from the system if necessary.

Click **Add/Edit Alternate Route** to open the Create Alternate Route page where you can provision a location. When you click **Add/Edit Alternate Route**, you are prompted to specify a server.

Related links

Add Alternate Route on page 275

Add Alternate Route

Navigation: **System Settings** > **Alternate Route Selection** > **Add/Edit Alternate Route**

Additional configuration information

See Configuring ARS on page 809.

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 806.

Configuration settings

Each ARS form contains short codes which are used to match the result of the short code that triggered use of the ARS form, ie. the Telephone Number resulting from the short code is used rather than the original number dialed by the user.

For Server Edition, this type of configuration record can be saved as a template and new records created from a template.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
ARS Route ID	The default value is automatically assigned. Range = 0 to 99999. For most deployments, do not edit this field. For those conditions where it is necessary to edit this field, the value must be unique within ARS and within the line Outbound Group IDs.

Table continues…

Field	Description
Route Name	Default = Blank. Range = Up to 15 characters. The name is used for reference and is displayed in other areas when selecting which ARS to use.
Dial Delay Time	Default = System. Range = 1 to 30 seconds. This settings defines how long ARS should wait for further dialing digits before assuming that dialing is complete and looking for a short code match against the ARS form short codes. When set to **System**, the system setting **System Settings** > **System** > **Telephony** > **Dial Delay Time** is used.
Secondary Dial Tone	Defaults = Off. When on, this setting instructs the system to play secondary dial tone to the user. The tone used is set by the field below. The tone used is set as either **System Tone** (normal dial tone) or **Network Tone** (secondary dial tone). Both tone types are generated by the system in accordance with the system specific locale setting. Note that in some locales normal dial tone and secondary dial tone are the same. When **Secondary Dial Tone** is selected, the ARS form will return tone until it receives digits with which it can begin short code matching. Those digits can be the result of user dialing or digits passed by the short code which invoked the ARS form. For example with the following system short codes: In this example, the 9 is stripped from the dialed number and is not part of the telephone number passed to the ARS form. So in this case secondary dial tone is given until the user dials another digit or dialing times out. • **Code**: 9N • **Telephone Number**: N • **Line Group ID**: 50 Main In this example, the dialed 9 is included in the telephone number passed to the ARS form. This will inhibit the use of secondary dial tone even if secondary dial tone is selected on the ARS form. • **Code**: 9N • **Telephone Number**: 9N • **Line Group ID**: 50 Main
Check User Call Barring	Default = Off If enabled, the dialing user's **Outgoing Call Bar** setting and any user short codes set to the function **Barred** are checked to see whether they are appropriate and should be used to bar the call.
Description	Default = Blank. Maximum 31 characters. You can use this field to enter a description for the configuration entry. The description is not used elsewhere.

Table continues…

Field	Description
In Service:	Default = On This field is used to indicate whether the ARS form is in or out of service. When out of service, calls are rerouted to the ARS form selected in the **Out of Service Route** field. Short codes can be used to take an ARS form in and out of service. This is done using the short code features Disable ARS Form and Enable ARS Form and entering the ARS Route ID as the short code **Telephone Number** value.
Out of Service Route	Default = None. This is the alternate ARS form used to route calls when this ARS form is not in service.
Time Profile	Default = None. Use of a ARS form can be controlled by an associate time profile. Outside the hours defined within the time profile, calls are rerouted to an alternate ARS form specified in the Out of Hours Route drop-down. Note that the Time Profile field cannot be set until an Out of Hours Route is selected.
Out of Hours Route	Default = None. This is the alternate ARS form used to route calls outside the hours defined within the Time Profile selected above.
Short Codes	Short codes within the ARS form are matched against the "Telephone Number" output by the short code that routed the call to ARS. The system then looks for another match using the short codes with the ARS form. Only short codes using the following features are supported within ARS: **Dial**, **Dial Emergency**, **Dial Speech**, **Dial 56K**, **Dial64K**, **Dial3K1**, **DialVideo**, **DialV110**, **DialV120** and **Busy**. Multiple short codes with the same **Code** field can be entered so long as they have differing **Telephone Number** and or **Line Group ID** settings. In this case when a match occurs the system will use the first match that points to a route which is available.
Alternate Route Priority	Default = 3. Range = 1 (low) to 5 (high). If the routes specified by this form are not available and an **Alternate Route** has been specified, that route will be used if the users priority is equal to or higher than the value set here. User priority is set through the **Call Management** > **Users** > **Add/Edit Users** > **User** form and by default is **5**. If the users priority is lower than this value, the **Alternate Route Wait Time** is applied. This field is grayed out and not used if an ARS form has not been selected in the **Alternate Route** field. If the caller's dialing matches a short code set to the **Barred** function, the call remains at that short code and is not escalated in any way.
Alternate Route Wait Time	Default = 30 seconds. Range = Off, 5 to 60 seconds. If the routes specified by this form are not available and an **Alternate Route** has been specified, users with insufficient priority to use the alternate route immediately must wait for the period defined by this value. During the wait the user hears camp on tone. If during that period a route becomes available it is used. This field is grayed out and not used if an ARS form has not been selected in the Alternate Route field.

Table continues…

Field	Description
Alternate Route	Default = None. This field is used when the route or routes specified by the short codes are not available. The routes it specifies are checked in addition to those in this ARS form and the first route to become available is used.

Cause Codes and ARS

ARS routing to digital trunks can be affected by signalling from the trunk.

The following cause codes cause ARS to no longer target the line group (unless it is specified by an alternate ARS route). The response to cause codes received from the line is as follows.

Code	Cause Code
1	Unallocated Number.
2	No route to specific transit network/(5ESS) Calling party off hold.
3	No route to destination./(5ESS) Calling party dropped while on hold.
4	Send special information tone/(NI-2) Vacant Code.
5	Misdialed trunk prefix.
8	Preemption/(NI-2) Prefix 0 dialed in error.
9	Preemption, cct reserved/ (NI-2) Prefix 1 dialed in error.
10	(NI-2) Prefix 1 not dialed.
11	(NI-2) Excessive digits received call proceeding.
22	Number Changed.
28	Invalid Format Number.
29	Facility Rejected.
50	Requested Facility Not Subscribed.
52	Outgoing calls barred.
57	Bearer Capability Not Authorized.
63	Service or Option Unavailable.
65	Bearer Capability Not Implemented.
66	Channel Type Not Implemented.
69	Requested Facility Not Implemented.
70	Only Restricted Digital Information Bearer Capability Is Available.
79	Service Or Option Not Implemented.
88	Incompatible.
91	Invalid Transit Network Selection.
95	Invalid Message.
96	Missing Mandatory IE.
97	Message Type Nonexistent Or Not Implemented.

Table continues…

Code	Cause Code
98	Message Not Implemented.
99	Parameter Not Implemented.
100	Invalid IE Contents.
101	Msg Not Compatible.
111	Protocol Error.
127	Interworking Unspecified.

Stop ARS The following cause codes stop ARS targeting completely.

Code	Cause Code
17	Busy.
21	Call Rejected.
27	Destination Out of Order.

No Affect All other cause codes do not affect ARS operation.

Related links

Alternate Route Selection on page 275

Chapter 22: Authorization Code

System Settings > **Authorization Code**

Each authorization code is associated with a particular user. That code allows the user to temporarily override the settings of another users phone and make a call from it using their own settings.

Click **Add/Edit Authorization Code** to open the Authorization Codes page where you can provision an authorization code. When you click **Add/Edit Authorization Code**, you are prompted to specify the server where the authorization code will be applied.

Related links

Add Authorization Code on page 280

Add Authorization Code

Navigation: **System Settings** > **Authorization Code** > **Add/Edit Authorization Code**

When a user dials an external number that matches a short code set to **Force Authorization Code**, the IP Office system will prompt the user to enter their associated **Authorization Code** before allowing the call to continue.

Valid/invalid authorization code entry is recorded in the SMDR output. The code used is not recorded.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

Note:

For Release 9.1 and higher, you can no longer associate **Authorization Code** entries with **User Rights**. **Authorization Code** configured in that way are removed during the upgrade.

Field	Description
Authorization Code	Range = Up to 12 digits. The digits used for the authorization code. Each code must be unique. Wildcards are not usable with authorization codes.
User	This field is used to select a user with which the authorization code is associated. The authorization code can then be used to authorize calls made by that user.

Related links

Authorization Code on page 280

Chapter 23: Firewall Profile

System Settings > **Firewall Profile**

Configure firewall profiles which can then be applied to IP connections.

Click **Add/Edit Firewall Profile** to open the Add Firewall page where you can provision a firewall. When you click **Add/Edit Firewall Profile**, you are prompted to specify the server where the firewall will be applied.

Related links

Add Firewall Profile on page 281

Add Firewall Profile

Navigation: **System Settings** > **Firewall Profile** > **Add/Edit Firewall Profile**

Additional configuration information

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 806.

Configuration settings

The IP Office system can act as a firewall, allowing only specified data traffic to start a session across the firewall and controlling in which direction such sessions can be started.

You can select a firewall profiles for the following areas of IP Office operation:

- You can apply a firewall profile to traffic between LAN1 and LAN2.
- You can select a firewall for users who are the destination of incoming RAS calls.
- You can select a firewall when you configure a service.

Note:

- The IP Office firewall profiles can include Static network address translation (NAT) records. If the firewall profile contains any Static NAT records, the IP Office blocks traffic that does not match one of those static NAT records.
- If Network Address Translation (NAT) is used with the firewall, you must configure the **Primary Trans. IP Address** setting on incoming services (**System Settings** > **Services** > **Add/Edit Service** > **Normal / WAN / Internet**).

- On Linux-based systems, to ensure that the firewall starts after a reboot, you must enable the **Solution** > ☰ > **Platform View** > **Settings** > **System** > **Firewall Settings** > **Activate**option.

By default, any protocol not listed in the standard firewall list is dropped unless a custom firewall entry is configured for that protocol.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

Field	Description		
Name	Range = Up to 15 characters. Enter the name to identify this profile.		
Protocol Control	For each of the listed protocols, the options **Drop**, **In** (Incoming traffic can start a session), **Out** (Outgoing traffic can start a session) and **Both Directions** can be selected. Once a session is started, return traffic for that session is also able to cross the firewall.		
	Protocol	**Default**	**Description**
	TELNET	Out	Remote terminal log in.
	FTP	Out	File Transfer Protocol.
	SMTP	Out	Simple Mail Transfer Protocol.
	TIME	Out	Time update protocol.
	DNS	Out	Domain Name System.
	GOPHER	Drop	Internet menu system.
	FINGER	Drop	Remote user information protocol.
	RSVP	Drop	Resource Reservation Protocol.
	HTTP/S	Bothway	Hypertext Transfer Protocol.
	POP3	Out	Post Office Protocol.
	NNTP	Out	Network News Transfer Protocol.
	SNMP	Drop	Simple Network Management Protocol.
	IRC	Out	Internet Relay Chat.
	PPTP	Drop	Point to Point Tunneling Protocol.
	IGMP	Drop	Internet Group Membership Protocol.
Service Control	For each of the listed services, the options **Drop**, **In**, **Out** and **Both Directions** can be selected. Once a session is started, return traffic for that session is also able to cross the firewall.		
	Protocol	**Default**	**Description**
	SSI	In	System Status Application access.
	SEC	Drop	TCP security settings access.
	CFG	Drop	TCP configuration settings access.
	TSPI	In	TSPI service access.
	WS	Drop	IP Office web management services.

Related links

Firewall Profile on page 281

Chapter 24: Incoming Call Route

System Settings > **Incoming Call Route**

Incoming call routes records are used to control the routing of incoming calls. Various aspects of the incoming call (for example the line it is on and the caller ID) are compared for matches to the available ICR records. The destination settings in the ICR record that is the best match are then used to route the call.

- Click **Add/Edit Incoming Call Route** to add an incoming call route. When you click **Add/Edit Incoming Call Route**, you are prompted to specify a server where the route will be configured.
- Click **MSN Configuration** to populate the incoming call route table with MSN or DID numbers. When you click **MSN Configuration**, you are prompted to specify a server.

Related links

Add Incoming Call Route on page 283
Incoming Call Route MSN Configuration on page 293

Add Incoming Call Route

Navigation: **System Settings** > **Incoming Call Route** > **Add/Edit Incoming Call Route**

Incoming call routes are used to determine the destination of voice and data calls received by the system. On systems where a large number incoming call routes need to be setup for DID numbers, the MSN/DID Configuration tool can be used.

Calls received on IP, S0 and QSIG trunks do not use incoming call routes. Routing for these is based on incoming number received as if dialed on-switch. Line short codes on those trunks can be used to modify the incoming digits.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Determining which incoming call route is used is based on the call matching a number of possible criteria. In order of highest priority first, the criteria, which if set must be matched by the call in order for the call to use that route are:

1. The **Bearer Capability** indicated, if any, with the call. For example whether the call is a voice, data or video call.
2. The **Incoming Group ID** of the trunk or trunk channel on which the call was received.
3. The **Incoming Number** received with the call.

4. The **Incoming Sub Address** received with the call.
5. The **Incoming CLI** of the caller.

Multiple Matches

If there is a match between more than one incoming call route record, the one added to the configuration first is used.

Incoming Call Route Destinations

Each incoming route can include a fallback destination for when the primary destination is busy. It can also include a time profile which control when the primary destination is used. Outside the time profile calls are redirected to a night service destination. Multiple time profiles can be associated with an incoming call route. Each time profile used has its own destination and fallback destination specified.

Incoming Call Routing Examples

Example 1

For this example, the customer has subscribes to receive two 2-digit DID numbers. They want calls on one routed to a Sales hunt group and calls on the other to a Services hunt group. Other calls should use the normal default route to hunt group Main. The following incoming call routes were added to the configuration to achieve this:

Line Group	Incoming Number	Destination
0	77	Sales
0	88	Services
0	blank	Main

Note that the incoming numbers could have been entered as the full dialed number, for example 7325551177 and 7325551188 respectively. The result would still remain the same as incoming number matching is done from right-to-left.

Line Group	Incoming Number	Destination
0	7325551177	Sales
0	7325551188	Services
0	blank	Main

Example 2

In the example below the incoming number digits 77 are received. The incoming call route records 677 and 77 have the same number of matching digit place and no non-matching places so both a potential matches. In this scenario the system will use the incoming call route with the Incoming Number specified for matching.

Line Group	Incoming Number	Destination
0	677	Support
0	77	Sales
0	7	Services
0	blank	Main

Example 3

In the following example, the 677 record is used as the match for 77 as it has more matching digits than the 7 record and no non-matching digits.

Line Group	Incoming Number	Destination
0	677	Support
0	7	Services
0	blank	Main

Example 4

In this example the digits 777 are received. The 677 record had a non-matching digit, so it is not a match. The 7 record is used as it has one matching digit and no non-matching digits.

Line Group	Incoming Number	Destination
0	677	Support
0	7	Services
0	blank	Main

Example 5

In this example the digits 77 are received. Both the additional incoming call routes are potential matches. In this case the route with the shorter Incoming Number specified for matching is used and the call is routed to **Services**.

Line Group	Incoming Number	Destination
0	98XXX	Support
0	8XXX	Services
0	blank	Main

Example 6

In this example two incoming call routes have been added, one for incoming number 6XXX and one for incoming number 8XXX. In this case, any three digit incoming numbers will potential match both routes. When this occurs, potential match that was added to the system configuration first is used. If 4 or more digits were received then an exact matching or non-matching would occur.

Line Group	Incoming Number	Destination
0	6XXX	Support
0	8XXX	Services
0	blank	Main

Related links

Incoming Call Route on page 283
Incoming Call Route General Settings on page 286
Incoming Call Route Voice Recording on page 289
Incoming Call Route Destinations on page 291

Incoming Call Route General Settings

Navigation: **System Settings** > **Incoming Call Route** > **Add/Edit Incoming Call Route**

Additional configuration information

For additional information on the **Tag** setting, see Call Tagging on page 837.

Incoming call routes are used to match call received with destinations. Routes can be based on the incoming line group, the type of call, incoming digits or the caller's ICLID. If a range of MSN/DID numbers has been issued, this form can be populated using the MSN Configuration tool. In Manager, see **Tools** > **MSN Configuration**.

Default Blank Call Routes

By default the configuration contains two incoming calls routes; one set for **Any Voice** calls (including analog modem) and one for **Any Data** calls. While the destination of these default routes can be changed, it is strongly recommended that the default routes are not deleted.

- Deleting the default call routes, may cause busy tone to be returned to any incoming external call that does not match any incoming call route.
- Setting any route to a blank destination field, may cause the incoming number to be checked against system short codes for a match. This may lead to the call being rerouted off-switch.

Calls received on IP, S0 and QSIG trunks do not use incoming call routes. Routing for these is based on incoming number received as if dialed on-switch. Line short codes on those trunks can be used to modify the incoming digits.

If there is no matching incoming call route for a call, matching is attempted against system short codes and finally against voicemail nodes before the call is dropped.

SIP Calls

For SIP calls, the following fields are used for call matching:

- **Line Group ID** This field is matched against the **Incoming Group** settings of the SIP URI (Line | SIP URI). This must be an exact match.
- **Incoming Number** This field can be used to match the called details (TO) in the SIP header of incoming calls. It can contain a number, SIP URI or Tel URI. For SIP URI's the domain part of the URI is removed before matching by incoming call routing occurs. For example, for the SIP URI mysip@example.com , only the user part of the URI, ie. mysip, is used for matching.

The Call Routing Method setting of the SIP line can be used to select whether the value used for incoming number matching is taken from the **To Header** or the **Request URI** information provided with incoming calls on that line.

Incoming CLI This field can be used to match the calling details (FROM) in the SDP header of incoming SIP calls. It can contain a number, SIP URI, Tel URI or IP address received with SIP calls. For all types of incoming CLI except IP addresses a partial record can be used to achieve the match, records being read from left to right. For IP addresses only full record matching is supported.

Configuration Settings

These settings can be edited online. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Incoming Call Matching Fields:

The following fields are used to determine if the Incoming Call Route is a potential match for the incoming call. By default the fields are used for matching in the order shown starting with **Bearer Capability**.

Field	Description
Line Group ID	Default = 0. Range = 0 to 99999. Matches against the Incoming Line Group to which the trunk receiving the call belongs. For Server Edition systems, the default value **0** is not allowed. You must change the default value and enter the unique **Line Group ID** for the line.
Incoming Number	Default = Blank (Match any unspecified) Matches to the digits presented by the line provider. A blank record matches all calls that do not match other records. By default this is a right-to-left matching. The options are: • *** = Incoming CLI Matching Takes Precedence** • **– = Left-to-Right Exact Length Matching** Using a **-** in front of the number causes a left-to-right match. When left-to-right matching is used, the number match must be the same length. For example -96XXX will match a DID of 96000 but not 9600 or 960000. • **X = Single Digit Wildcard** Use **X**'s to enter a single digit wild card character. For example **91XXXXXXXX** will only match DID numbers of at least 10 digits and starting with 91, **-91XXXXXXXX** would only match numbers of exactly 10 digits starting with 91. Other wildcard such as **N**, **n** and **?** cannot be used. Where the incoming number potentially matches two incoming call routes with X wildcards and the number of incoming number digits is shorter than the number of wildcards, the one with the shorter overall **Incoming Number** specified for matching is used. • **i = ISDN Calling Party Number 'National'** The **i** character does not affect the incoming number matching. It is used for Outgoing Caller ID Matching, see notes below.

Table continues…

Field	Description
Incoming CLI	Default = Blank (Match all) Enter a number to match the caller's number (ICLID) provided with the call. This field is matched left-to-right. The number options are: • Full telephone number. • Partial telephone number, for example just the area code. • `!` : Matches calls where the ICLID was withheld. • `?` : for number unavailable. • For SIP call on a line using calling number verification, the characters `P`, `F` and `Q` can be used to match calls that have passed authentication, failed authentication or were unauthenticated respectively. See SIP Calling Number Verification (STIR/SHAKEN) on page 963. • Blank for all.

Call Setting Fields:

For calls routed using this Incoming Call Route, the settings of the following fields are applied to the call regardless of the destination.

Field	Description
Locale	Default = Blank (Use system setting) This option specifies the language prompts, if available, that voicemail should use for the call if it is directed to voicemail.
Priority	Default = 1-Low. Range = 1-Low to 3-High. This setting allows incoming calls to be assigned a priority. Other calls such as internal calls are assigned priority **1-Low** In situations where calls are queued, high priority calls are placed before calls of a lower priority. This has a number of effects: • Mixing calls of different priority is not recommended for destinations where Voicemail Pro is being used to provided queue ETA and queue position messages to callers since those values will no longer be accurate when a higher priority call is placed into the queue. Note also that Voicemail Pro will not allow a value already announced to an existing caller to increase. • If the addition of a higher priority call causes the queue length to exceed the hunt group's Queue Length Limit, the limit is temporarily raised by 1. This means that calls already queued are not rerouted by the addition of a higher priority call into the queue. A timer can be used to increase the priority of queued calls, see the setting **System | Telephony | Telephony | Call Priority Promotion TimeSystem Settings** > **System** > **Telephony** > **Call Priority Promotion Time**. The current priority of a call can be changed through the use of the **p** short code character in a short code used to transfer the call.

Table continues…

Field	Description
Tag	Default = Blank (No tag). Allows a text tag to be associated with calls routed by this incoming call route. This tag is displayed with the call within applications and on phone displays.
Hold Music Source	Default = System source. The system can support several music on hold sources. See **System Settings** > **System** > **Telephony** > **Tones and Music**. If the system has several hold music sources available, this field allows selection of the source to associate with calls routed by this incoming call route. The new source selection will then apply even if the call is forwarded or transferred away from the Incoming Call Route destination. If the call is routed to another system in a multi-site network, the matching source on that system is used if available. The hold music source associated with a call can also be changed by a hunt group's Hold Music Source setting.
Ring Tone Override	Default = Blank If ring tones have been configured in **System Settings** > **System** > **Telephony** > **Ring Tones**, they are available in this list. Setting a ring tone override applies a unique ring tone for the incoming call route. Ring tone override features are only supported on 1400 Series, 9500 Series and J100 Series (except J129) phones.

Outgoing Caller ID Matching

In cases where a particular Incoming Number is routed to a specific individual user, the system will attempt to use that Incoming Number as the user's caller ID when they make outgoing calls if no other number is specified. This requires that the Incoming Number is a full number suitable for user as outgoing caller ID and acceptable to the line provider.

When this is the case, the character **i** can also be added to the Incoming Number field. This character does not affect the incoming call routing. However when the same Incoming Number is used for an outgoing caller ID, the calling party number plan is set to ISDN and the type is set to National. This option may be required by some network providers.

For internal calls being forwarded or twinned, if multiple incoming call route entries match the extension number used as caller ID, the first entry created is used. This entry should start with a “-” character (meaning fixed length) and provide the full national number. These entries do not support wildcards. If additional entries are required for incoming call routing, they should be created after the entry required for reverse lookup.

Related links

Add Incoming Call Route on page 283

Incoming Call Route Voice Recording

Navigation: **System Settings** > **Incoming Call Route** > **Add/Edit Incoming Call Route**

These settings are used to activate the automatic recording of incoming calls that match the incoming call route.

- Call recording requires Voicemail Pro to be installed and running. Call recording also requires available conference resources similar to a 3-way conference.

- Call recording starts when the call is answered.
- Call recording is paused when the call is parked or held. It restarts when the call is unparked or taken off hold. This does not apply to SIP terminals.
- Calls to and from IP devices, including those using Direct media, can be recorded.
- Recording continues for the duration of the call or up to the maximum recording time configured on the voicemail server.
- Recording is stopped when the call ends or if:
  - User call recording stops if the call is transferred to another user.
  - Account code call recording stops if the call is transferred to another user.
  - Hunt group call recording stops if the call is transferred to another user who is not a member of the hunt group.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Record Inbound	Default = None Select whether automatic recording of incoming calls is enabled. The options are: • **None**: Do not automatically record calls. • **On**: Record the call if possible. Otherwise, allow the call to continue without recording. • **Mandatory**: Record the call if possible. Otherwise, block the call and return busy tone. • **Percentages of calls**: Record a selected percentages of the calls.
Record Time Profile	Default = <None> (Any time) Used to select a time profile during which automatic call recording of incoming calls is applied. If no profile is selected, automatic recording is always active.
Recording (Auto)	Default = Mailbox Sets the destination for automatically triggered recordings. The options are: • **Mailbox** This option sets the destination for the recording to be a selected user or hunt group mailbox. The adjacent drop down list is used to select the mailbox. • **Voice Recording Library**: This option set the destination for the recording to be a VRL folder on the voicemail server. The VRL application polls that folder and collects waiting recordings which it then places in its archive. Recording is still done by Voicemail Pro. • **Voice Recording Library Authenticated**: This option is similar to the above but instructs the voicemail server to create an authenticated recording. If the file contents are changed, the file is invalidated though it can still be played. - For systems recording to `.opus` format (the default), both settings create authenticated recordings.

Related links

Add Incoming Call Route on page 283

Incoming Call Route Destinations

Navigation: **System Settings** > **Incoming Call Route** > **Add/Edit Incoming Call Route**

The system allows you to associate multiple time profiles with an incoming call route. For each time profile, you can specify separate Destination and Fallback Extension settings.

When you add multiple records, the IP Office looks for the first time profile match starting from the bottom up. If the IP Office does not find a match, it uses the Default Value destinations. Once the IP Office makes a match, it does not use any other destinations.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

- For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Description
Time Profile	This column is used to specify the time profiles used by the incoming call route. The drop-down list display existing time profiles from you can make a selection. To remove an existing entry, select it by clicking on the button on the left of the row, then right-click on the row and select **Delete**. • The **Default Value** entry is used if no match to a time profile occurs.

Table continues…

Field	Description
Destination	Default = Blank Either enter the destination manually or select the destination from the drop-down list. The following options appear in the drop-down list: • **Voicemail** allows remote mailbox access with voicemail. Callers are asked to enter the extension ID of the mailbox required and then the mailbox access code. • Local user names. • Local hunt groups names. • **AA**: **Name** directs calls to an Embedded Voicemail auto-attendant services. In addition to short codes, extension and external numbers, you can manually enter the following options: • **VM:Name** Directs calls to the matching start point in Voicemail Pro. • A **.** matches the Incoming Number field. This can be used even when X wildcards are being used in the Incoming Number field. • A **#** matches all **X** wildcards in the **Incoming Number** field. For example, if the Incoming Number was -91XXXXXXXXXX, the **Destination** of # would match XXXXXXXXXX. • Text and number strings entered here are passed through to system short codes, for example to direct calls into a conference. Note that not all short code features are supported. • You must use quote marks where necessary to stop characters in the destination string being interpreted as special characters.
Fallback Extension	Default = Blank (No fallback) Defines an alternate destination which the IP Office should use when the **Destination** cannot accept new calls and has no coverage settings to redirect calls. For example: • For an extension as the destination:, use the fallback if: - The target extension has no more call appearance buttons available and does not have voicemail on. - The target extension is logged out. - The target extension is set to 'do not disturb' and does not have voicemail on. - The target extension has been unplugged and has no voicemail. • Not supported for analog extensions. • For IP extensions, there is a 3-minute delay before the extension is unregistered from the IP Office during which the IP Office still attempts to present new calls to the extension. • For a hunt group as the destination:, use the fallback if: - The hunt group members are all busy and the group does not have queuing and voicemail enabled.

Related links

Add Incoming Call Route on page 283

Incoming Call Route MSN Configuration

Navigation: **System Settings** > **Incoming Call Route** > **MSN Configuration**

Used to populate the **Incoming Call Route** table with a range of MSN or DID numbers.

Setting	Description
MSN/DID	The first number in the set of MSN numbers for which you have subscribed. **Note:** If you require to find an exact match between the MSN numbers and the destination numbers, enter a minus (-) sign before the first MSN number.
Destination	Where incoming calls with matching digits should be routed. The drop-down list contains the extensions and groups on the system.
Line Group ID	Specifies the incoming line group ID of the trunks to which the DID routing is applied.
Presentation Digits	Set to match the number of digits from the MSN/DID number that the central office exchange will actually present to the system.
Range	How many MSN or DID number routes to create in sequence using the selected MSN/DID and Destination as start points. Only routing to user extensions is supported when creating a range of records.

Related links

Incoming Call Route on page 283

Chapter 25: IP Route

System Settings > **IP Route**

This menu is used to configure static IP routes to control the routing of matching IP addresses and address ranges.

For additional configuration information, see Configuring IP Routes on page 744.

Main content pane

The **IP Route** main content pane lists provisioned IP routes. The contents of the list depends on the filter options selected. Click the icons beside a route to edit or delete.

Bulk delete: You can delete multiple records. Select the check box to the right of each record you want to delete and click **Delete**. You receive a prompt to confirm the deletion.

Click **Add/Edit IP Route** to open the Add IP Route window where you can provision a location. When you click **Add/Edit IP Route**, you are prompted to specify a server.

Related links

Add IP Route on page 294

Add IP Route

Navigation: **System Settings** > **IP Route** > **Add/Edit IP Route**

Additional configuration information

For additional configuration information, see Configuring IP Routes on page 744.

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 806.

Configuration settings

You can use these settings to setup static IPv4 routes for the IP Office system. The IP Office supports up to 100 static, dynamic, and internal routes.

Warning:

- The 'on-boarding' process (see the Deploying Avaya IP Office™ Platform SSL VPN Services manual) can automatically add a static route to an SSL VPN service when the on-boarding file is uploaded to the IP Office system. Do not delete or amend that route except when advised to by Avaya.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
IP Address	The IP address to match for ongoing routing. The IP Office routes any packets matching the **IP Address** and **IP Mask** settings to the configured **Destination**. • When left blank, the address 255.255.255.255 (all) is used.
IP Mask	The subnet mask used to mask the **IP Address** for ongoing route matching. • If blank, the mask used is 255.255.255.255 (all). • A **0.0.0.0** entry in the **IP Address** and **IP Mask** fields routes all packets for which there is no other specific **IP Route** available. The Default Route option with Services can be used to do this if a blank IP route is not added.
Gateway IP Address	Default = Blank The address of the gateway to which the IP Office sends packets that match the route. • If left blank or set to **0.0.0.0**, then all packets are sent to the **Destination** specified. This is normally only used to forward packets to another router on the local LAN.
Destination	Select **LAN1**, **LAN2**, any configured **Service**, or any **Tunnel** (**L2TP** only).
Metric:	Default = 0 The number of "hops" this route counts as.
Proxy ARP	Default = Off This allows the IP Office system to respond on behalf of this IP address when receiving an ARP request.

Related links

IP Route on page 294

Chapter 26: Licenses

System Settings > **Licenses**

This menu is used to configure the license source settings on non-subscription systems.

Note:

This section is not applicable to systems running in subscription mode.

For additional configuration information, see the following.

- Applying Licenses on page 790.
- Converting from Nodal Licensing to Centralized Licensing on page 803
- Migrating ADI Licenses to PLDS on page 804
- “Licenses” in Avaya IP Office™ Platform Solution Description.

Main content pane

Clicking **System Settings** > **Licenses** opens the Systems page with a list of all IP Office systems. Click on the three bar menu icon to the right of a system to view the licensing information for that system.

Related links

License on page 296
Remote Server on page 299

License

Navigation: **System Settings** > **Licenses** > **Server Menu** > **Manage Licenses**

These settings can be edited online. Changes to these settings do not require a reboot of the system.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>License Mode</td><td>Identifies the status of the system licenses. The two license configuration types are nodal and WebLM. Nodal licenses are licenses that are present on the system. WebLM licenses means licenses obtained from the WebLM server.

The possible states are:
• Normal Mode Normal nodal licensing mode. In this mode, WebLM is not configured and only nodal licensing is allowed.
• Server Error This mode occurs when transitioning to WebLM licensing. WebLM has been configured but the server is not available.
• Configuration Error This mode occurs when transitioning to WebLM licensing. WebLM has been configured and the server is available, but there are not enough licenses available to license all of the configured features. Only nodal licenses are valid on Standard mode IP500 V2 systems.
• WebLM Normal Mode The system is fully licensed. WebLM has been configured and there are enough licenses available to license all of the configured features.
• WebLM Error Mode Action is required to correct the License Mode. Refer to the License Status column and the Error List section at the bottom of the screen to determine why the system is in License Error Mode. A 30-day grace period provides access to the capacities and features of the installed license when the system is in License Error Mode.
• WebLM Restricted Mode When the system is in License Error Mode, if the problem is not resolved with the 30-day grace period, the system will enter License Restricted Mode. When in this mode, configuration changes are blocked, except for fixing the licensing errors. If a feature license cannot be acquired from the WebLM server, the feature will not function.
<table>
<tr><th>Type</th><th>Mode</th><th>WebLM Configured</th><th>Virtual License and Grace Period (30 days)</th></tr>
<tr><td>Nodal</td><td>Normal</td><td>✗</td><td>✗</td></tr>
<tr><td>WebLM</td><td>Server Error</td><td>✓</td><td>✗</td></tr>
<tr><td>WebLM</td><td>Configuration Error</td><td>✓</td><td>✗</td></tr>
<tr><td>WebLM</td><td>Normal</td><td>✓</td><td>✗</td></tr>
<tr><td>WebLM</td><td>Error</td><td>✓</td><td>✓</td></tr>
<tr><td>WebLM</td><td>Restricted</td><td>✓</td><td>✗</td></tr>
</table></td></tr>
<tr><td>Licensed Version</td><td>Indicates the software version the system is currently licensed for.</td></tr>
<tr><td>PLDS Host ID</td><td>The ID used when generating PLDS nodal license files.

Not used with WebLM licensing. WebLM licensing uses the host ID of the WebLM server.</td></tr>
<tr><td>PLDS File Status</td><td>If a PLDS nodal license file is loaded, this field indicates if the file is valid or not.</td></tr>
<tr><td>Select Licensing</td><td>Indicates that the system has a valid Select license.</td></tr>
<tr><td>Feature</td><td>Identifies the licenses installed on the system.</td></tr>
</table>

Table continues…

Name	Description
Key	This is the license key string supplied. It is a unique value based on the feature being licensed and the either the system's **Dongle Serial Number** or **System Identification** depending on the type of system. Not applicable when using PLDS or WebLM licensing. This field is not displayed if there are no ADI licenses.
Instance	For information only. Some licenses enable a number of port, channels or users. When that is the case, the number of such is indicated here. Multiple licenses for the same feature are usually cumulative.
Status	For information only. This field indicates the current validation status of the license key. • **Unknown** This status is shown for licenses that have just been added to the configuration shown in Manager. Once the configuration has been sent back to the system and then reloaded, the status will change to one of those below. • **Valid**: The license is valid. • **Invalid**: The license was not recognized. It did not match the PLDS host ID. • **Dormant**: The license is valid but is conditional on some other pre-requisite licenses. • **Obsolete**: The license is valid but is one no longer used by the level of software running on the system.
Expiry Date	For information only. Trial licenses can be set to expire within a set period from their issue. The expiry date is shown here.
Source	The source of the license file. The options are: • **ADI Nodal**: ADI licenses added locally to the system. This may appear on upgraded systems. • **PLDS Nodal**: PLDS licenses added locally to the system. • **WebLM**: Licenses obtained from the WebLM server. • **Virtual**: Licenses created by the system. This may appear on upgraded systems. • **Virtual Grace**: Licenses created by the system while in WebLM error mode.

Additional Configuration Information

Click **PLDS License** > **Send To IP Office** > **OK** to open the **Select PLDS License File** dialog from where you can upload a PLDS license to IP Office. You can browse to a location on your system and select a file to upload.

Select an existing license and click **PLDS License** > **Delete From IP Office** > **OK** to delete the selected license.

Related links

Licenses on page 296

Remote Server

Navigation: **System Settings** > **Licenses** > **Server Menu** > **Remote Server**

This tab is used for:

- For licensing of IP500 V2 systems in Enterprise Branch deployments.
- To specify the method of centralized licensing used for PLDS licensed IP Office Server Edition and Select systems

Offline Editing

The **Reserved Licenses** setting can be edited online. The remaining settings must be edited offline. Changes to these settings require a reboot of the system.

To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

The following fields control which source the IP Office system uses for its licenses. The fields shown depends on the type of IP Office system:

Field	Description
Licence Source	Default = WebLM. This field is available on Server Edition systems. All IP Office systems in the network must use the same source for licensing. The options are: • **WebLM** Use licenses obtained from the PLDS license file uploaded to the WebLM service. All IP Office servers in the network request license reservations from the WebLM service. - On Server Edition systems, a **Deploy** button appears when you select **WebLM** as **License Source**. Click the **Deploy** button to browse and select a license file to deploy. • **Local / Primary Server** PLDS license files are uploaded to the IP Office service of each IP Office server. Depending on the particular licenses: - Some licenses are obtained by reservation requests to the primary IP Office server - Others licenses are obtained from the IP Office server's own license file.
Enable Remote Server	Default = Off. This field is available on non-Server Edition IP500 V2 systems. The options are: • If disabled, the IP Office system is licensed locally by uploading a license file to the system. • If enabled, the system uses licenses requested from a remote WebLM server. This option is only supported for systems in a branch enterprise supported via Avaya Aura® System Manager.

The additional fields displayed depend on the license source selection above:

Local/Primary Server Licensed Server Settings

Field	Description
License Server IP Address	Default = 127.0.0.1 on Primary. On Secondary and expansion systems, the default is the Primary IP address. This field is available when the **Licence Source** is set to **Local Primary Server**. This field contains the IP address of the Server Edition Primary server.

WebLM Licensed Primary Server Settings

Field	Description
Domain Name (URL)	Default = Blank for IP500 V2 systems and for Server Edition Primary hosted deployments. For Server Edition, the IP address of the Primary Server. • For Enterprise Branch deployments, the domain name or IP address of the WebLM server or the domain name of System Manager if the system is under System Manager control. • For Server Edition deployments, the domain name or IP address of the Primary Server. • For Server Edition hosted deployments, the domain name of the WebLM server. The format can be the FQDN or the IP address prefixed with https://.
Path	Default = WebLM/LicenseServer. The path on the web server of the WebLM resource.
Port Number	Default = 52233. The port number of the WebLM server.
WebLM Client ID	Default = An ID based on MAC address and hostname of the system. This field is editable but must only be changed on Avaya Partner Hosted systems. **Important:** • For all other deployment scenarios, you must ensure the value matches the **WebLM Node ID** below. Changing the value will cause license issues for users and phones, including non-IP phones.
WebLM Node ID	Default = An ID based on MAC address and hostname of the system. Read-only. Used by the WebLM service to identify the IP Office system requesting licenses.

WebLM Licensed Server (non-Primary) Settings

Field	Description
Enable proxy via Primary IP Office line	Default = On. Available on Server Edition Secondary and Expansion systems. • Enables retrieval of licenses from the WebLM server through the IP Office Line connection to the Server Edition Primary server. • If the check box is cleared, the WebLM request is done directly to the WebLM server. Note that this field is not available if the node is not configured as a WebSocket client to the Server Edition Primary server.
Primary IP Address	Default = The IP address of the Server Edition Primary server. Available on Server Edition Secondary and Expansion systems when **Enable proxy via Primary IP Office line** is enabled
WebLM Client ID	Default = An ID based on MAC address and hostname of the system. Read-only.
WebLM Node ID	Used by the WebLM service to identify the IP Office system requesting licenses.

Reserved Licenses

These fields are used to reserve licenses from the license server, WebLM or, if using nodal licensing, the Primary server. There are two types of reservation field; manual and automatic.

- Manual fields can be used to set the number of licenses that the server should request from those available on the primary/WebLM server.
- Automatic fields are set to match other aspects of the server configuration, for example the number of configured power users. Note that these values may not change until after the configuration is saved and then reloaded.

WebLM Reserved Licenses — Manual	Primary Server	Secondary Server	Expansion (Linux)	Expansion (IP500 V2)
SIP Trunk Sessions	✓	✓	✓	✓
SM Trunk Sessions	✓	✓	✓	✓
Voicemail Pro Ports	✓	✓	-	-
VMPro Recordings Administrators	✓	✓	-	-
VMPro TTS Professional	✓	✓	-	-
Wave Users	-	-	-	✓
CTI Link Pro	✓	✓	✓	✓
UMS Web Services	✓	✓	✓	✓
MAC Softphones	✓	✓	✓	✓
Avaya Contact Center Select	✓	✓	-	-
Third Party Recorder	✓	✓	-	-
VM Media Manager	✓	✓	✓	-

Table continues…

Customer Service Supervisor	✓	✓	✓	✓
Customer Service Agent	✓	✓	✓	✓

Nodal Reserved Licenses — Manual	**Primary Server**	**Secondary Server**	**Expansion (Linux)**	**Expansion (IP500 V2)**
SIP Trunk Sessions	✓	✓	✓	✓

WebLM/Nodal Reserved Licenses — Automatic	**Primary Server**	**Secondary Server**	**Expansion (Linux)**	**Expansion (IP500 V2)**
Server Edition	✓	✓	✓	✓
Avaya IP Endpoints	✓	✓	✓	✓
3rd-Party IP Endpoints	✓	✓	✓	✓
Receptionist	✓	✓	✓	✓
Office Worker	✓	✓	✓	✓
Power User	✓	✓	✓	✓
Avaya Softphone	✓	✓	✓	✓
Web Collaboration	✓	✓	✓	✓
Universal PRI Additional Channels	-	-	-	✓
IPSec Tunneling	-	-	✓	✓

Related links

Licenses on page 296

Chapter 27: Line

System Settings > **Line**

Lines are used for external calls, both incoming and outgoing.

Click **Add/Edit Trunk Line** to select a line type to add and to specify the system where the line will be added.

Related links

Add Trunk Line on page 303
ACO Line on page 305
Analog Line on page 311
BRI Line on page 319
H.323 Line on page 324
IP DECT on page 331
IP Office Line on page 335
Legacy SIP DECT Line on page 345
MS Teams Line on page 348
PRI Trunks on page 356
E1 Line on page 357
E1 R2 Line on page 365
T1 Line on page 371
SIP Line on page 376
T1 PRI Line on page 405
SM Line on page 414

Add Trunk Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line**

The line settings shown in the system configuration will change according to the types of trunk cards installed in the control unit or added using external expansion modules.

Warning:

Changing Trunk Cards - Changing the trunk card installed in a control unit will result in line settings for both the previous trunk card and the installed trunk card. To change the type of

trunk card installed in a particular card slot, the configuration must be defaulted. This does not apply if replacing an existing card with one of a higher capacity or fitting a trunk card into an unused slot.

Trunk Incoming Call Routing

Trunks are categorized as external or trunk. The trunk type affects how the system routes calls received on that trunk and the routing of calls to the trunk.

Trunk Types	Incoming Calls Routed by
External Trunks • **Analog trunks** • **T1 Robbed Bit** • **E1R2** • **ISDN BRI** (excluding So) • **ISDN PRI T1** • **ISDN PRI E1** • **SIP**	• Incoming calls are routed by matching call details against the settings of the system **Incoming Call Routes**. • Line short codes are not used.
Internal Trunks • **QSIG** (T1, E1 or H.323) • **BRI So** • **H.323** • **SCN** • **SM** • **IP Office Line**	Incoming calls are routed by looking for a match to the incoming digits in the following order: • Extension number. • Trunk short codes (excluding ? short code). • System short codes (excluding ? short code). • Trunk ? short code. • System ? short code.

Line Groups

Each system trunk (or in some cases individual trunk channels) can be configured with an **Incoming Group ID** and an **Outgoing Group ID**. These group IDs are used as follows:

- **Incoming Call Routes** - For incoming calls on external trunks, the Incoming Group ID of the trunk is one of the factors used to match the call to one of the configured incoming call routes.
- **Short Codes** - For dialing which matches a short code set to a **Dial** feature, the short codes **Line Group ID** can indicate either an ARS form or to use a trunk from set to the same **Outgoing Group ID**. If the call is routed to an ARS form, the short codes in the ARS form will specify the trunks to use by matching **Outgoing Group ID**.

Removing Unused Trunks

In cases where a trunk card is installed but the trunk is not physically connected, it is important to ensure that the trunk is disabled in the configuration. This can be done on most trunks using by setting the line's **Admin** setting to **Out of Service**.

This is especially important with analog trunks. Failure to do this may cause the system to attempt to present outgoing calls to that trunk. Similarly, where the number of channels subscribed is less than those supportable by the trunk type, the unsubscribed channels should be disabled.

Clock Quality

Calls between systems using digital trunks (for example E1, E1R2, T1 PRI and BRI) require an common clock signal. The system will try to obtain this clock signal from a PSTN exchange through one of its digital trunks. This is done by setting the **Clock Quality** setting of that line to **Network**. If there are multiple trunks to public exchanges, another trunk can be set as **Fallback** should the primary clock signal fail. Other trunks should be set as **Unsuitable**.

Related links

Line on page 303

ACO Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **ACO Line**

This type of line is only supported in IP500 V2 systems configured for operation as an Avaya Aura X for Avaya Cloud Office (ACO) gateway. Refer to the Deploying IP Office as an Avaya Aura X for Avaya Cloud Office (ACO) ATA Gateway manual.

Related links

Line on page 303
ACO Line | ACO on page 305
ACO Line | VoIP on page 307
ACO Line | T38 FAX on page 309

ACO Line | ACO

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **ACO Line** > **ACO**

Configuration Settings

These settings are mergeable with the exception of the **Line Number** setting. Changing the **Line Number** setting requires a “merge with service disruption”. When the configuration file is sent to the system, the SIP trunk is restarted and all calls on the line are dropped.

Offline editing is not required.

Field	Description
Line Number	Default = Auto-filled. Range = 1 to 249 Enter the line number that you wish. Note that this must be unique. This value is used as the incoming group ID for the line needed for incoming call routing.
ACO Domain Name	Default = Blank.

Table continues…

Field	Description
ACO Proxy Address	These two values should be set to match the values provided for the customer by Avaya Aura X for Avaya Cloud Office (ACO), omitting the port number shown in that information.
Outgoing Group ID	Default = 96666 Fixed value. This value is used is used as the Line Group ID on short codes used to route calls to Avaya Aura X for Avaya Cloud Office (ACO).
URI Type	Default = SIP URI. Set the format the IP Office uses for SIP URI entries in headers. • **SIP URI** - Use SIP URI format. For example, `display <sip:content@hostname>` • **Tel** - Use Tel URI format. For example, +1-425-555-4567. This affects the `From` field of outgoing calls. The `To` field for outgoing calls uses the format specified by the short codes used for outgoing call routing. • **SIPS** - Use SIPS format for all URIs. SIPS can be used only when **Layer 4 Protocol** is set to **TLS**.
Location	Default = Cloud. You can set Location values for the IP Office system and for individual extensions and lines. Associating a line with a location: • Applies the location's call admission control (CAC) settings to the line • For SIP lines that support RFC4119/RFC5139, emergency calls using the line can include the location's address information.

Network Configuration

Field	Description
Layer 4 Protocol	Default = TLS Fixed value. Not changeable.
Use Network Topology Info	Default = None. • **LAN1** - Associate the line with the **Network Topology** and **DiffServ Settings** settings of IP Office LAN1. - If no STUN server address is set for the LAN interface, then the **Binding Refresh Time** is ignored when calculating the timing for periodic `OPTIONS` messages unless the **Firewall/NAT Type** is set to **Open Internet**. • **LAN2** - As above but using the settings of IP Office LAN2. • **None** - If selected, the IP Office does not apply STUN lookup. The IP Office system IP routing tables determine routing for the line.
Send Port	Default = 5096 Fixed value. Not changeable.
Listen Port	Default = 5061 Fixed value. Not changeable.

Related links

ACO Line on page 305

ACO Line | VoIP

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **ACO Line** > **VoIP**

This form is used to configure the VoIP settings applied to calls on the ACO line.

You can edit these settings online without needing to reboot the IP Office.

Configuration Settings

Field	Description
Re-Invite Supported	Default = Off. When enabled, the IP Office can use `Re-Invite` during a call to change the characteristics of the call. For example, when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk. • Requires the ITSP to also support `Re-Invite`. • This setting must be enabled for video support.
Codec Selection	Default = System Default Set the supported codecs. Where possible, Avaya recommend that you use the same set of codecs for all IP Office systems, lines, and extensions. The options are: • **System Default** - Use the codec list set in the system settings. • **Custom** - Configure a list of codec preferences for the line. - You can move codecs between the **Unused** and **Selected** sets and change the order of the codecs. - The codecs available are set by **System Settings** > **System** > **VoIP**. The possible codecs are: • **OPUS** - Supported on Linux-based IP Office systems only. • **G.711 ALAW/G.711 ULAW** • **G.729** • **G.723.1** - Supported on IP500 V2 systems only. • **G.722 64K** - Supported by Linux-based IP Office systems and on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards.

Table continues…

Field	Description
Fax Transport Support	Default = None. If enabled, when the IP Office detects fax tone, it will renegotiate the call codec as configured below. • This option requires **Re-Invite Supported**. • IP Office systems in a network support fax relay for fax calls between systems. • IP500 V2 systems can terminate T38 fax calls. • Linux-based IP Office systems can route the calls between trunks/terminals with compatible fax types. The supported options are: • **None** - Do not support fax. • **G.711** - Use G.711 to send and receive faxes. • **T38** - Use T38 to send and receive faxes. • **T38 Fallback** - Use T38 to send and receive faxes. If the call destination does not support T38, the IP Office will send a re-invite to change the transport method to **G.711**.
Call Initiation Timeout (s)	Default = 4 seconds. Range = 1 to 99 seconds. Sets how long the IP Office system should wait for a response to an attempt to initiate a call before following the alternate routes set in an ARS form.
DTMF Support	Default = RFC2833 (IP500 V2), RFC2833/RFC4733 (Linux-Based Server) Sets how the IP Office signals DTMF key press digits to the remote end. The options are: • **In Band** - Send digits as tones within the call audio. • **RFC2833** or **RFC2833/RF4733** - Send digits using a separate audio stream from the call audio. If not supported by the far end, the line reverts to using **In Band** signaling. • **Info** - Send the digits in SIP `INFO` packets.
Media Security	Default = Enforced. These setting control whether SRTP is used for this line and the settings used for the SRTP. The options are: • **Same as System**: Matches the system setting at **System Settings** > **System** > **VoIP Security**. • **Disabled**: Use RTP. • **Preferred**: Attempt to use SRTP. If SRTP call setup is unsuccessful, fall back to RTP. • **Enforced**: Use SRTP. If SRTP call setup is unsuccessful, the call fails. - For calls using **Dial Emergency**, the IP Office will switch to RTP if SRTP call setup fails.

Table continues…

Field	Description
Advanced Media Security Options	Default = Same as System. Sets the requirements for SRTP when enabled. • **Same as System**: Use the same settings as configured on **System Settings** > **System** > **VoIP Security**. • **Encryptions**: Default = RTP Sets which parts of a session SRTP protects using encryption. • **Authentication**: Default = RTP and RTCP Sets which parts of the session SRTP protects using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Not adjustable. The IP Office will accept authenticated packets that have a sequence number that is higher than or within 64 packets of the highest-numbered packet already received. • **Crypto Suites**: Default = *SRTP_AES_CM_128_SHA1_80*. Set the crypto suites SRTP uses for encryption. The options are *SRTP_AES_CM_128_SHA1_32* and *SRTP_AES_CM_128_SHA1_80*.

Related links

ACO Line on page 305

ACO Line | T38 FAX

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **ACO Line** > **T38 FAX**

The settings are available only on IP500 V2 since it can terminate T38 fax. On the **VoIP** settings for the line type, **Fax Transport Support** must be set to **T38** or **T38 Fallback**.

These settings are mergeable.

Field	Description
Use Default Values	Default = On. If selected, all the fields are set to their default values and greyed out.
T38 Fax Version	Default = 3. During fax relay, the two gateways will negotiate to use the highest version which they both support. The options are: **0**, **1**, **2**, **3**.
Transport	Default = UDPTL (fixed). Only **UDPTL** is supported. **TCP** and **RTP** transport are not supported. For **UDPTL**, redundancy error correction is supported. Forward Error Correction (FEC) is not supported.

Table continues…

Field	Description
Redundancy Redundancy sends additional fax packets in order to increase the reliability. However increased redundancy increases the bandwidth required for the fax transport.	
Low Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for low speed V.21 T.30 fax transmissions.
High Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for V.17, V.27 and V.28 fax transmissions.
TCF Method	Default = Trans TCF. TCF = Training Check Frame.
Max Bit Rate (bps)	Default = 14400. Lower rates can be selected if the current rate is not supported by the fax equipment or is found to not be reliable.
EFlag Start Timer (msecs)	Default = 2600.
EFlag Stop Timer (msecs)	Default = 2300.
Tx Network Timeout (secs)	Default = 150.
Scan Line Fix-up	Default = On.
TFOP Enhancement	Default = On.
Disable T30 ECM	Default = Off. When selected, disabled the T.30 Error Correction Mode used for fax transmission.
Disable EFlags For First DIS	Default = Off.
Disable T30 MR Compression	Default = Off.
NSF Override	Default = Off. If selected, the NSF (Non-Standard Facility) information sent by the T38 device can be overridden using the values in the fields below. **Country Code**: Default = 0. **Vendor Code**: Default = 0.

Related links

ACO Line on page 305

Analog Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **Analog Line**

Analog trunks can be provided within the systems in the following ways. In all cases the physical ports are labeled as Analog. For full details of installation refer to the IP Office Installation manual.

Using ICLID: The system can route incoming calls using the ICLID received with the call. However ICLID is not sent instantaneously. On analog trunks set to Loop Start ICLID, there will be a short delay while the system waits for any ICLID digits before it can determine where to present the call.

Line Status: Analog line do not indicate call status other than whether the line is free or in use. Some system features, for example retrieving unanswered forwards and making twinned calls make use of the call status indicated by digital lines. This is not possible with analog lines. Once an analog line has been seized, the system has to assume that the call is connected and treats it as having been answered.

Dialing Complete: The majority of North-American telephony services use en-bloc dialing. Therefore the use of a ; is recommended at the end of all dialing short codes that use an N. This is also recommended for all dialing where secondary dial tone short codes are being used.

Ground Start: This type of analog trunk is only supported through the Analog Trunk external expansion module.

Related links

Line on page 303
Line Settings on page 311
Line Options on page 313

Line Settings

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **Analog Line** > **Line Settings**

Configuration Settings

These settings are mergeable with the exception of the **Network Type** setting. Changes to this setting will require a reboot of the system.

Field	Description
Line Number	This parameter is not configurable, it is allocated by the system.
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.

Table continues…

Field	Description
Network Type	Default = Public. This option is available when **System | Telephony | Telephony | Restrict Network Interconnect** is enabled. It allows you to configure trunks as either **Public** or **Private**. • The IP Office will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or the opposite. • The call restriction includes transfers, forwarding and conference calls. • Avaya does not recommended use of this feature on IP Office systems using any of the following features: multi-site networks, VPNremote, application telecommuter mode.
Telephone Number	Used to remember the external telephone number of this line to assist with loop-back testing. For information only.
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.
Outgoing Group ID	Default = 1. Range 0 to 99999. When a short code specifies a number to dial, the IP Office will seize an available line from those available with a matching **Outgoing Group ID**. In a Server Edition/Select network, the **Outgoing Group ID** used for lines to a system must be unique within the network. **Reserved Group ID Numbers:** • **0** - In a Server Edition/Select network, the ID 0 cannot be used. • **90000 - 99999** - Reserved for system use (not enforced). - **96666** - Use for ACO lines. - **98888** - For IP Office deployed in an Enterprise Branch environment, reserved for the SM line. - **99001 - 99148** - In a Server Edition/Select network, reserved for the IP Office lines from the primary and secondary servers to each expansion system in the network. - **99998** - In a Server Edition/Select network, reserved for the IP Office lines to the secondary server. - **99999** - In a Server Edition/Select network, reserved for the IP Office lines to the primary server.
Outgoing Channels	Default = 1 (not changeable)
Voice Channels	Default = 1 (not changeable)
Prefix	Default = Blank Enter the number to prefix to all incoming numbers for callback. This is useful if all users must dial a prefix to access an outside line. The prefix is automatically placed in front of all incoming numbers so that users can dial the number back. For outgoing calls: The system does not strip the prefix, therefore any prefixes not suitable for external line presentation should be stripped using short codes.

Table continues…

Field	Description
Line Appearance ID	Default = Auto-assigned. Range = 2 to 9 digits. Allows a number to be assigned to the line to identify it. On phones that support call appearance buttons, a Line Appearance button with the same number will show the status of the line and can be used to answer calls on the line. The line appearance ID must be unique and not match any extension number.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.

Related links

Analog Line on page 311

Line Options

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **Analog Line** > **Analog Options**

Covers analog line specific settings. The system wide setting **System Settings** > **System** > **Telephony** > **Tones and Music** > **CLI Type** is used for to set the incoming CLI detection method for all analogue trunks.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Channel	Set by the system. Shown for information only.
Trunk Type	Default = Loop Start Sets the analog line type. The options are: • **Ground Start**: Ground Start is only supported on trunks provided by the Analog Trunk 16 expansion module. It requires that the module and the control unit are grounded. Refer to the IP Office installation manual. • **Loop Start** • **Loop Start ICLID**: As the system can use ICLID to route incoming calls, on analog Loop Start ICLID trunks there is a few seconds delay while ICLID is received before the call routing can be determined.
Signaling Type	Default = DTMF Dialing Sets the signaling method used on the line. The options are: **DTMF Dialing**, **Pulse Dialing**.
Direction	Default = Both Directions Sets the allowed direction of operation of the line. The options are: **Incoming**, **Outgoing**, **Both Directions**.
Flash Pulse Width	Default = 0. Range = 0 to 2550ms. Set the time interval for the flash pulse width.

Table continues…

Field	Description
Await Dial Tone	Default = 0. Range = 0 to 25500ms. Sets how long the system should wait before dialing out.
Echo Cancellation	Default = 16ms. The echo cancellation should only be adjusted as high as required to remove echo problems. Setting it to a higher value than necessary can cause other distortions. Not used with external expansion module trunks. The options are (milliseconds): **Off**, **8**, **16**, **32**, **64**, **128**.
Echo Reduction	Default = On. (ATM4Uv2 card only) Used when impedance matching is not required but echo reduction is.
Mains Hum Filter	Default = Off. If mains hum interference on the lines is detected or suspected, this settings can be used to attempt to remove that interference. Useable with ATM16 trunks and IP500 ATM4U trunks. The options are: **Off**, **50Hz**, **60Hz**.
Impedance	Set the impedance used for the line. This field is only available for system locales where the default value can be changed. The value used for **Default** is set by the setting **System Settings** > **System** > **System** > **Locale**. For information, see Avaya IP Office Locale Settings. The following values are used for **Automatic Impedance Matching**: 600+2150nF, 600, 900+2150nF, 900, 220+820||115nF, 370+620||310nF, 270+750||150nF, 320+1050||230nF, 350+1000||210nF, 800+100||210nF.
Quiet Line	This field is only available for certain system locales (see above). The setting may be required to compensate for signal loss on long lines.
Digits to break dial tone	Default = 2. Range = Up to 3 digits. During automatic impedance testing (see below), once the system has seized a line, it dials this digit or digits to the line. In some cases it may be necessary to use a different digit or digits. For example, if analog trunk go via another PBX system or Centrex, it will be necessary to use the external trunk dialing prefix of the remote system plus another digit, for example 92.

Table continues…

Field	Description
Automatic	Default = Yes. (ATM4Uv2 card only) When set to **Yes**, the **Default** value is used. The value used for **Default** is set by the system **Locale**. When set to **No**, the **Impedance** value can be manually selected from the list of possible values: • 600 • 900 270+(750R || 150nF) and 275R + (780R || 150nF) • 220+(820R || 120nF) and 220R+ (82R || 115nF) • 370+(620R || 310nF) • 320+(1050R || 230nF) • 370+(820R || 110nF) • 275+(780R || 115nF) • 120+(820R || 110nF) • 350+(1000R || 210nF) • 200+(680R || 100nF) • 600+2.16µF • 900+1µF • 900+2.16µF • 600+1µF Global Impedance

Table continues…

Field	Description
Automatic Balance Impedance Match	These controls can be used to test the impedance of a line and to then display the best match resulting from the test. Testing should be performed with the line connected but the system otherwise idle. To start testing click **Start**. The system will then send a series of signals to the line and monitor the response, repeating this at each possible impedance setting. Testing can be stopped at any time by clicking **Stop**. When testing is complete, Manager will display the best match and ask whether that match should be used for the line. If **Yes** is selected, Manager will also ask whether the match should be applied to all other analog lines provided by the same analog trunk card or module. Note that on the Analog Trunk Module (ATM16), there are four control devices, each supporting four channels. The impedance is set by the control device for all four channels under its control. Consequently, the impedance match tool only functions on lines 1, 5, 9, and 13. Before testing, ensure that the following system settings are correctly set: • **System Settings** > **System** > **System** > **Locale** • **System Settings** > **System** > **Telephony** > **Companding Law** If either needs to be changed, make the required change and save the setting to the system before proceeding with impedance matching. Due to hardware differences, the impedance matching result will vary slightly depending on which type of trunk card or expansion module is being used. **Automatic Balance Impedance Matching**, **Quiet Line** and **Digits to break dial tone** are available for the Bahrain, Egypt, French Canadian, India, Kuwait, Morocco, Oman, Pakistan, Qatar, Saudi Arabia, South Africa, Turkey, United Arab Emirates, United States and Customize locales.
Allow Analog Trunk to Trunk Connect	Default = Not selected (Off). When not enabled, users cannot transfer or forward external calls back off-switch using an analog trunk if the call was originally made or received on another analog trunk. This prevents transfers to trunks that do not support disconnect clear. If the setting **System Settings** > **System** > **Telephony** > **Unsupervised Analog Trunk Disconnect Handling** is enabled, this setting is greyed out and trunk to trunk connections to any analog trunks are not allowed.
BCC	Default = Not selected [Brazil locale only] A collect call is a call at the receiver's expense and by his permission. If supported by the line provider, BCC (Block Collect Call) can be used to bar collect calls.
Long CLI Line	Default = Off The CLI signal on some analog lines can become degraded and is not then correctly detected. If you are sure that CLI is being provided but not detected, selecting this option may resolve the problem.

Table continues…

Field	Description
Modem Enabled	Default = Off The first analog trunk in a control unit can be set to modem operation (V32 with V42 error correction). This allows the trunk to answer incoming modem calls and be used for system maintenance. When on, the trunk can only be used for analog modem calls. The default system short code *9000* can be used to toggle this setting. For the IP500 ATM4U-V2 Trunk Card Modem, it is not required to switch the card's modem port on/off. The trunk card's V32 modem function can be accessed simply by routing a modem call to the RAS service's extension number. The modem call does not have to use the first analog trunk, instead the port remains available for voice calls.
MWI Standard	Default = None. This setting is only displayed for ATM4U-V2 cards. When **System Settings** > **System** > **Voicemail** is set to **Analogue MWI**, change this setting to **Bellcore FSK**.
BCC Flash Pulse Width	Default = 100 (1000ms). Range = 0 to 255. Brazil locale only. Sets the BCC (Block collect call) flash pulse width.

Pulse Dialing

These settings are used for pulse dialing.

Field	Description
Mark	Default = 40ms. Range = 0 to 255. Interval when DTMF signal is kept active during transmission of DTMF signals.
Space	Default = 60ms. Range = 0 to 255. Interval of silence between DTMF signal transmissions.
Inter-Digit Pause	Default = 500ms. Range = 0 to 2550ms. Sets the pause between digits transmitted to the line.

Ring Detection

These settings are used for ring detection.

Field	Description
Ring Persistency	Default = Set according to system locale. Range = 0 to 2550ms. The minimum duration of signal required to be recognized.
Ring Off Maximum	Default = Set according to system locale. Range = 0 to 25500ms. The time required before signaling is regarded as ended.

Disconnect Clear

Disconnect clear (also known as 'Line Break' or 'Reliable Disconnect') is a method used to signal from the line provider that the call has cleared. The system also uses 'Tone Disconnect', which

clears an analog call after 6 seconds of continuous tone, configured through the Busy Tone Detection (**System | Telephony | Tones & Music**) settings.

Field	Description
Disconnect Clear	Default = On Enables the use of disconnect clear. If the setting **System Settings** > **System** > **Telephony** > **Unsupervised Analog Trunk Disconnect Handling** is enabled, this setting is greyed out and disconnect clear disabled.
Units	Default = 500ms. Range = 0 to 2550ms. This time must be less than the actual disconnect time period used by the line provider by at least 150ms.

Secondary Dial Tone

Configures the use of secondary dial tone on analog lines. This is a different mechanism from secondary dial tone using short codes. This method is used mainly within the Russian locale. When selected, the options are:

Field	Description
Secondary Dial Tone	Default = Off
Await time:	Default = 3000ms. Range = 0 to 25500ms. Used when secondary dial tone (above) is selected. Sets the delay.
After n Digits	Default = 1. Range = 0 to 10. Sets where in the dialing string, the delay for secondary dial tone, should occur.
Matching Digit	Default =8. Range = 0 to 9. The digit which, when first matched in the dialing string, will cause secondary dial tone delay.

DTMF

These settings are used for DTMF dialing.

Field	Description
On	Default = 80ms. Range = 0 to 255ms. The width of the on pulses generated during DTMF dialing.
Off	Default = 80ms. Range = 0 to 255ms. The width of the off pulses generated during DTMF dialing.

Gains

These settings are used to adjust the perceived volume on all calls.

Field	Description
A | D	Default = 0dB. Range =-10.0dB to +6.0dB in 0.5dB steps. Sets the analog to digital gain applied to the signal received from the trunk by the system. To conform with the Receive Objective Loudness Rating at distances greater than 2.7km from the central office, on analog trunks a receive gain of 1.5dB must be set.
D | A	Default = 0dB. Range =-10.0dB to +6.0dB in 0.5dB steps. Sets the digital to analog gain applied to the signal from the system to the trunk.
Voice Recording	Default = Low Used to adjust the volume level of calls recorded by voicemail. The options are **Low**, **Medium** or **High**.

Related links

Analog Line on page 311

BRI Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **BRI Line**

BRI trunks are provided by the installation of a BRI trunk card into the control unit. The cards are available in different variants with either 2 or 4 physical ports. Each port supports 2 B-channels for calls. For full details of installation refer to the IP Office Installation manual.

Point-to-Point or Multipoint

BRI lines can be used in either Point-to-Point or Point-to-Multipoint mode. Point-to-Point lines are used when only one device terminates a line in a customer's office. Point-to-Multipoint lines are used when more than one device may be used on the line at the customer's premises. There are major benefits in using Point-to-Point lines:-

- The exchange knows when the line/terminal equipment is down/dead, thus it will not offer calls down that line. If the lines are Point-to-Multipoint, calls are always offered down the line and fail if there is no response from the terminal equipment. So if you have two Point-to-Multipoint lines and one is faulty 50% of incoming calls fail.
- You get a green LED on the Control Unit when the line is connected. With Point-to-Multipoint lines some exchanges will drop layer 1/2 signals when the line is idle for a period.
- The timing clock is locked to the exchange. If layer 1/2 signals disappear on a line then the Control Unit will switch to another line, however this may result in some audible click when the switchover occurs.

The system's default Terminal Equipment Identifier (TEI) will normally allow it to work on Point-to-Point or Point-to-Multipoint lines. However if you intend to connect multiple devices simultaneously to an BRI line, then the TEI should be set to 127. With a TEI of 127, the control unit will ask the exchange to allocate a TEI for operation.

Note:

When connected to some manufactures equipment, which provides an S0 interface (BRI), a defaulted Control Unit will not bring up the ISDN line. Configuring the Control Unit to a TEI of 127 for that line will usually resolve this.

Related links

Line on page 303
Line Settings on page 320
Channels on page 324

Line Settings

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **BRI Line** > **Line Settings**

The following settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

- **Line Sub Type**, **Network Type**, **TEI**, **Add 'Not-end-to-end ISDN' Information Element**, **Progress Replacement**, **Clock Quality**, **Force Number Plan to ISDN**, **Number of Channels**.

The remaining settings can be edited online.

Field	Description
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Line Number	This parameter is not configurable; it is allocated by the system.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.
Line Sub Type	Default = **NTT** for Japan/**ETSI** for other locales. Select to match the particular line type provided by the line provider. IP500 BRI daughter cards can be configured for **S-Bus** (So) operation for connection to ISDN terminal devices. Note that this requires the addition of terminating resistors at both the system and remote ends, and the use of a suitable cross-over cable. For full details refer to the Deploying Avaya IP Office Platform IP500 V2 manual.

Table continues…

Field	Description
Network Type	Default = Public. This option is available when **System | Telephony | Telephony | Restrict Network Interconnect** is enabled. It allows you to configure trunks as either **Public** or **Private**. • The IP Office will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or the opposite. • The call restriction includes transfers, forwarding and conference calls. • Avaya does not recommended use of this feature on IP Office systems using any of the following features: multi-site networks, VPNremote, application telecommuter mode.
Telephone Number	Used to remember the external telephone number of this line to assist with loop-back testing. For information only.
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.
Outgoing Group ID	Default = 1. Range 0 to 99999. When a short code specifies a number to dial, the IP Office will seize an available line from those available with a matching **Outgoing Group ID**. In a Server Edition/Select network, the **Outgoing Group ID** used for lines to a system must be unique within the network. **Reserved Group ID Numbers:** • **0** - In a Server Edition/Select network, the ID 0 cannot be used. • **90000 - 99999** - Reserved for system use (not enforced). - **96666** - Use for ACO lines. - **98888** - For IP Office deployed in an Enterprise Branch environment, reserved for the SM line. - **99001 - 99148** - In a Server Edition/Select network, reserved for the IP Office lines from the primary and secondary servers to each expansion system in the network. - **99998** - In a Server Edition/Select network, reserved for the IP Office lines to the secondary server. - **99999** - In a Server Edition/Select network, reserved for the IP Office lines to the primary server.
Prefix	Default = Blank. The prefix is used in the following ways: • **For incoming calls**: The ISDN messaging tags indicates the call type (National, International or Unknown). If the call type is unknown, then the number in the Prefix field is added to the ICLID. • **For outgoing calls**: The prefix is not stripped, therefore any prefixes not suitable for external line presentation should be stripped using short codes.

Table continues…

Field	Description
National Prefix	Default = 0 This indicates the digits to be prefixed to a incoming national call. When a number is presented from ISDN as a "national number" this prefix is added. For example 1923000000 is converted to 01923000000.
International Prefix	Default = 00 This indicates the digits to be prefixed to an incoming international call. When a number is presented from ISDN as an "international number" this prefix is added. For example 441923000000 is converted to 00441923000000.
TEI	Default = 0 The Terminal Equipment Identifier. Used to identify each device connected to a particular ISDN line. For Point-to-Point lines this is 0. It can also be 0 on a Point to Multipoint line, however if multiple devices are sharing a Point-to-Multipoint line it should be set to 127 which results in the exchange allocating the TEI's to be used.
Number of Channels	Default = 2. Range = 0 to 2. Defines the number of operational channels that are available on this line.
Outgoing Channels	Default = 2. Range = 0 to 2. This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as Number of Channels field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls.
Voice Channels	Default = 2. Range = 0 to 2. The number of channels available for voice use.
Data Channels	Default = 2. Range = 0 to 2. The number of channels available for data use. If left blank, the value is 0.
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available. • Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source. • In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.

Table continues…

Field	Description
Add 'Not-end-to-end ISDN' Information Element	Default = Never*. Sets whether the optional 'Not end-to-end ISDN' information element should be added to outgoing calls on the line. The options are **Never**, **Always** or **POTS** (only if the call was originated by an analog extension). *The default is **Never** except for the following locales; for Italy the default is **POTS**, for New Zealand the default is **Always**.
Progress Replacement	Default = None. Progress messages are defined in the Q.931 ISDN connection control signaling protocol. Generally, if a progress message is sent, the caller does not get connected and so typically does not accrue call costs. Not all ISDN lines support Q.931 Progress messages. Use this setting to configure alternative signaling to the ISDN line for internally generated Progress messages. The options are: • **Alerting**: Map to Q.931 Alerting. The call is not connected. The caller does not hear the message and typically does not accrue call costs. • **Connect**: Map to Q.931 Connect. The caller hears the message and typically will accrue call costs.
Supports Partial Rerouting	Default = Off. Partial rerouting (PR) is an ISDN feature. It is supported on external (non-network and QSIG) ISDN exchange calls. When an external call is transferred to another external number, the transfer is performed by the ISDN exchange and the channels to the system are freed. Use of this service may need to be requested from the line provider and may incur a charge.
Force Number Plan to ISDN	Default = Off. This option is only configurable when **Support Partial Rerouting** is also enabled. When selected, the plan/type parameter for Partial Rerouting is changed from **Unknown/Unknown** to **ISDN/Unknown**.
Send Redirecting Number	Default = Off. This option can be used on ISDN trunks where the redirecting service is supported by the trunk provider. Where supported, on twinned calls the caller ID of the original call is passed through to the twinning destination. This option is only used for twinned calls.
Support Call Tracing	Default = Off. The system supports the triggering of malicious caller ID (MCID) tracing at the ISDN exchange. Use of this feature requires liaison with the ISDN service provider and the appropriate legal authorities to whom the call trace will be passed. The user will also need to be enabled for call tracing and be provider with either a short code or programmable button to activate MCID call trace. Refer to Malicious Call Tracing in the Telephone Features section for full details.
Active CCBS Support	Default = Off. Call completion to a busy subscriber (CCBS). It allows automatic callback to be used on outgoing ISDN calls when the destination is busy. This feature can only be used on point-to-point trunks. Use of this service may need to be requested from the line provider and may incur a charge.

Table continues…

Field	Description
Passive CCBS	Default = Off.
Cost Per Charging Unit	The information is provided in the form of charge units. This setting is used to enter the call cost per charging unit set by the line provider. The values are 1/10,000th of a currency unit. For example if the call cost per unit is £1.07, a value of 10700 should be set on the line. Refer to Advice of Charge.
Send original calling party for forwarded and twinning calls	Default = Off. Use the original calling party ID when forwarding calls or routing twinned calls. This setting applies to BRI lines with subtype ETSI.
Originator number for forwarded and twinning calls	Default = blank. The number used as the calling party ID when forwarding calls or routing twinned calls. This field is grayed out when the **Send original calling party for forwarded and twinning calls** setting is enabled. This setting applies to BRI lines with subtype ETSI.

Related links

BRI Line on page 319

Channels

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **BRI Line** > **Channels**

This tab allows settings for individual channels within the trunk to be adjusted. To edit a channel either double-click on it or click the channel and then select **Edit**.

To edit multiple channels at the same time, select the required channels using Ctrl or Shift and then click **Edit**. When editing multiple channels, fields that must be unique such as **Line Appearance ID** are not shown.

These settings can be edited online.

Field	Description
Line Appearance ID	Default = Auto-assigned. Range = 2 to 9 digits. Used for configuring Line Appearances with button programming. The line appearance ID must be unique and not match any extension number. Line appearance is not supported for trunks set to QSIG operation and is not recommended for trunks be used for DID.

Related links

BRI Line on page 319

H.323 Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **H323 Line**

These lines are added manually. They allow voice calls to be routed over data links within the system. They are therefore dependent on the IP data routing between the system and the destination having being configured and tested.

Calls received on IP, S0 and QSIG trunks do not use incoming call routes. Routing for these is based on incoming number received as if dialed on-switch. Line short codes on those trunks can be used to modify the incoming digits.

Network Assessments

Not all data connections are suitable for voice traffic. A network assessment is required for internal network connections. For external network connections a service level agreement is required from the service provider. Avaya cannot control or be held accountable for the suitability of a data connection for carrying voice traffic.

QSIG trunks trunks are not supported on IP500 V2 systems without IP500 Voice Networking licenses.

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 806.

Related links

Line on page 303
H.323 Line VoIP on page 325
H.323 Line Short Codes on page 327
H.323 Line VoIP Settings on page 328

H.323 Line VoIP

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **H323 Line** > **VoIP Line**

Configuration Settings

These settings can be edited online. Changes to these settings does not require a reboot of the system.

Field	Description
Line Number	Default = Auto-filled. Range = 1 to 249 *(IP500 V2)*/349 *(Server Edition)*. Enter the line number that you wish. Note that this must be unique. On IP500 V2 systems, line numbers 1 to 16 are reserved for internal hardware.
Telephone Number	Used to remember the telephone number of this line. For information only.

Table continues…

Field	Description
Network Type	Default = Public. This option is available when **System | Telephony | Telephony | Restrict Network Interconnect** is enabled. It allows you to configure trunks as either **Public** or **Private**. • The IP Office will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or the opposite. • The call restriction includes transfers, forwarding and conference calls. • Avaya does not recommended use of this feature on IP Office systems using any of the following features: multi-site networks, VPNremote, application telecommuter mode.
Prefix	Default = Blank. The prefix is used in the following ways: • **For incoming calls** The ISDN messaging tags indicates the call type (National, International or Unknown). If the call type is unknown, then the number in the Prefix field is added to the ICLID. • **For outgoing calls** The prefix is not stripped, therefore any prefixes not suitable for external line presentation should be stripped using short codes.
National Prefix	Default = 0 This indicates the digits to be prefixed to a incoming national call. When a number is presented from ISDN as a "national number" this prefix is added. For example 1923000000 is converted to 01923000000.
International Prefix	Default = 00 This indicates the digits to be prefixed to an incoming international call. When a number is presented from ISDN as an "international number" this prefix is added. For example 441923000000 is converted to 00441923000000.
Location	Default = Cloud. You can set Location values for the IP Office system and for individual extensions and lines. Associating a line with a location: • Applies the location's call admission control (CAC) settings to the line • For SIP lines that support RFC4119/RFC5139, emergency calls using the line can include the location's address information.
Description	Default = Blank. Maximum 31 characters. You can use this field to enter a description for the configuration entry. The description is not used elsewhere.
Send original calling party for forwarded and twinning calls	Default = Off. Use the original calling party ID when forwarding calls or routing twinned calls.

Table continues…

Field	Description
Outgoing Group ID	Default = 1. Range 0 to 99999. When a short code specifies a number to dial, the IP Office will seize an available line from those available with a matching **Outgoing Group ID**. In a Server Edition/Select network, the **Outgoing Group ID** used for lines to a system must be unique within the network. **Reserved Group ID Numbers:** • **0** - In a Server Edition/Select network, the ID 0 cannot be used. • **90000 - 99999** - Reserved for system use (not enforced). - **96666** - Use for ACO lines. - **98888** - For IP Office deployed in an Enterprise Branch environment, reserved for the SM line. - **99001 - 99148** - In a Server Edition/Select network, reserved for the IP Office lines from the primary and secondary servers to each expansion system in the network. - **99998** - In a Server Edition/Select network, reserved for the IP Office lines to the secondary server. - **99999** - In a Server Edition/Select network, reserved for the IP Office lines to the primary server.
Number of Channels	Default = 20, Range 1 to 250. Defines the number of operational channels that are available on this line.
Outgoing Channels	Default = 20, Range 0 to 250. This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as Number of Channels field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls.
TEI	Default = 0. Range = 0 to 127. The Terminal Equipment Identifier. Used to identify each Control Unit connected to a particular ISDN line. For Point to Point lines this is typically (always) 0. It can also be 0 on a Point to Multi-Point line, however if multiple devices are actually sharing a Point to Multi-Point line it should be set to 127 which will result in the exchange deciding on the TEI's to be used by this Control Unit.

Related links

H.323 Line on page 324

H.323 Line Short Codes

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **H323 Line** > **Short Codes**

For some types of line, Line short codes can be applied to any digits received with incoming calls.

The line Short Code tab is shown for the following trunk types which are treated as internal or private trunks: **QSIG** (T1, E1, H.323), **BRI S0**, **H.323**, **SCN**, **IP Office**. Incoming calls on those

types of trunk are not routed using **Incoming Call Route** settings. Instead the digits received with incoming calls are checked for a match as follows:

Extension number (including remote numbers in a multi-site network).

- Line short codes (excluding ? short code).
- System short codes (excluding ? short code).
- Line ? short code.
- System ? short code.

Short codes can be added and edited using the **Add**, **Remove** and **Edit** buttons. Alternatively you can right-click on the list of existing short code to add and edit short codes.

These settings can be edited online.

Related links

H.323 Line on page 324

H.323 Line VoIP Settings

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **H323 Line** > **VoIP Settings**

This form is used to configure the VoIP setting applied to calls on the H.323 line.

Configuration Settings

These settings can only be edited online. Changes to these settings does not require a reboot of the system.

Field	Description
Gateway IP Address	Default = Blank Enter the IP address of the gateway device at the remote end.
Port	Default = 1720 The H.323 line is identified by the IP Address:Port value. Specifying a unique port value for this IP address allows multiple lines to use the same IP address.

Table continues…

Field	Description
Codec Selection	Default = System Default Set the supported codecs. Where possible, Avaya recommend that you use the same set of codecs for all IP Office systems, lines, and extensions. The options are: • **System Default** - Use the codec list set in the system settings. • **Custom** - Configure a list of codec preferences for the line. - You can move codecs between the **Unused** and **Selected** sets and change the order of the codecs. - The codecs available are set by **System Settings** > **System** > **VoIP**. The possible codecs are: • **OPUS** - Supported on Linux-based IP Office systems only. • **G.711 ALAW/G.711 ULAW** • **G.729** • **G.723.1** - Supported on IP500 V2 systems only. • **G.722 64K** - Supported by Linux-based IP Office systems and on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards.
Supplementary Services	Default = H450. Selects the supplementary service signaling method for use across the H.323 trunk. The remote end of the trunk must support the same option. The options are: • **None**: No supplementary services are supported. • **H450**: Use for H.323 lines connected to another PBX or device that uses H450. • **QSIG**: Use for H.323 lines connected to another PBX or device that uses QSIG.
Call Initiation Timeout	Default = 4 seconds. Range = 1 to 99 seconds. This option sets how long the system should wait for a response to its attempt to initiate a call before following the alternate routes set in an ARS form.
VoIP Silence Suppression	Default = Off. When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.
Enable FastStart for non-Avaya IP Phones	Default = Off A fast connection procedure. Reduces the number of messages that need to be exchanged before an audio channel is created.

Table continues…

Field	Description
Fax Transport Support	Default = Off This option is only supported on trunks with their **Supplementary Services** set to **IP Office SCN** or **IP Office Small Community Network - Fallback**. Fax relay is supported across H.323 multi-site network lines with **Fax Transport Support** selected. This will use 2 VCM channels in each of the systems. Fax relay is only supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 and or IP500 Combo cards. Fax relay is not supported on Server Edition Linux servers.
Local Tones	Default = Off When selected, the tones are generated by the local system to which the phone is registered. This option should not be used with lines being used for a multi-site network.
DTMF Support	Default = Out of Band DTMF tones can be sent to the remote end either as DTMF tones within the calls audio path (**In Band**) or a separate signals (**Out of Band**). Out of Band is recommended for compression modes such as G.729 and G.723 compression modes where DTMF in the voice stream could become distorted.
Allow Direct Media Path	Default = On This settings controls whether calls between IP endpoints and/or lines must go through the IP Office. • If disabled, calls go through the IP Office and use its resources. RTP relay allows calls between devices using the same audio codec to not require a voice compression channel. • If enabled, calls can take routes other than through the IP Office system. Both ends must support direct media and have matching VoIP settings. For example, both ends must use the same protocol (SIP or H.323), same addressing (IPv4 or IPv6), and so on. Otherwise, the call goes through the IP Office system. - For extensions, disabling **Requires DTMF** allows the extension to attempt direct media even if the other end has differing DTMF settings.
Progress Ends Overlap Send	Default = Off. Some telephony equipment, primarily AT&T switches, over IP trunks send a H.323 Progress rather than H.323 Proceeding message to signal that they have recognized the digits sent in overlap state. By default the system expects an H.323 Proceeding message. This option is not available by default. If required, the value **ProgressEndsOverlapSend** must be entered into the Source Numbers tab of the NoUser user.
Default Name From Display IE	Default = Off. When set, the Display IE is used as the default source for the name.

Related links

H.323 Line on page 324

IP DECT

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP DECT Line**

You can add this type of line manually. The line is then used to route voice calls over IP to an Avaya Wireless DECT system. Only one IP DECT line is supported. See the Deploying Avaya Wireless DECT with IP Office manual.

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 806.

Related links

Line on page 303
IP DECT Line on page 331
Gateway on page 331
VoIP on page 333

IP DECT Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP DECT Line** > **Line**

When creating an IP DECT line, these settings are mergeable. You can also remove an IP DECT line without rebooting. Changing an IP DECT line that has been imported into the configuration is not mergeable.

Field	Description
Line Number	This number is allocated by the system and is not adjustable.
Associated Extensions	Lists all the DECT extensions associated with the IP DECT line by the extension's **DECT Line ID** setting.
Call based Location Information	If enabled, the DECT extension location can be overridden on a call-by-call basis using the location specified in the base station configuration. Supported with R11.1 FP2 SP2 and higher. Requires each base station to be configured with a location ID that matches a location in the IP Office configuration. Refer to the Deploying Avaya Wireless DECT with IP Office manual.
Description	Default = Blank. Maximum 31 characters. You can use this field to enter a description for the configuration entry. The description is not used elsewhere.

Related links

IP DECT on page 331

Gateway

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP DECT Line** > **Gateway**

This form is used to configure the link between the IP Office and Avaya Wireless DECT systems.

When creating an IP DECT line, these settings are mergeable. You can also remove an IP DECT line without rebooting. Changing an IP DECT line that has been imported into the configuration is not mergeable.

Field	Description
Auto-Create Extension	Default = Off. If enabled, subscription of a handset with the Avaya Wireless DECT system causes the auto-creation of a matching numbered extension within the system configuration if one does not already exist. This setting is not supported on systems configured to use WebLM server licensing. • For security, auto-create is automatically disabled after 24 hours.
Auto-Create User	Default = Off. This option is only usable if **Auto-Create Extension** is also enabled. If enabled, subscription of a handset with the DECT system causes the auto-creation of a matching user within the system configuration if one does not already exist. • For security, auto-create is automatically disabled after 24 hours.
Enable DHCP Support	Default = Off This option is not used with Avaya Wireless DECT.
Boot File	Default = ADMM_RFP_1_0_0.tftp. Range = Up to 31 characters. This option is not used with Avaya Wireless DECT.
ADMM MAC Address	Default = 00:00:00:00:00:00 This option is not used with Avaya Wireless DECT.
VLAN ID	Default = Blank. Range = 0 to 4095. This option is not used with Avaya Wireless DECT.
Base Station Address List	Default = Empty This option is not used with Avaya Wireless DECT.
Enable Provisioning This option can be used with Avaya Wireless DECT systems. It allows the setting of several values in the IP Office system configuration that previously needed to be set separately in the master base stations configuration. The use of provisioning requires the system security settings to include an **IPDECT Group**. For full details, see the Deploying Avaya Wireless DECT with IP Office manual.	
SARI/PARK	Default = 0 Enter the PARK (Portable Access Rights Key) license key of the Avaya Wireless DECT system.

Table continues…

Field	Description
Subscriptions	Default = Disabled Select the method of subscription supported for handsets subscribing to the Avaya Wireless DECT system. The options are: • **Disabled** Disables subscription of handsets. • **Auto-Create** Allow anonymous subscription of handsets. Once subscribed, the handset is assigned a temporary extension number. That extension number can be confirmed by dialing `*#`. A new extension number can be specified by dialing `<Extension Number>*<Login Code>#`. The **Auto-Create Extension** and **Auto-Create User** settings above should also be enabled. While configured to this mode, Manager will not allow the manual addition of new IP DECT extensions. • **Preconfigured** Allow subscription only against existing IP DECT extensions records in the system configuration. The handset IPEI number is used to match the subscribing handset to a system extension.
Authentication Code	Default = Blank. Set an authentication code that DECT handset users should enter when subscribing to the DECT system.
Enable Resiliency Default = Off. Enables resiliency on the IP DECT Line. To configure resiliency, you must also configure an IP Office with **Backs up my IP Dect Phones** set to **On**.	
Status Enquiry Period	Default = 30 seconds. The period between successive verifications on the H.323 channel. The smaller the interval, the faster the IP DECT system recognizes that IP Office is down.
Prioritize Primary	Default = Off. Set to **On** for automatic failover recovery. When on, the Avaya Wireless DECT system switches automatically from the backup IP Office to the "primary" IP Office. Only available when **Enable Provisioning** is set to **On**.
Supervision Timeout	Default = 120 seconds. The period of time the Avaya Wireless DECT system will wait between attempts to switch from the backup IP Office to its "primary" IP Office. Only available when **Enable Provisioning** is set to **On**.

Related links

IP DECT on page 331

VoIP

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP DECT Line** > **VoIP**

Used to configure the VoIP setting applied to calls on the IP DECT line.

When creating an IP DECT line, these settings are mergeable. You can also remove an IP DECT line without rebooting. Changing an IP DECT line that has been imported into the configuration is not mergeable.

Field	Description
Gateway IP Address	Default = Blank. Enter the IP address of the gateway device at the remote end. This address must not be shared by any other IP line (H.323, SIP, SES or IP DECT).
Standby IP Address	Default = Blank. IP Address of the Standby Master IP Base Station or the second Mirror Base Station. When the primary Mirror Base Station or Master Base Station is offline the second Mirror or the Standby Master will take over and the system will use this IP address.
Codec Selection	Default = System Default Set the supported codecs. Where possible, Avaya recommend that you use the same set of codecs for all IP Office systems, lines, and extensions. The options are: • **System Default** - Use the codec list set in the system settings. • **Custom** - Configure a list of codec preferences for the line. - You can move codecs between the **Unused** and **Selected** sets and change the order of the codecs. - The codecs available are set by **System Settings** > **System** > **VoIP**. The possible codecs are: • **OPUS** - Supported on Linux-based IP Office systems only. • **G.711 ALAW/G.711 ULAW** • **G.729** • **G.723.1** - Supported on IP500 V2 systems only. • **G.722 64K** - Supported by Linux-based IP Office systems and on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards.
TDM | IP Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the system TDM interface to the IP connection. This field is not shown on Linux based platforms.
IP | TDM Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the IP connection to the system TDM interface. This field is not shown on Linux based platforms.

Table continues…

Field	Description
VoIP Silence Suppression	Default = Off. When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.
Allow Direct Media Path	Default = On This settings controls whether IP calls must be routed via the system or can be routed alternatively if possible within the network structure. • If enabled, IP calls can take routes other than through the system, removing the need for system resources such as voice compression channels. Both ends of the calls must support Direct Media and have compatible VoIP settings such as matching codec, etc. If otherwise, the call will remain routed via the system. Enabling this option may cause some vendors problems with changing the media path mid call. • If disabled, the call is routed via the system. In that case, RTP relay support may still allow calls between devices using the same audio codec to not require a voice compression channel.

Related links

IP DECT on page 331

IP Office Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP Office Line**

This line type is used to connect two IP Office systems.

In previous releases, connecting two IP Office systems was achieved using H.323 Lines configured with **Supplementary Services** set to **IP Office SCN**. In the current release, the IP Office line type is used to connect IP Office systems. Separating out the IP Office line type from the H.323 line type allows for the logical grouping of features and functions available when connecting two IP Office systems, including IP Office systems connected through the cloud.

Note:

Setting an IP Office line with **Transport Type** = **Proprietary** and **Networking Level** = **SCN** will interwork with a previous release system configured with an H.323 SCN line.

Related links

Line on page 303
IP Office Line on page 336
IP Office Line Short Codes on page 341
IP Office Line VoIP Settings on page 341

T38 Fax on page 344

IP Office Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP Office Line** > **Line**

Additional configuration information

For information on the **SCN Resiliency Options**, refer to the IP Office Resilience Overview manual.

Configuration Settings

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Line Number	Default = Auto-filled. Range = 1 to 249 *(IP500 V2)*/349 *(Server Edition)*. Enter the line number that you wish. Note that this must be unique. On IP500 V2 systems, line numbers 1 to 16 are reserved for internal hardware.
Description	Default = Blank. Maximum 31 characters. You can use this field to enter a description for the configuration entry. The description is not used elsewhere.
Transport Type	Default = Proprietary. The options are • **Proprietary**: The default connection type when connecting two IP Office systems. • **WebSocket Client / Websocket Server**: A WebSocket connection is an HTTP / HTTPS initiated TCP pipe through which Call signalling and Network Signaling is tunneled. This transport type is used to connect IP Office systems through the cloud. Selecting one of the WebSocket options enables the **Security** field and the **Password** fields.
Networking Level	Default = SCN. The options are • **None**: No supplementary services are supported. • **SCN**: This option is used to link IP Office system within a multi-site network. The systems within a multi-site network automatically exchange information about users and extensions, allowing remote users to be called without any additional configuration on the local system.

Table continues…

Field	Description
Security	Default = Unsecured. The Security field is available when **Transport Type** is set to **WebSocket Client** or **WebSocket Server**. The options are • **Unsecured** : The connection uses HTTP/TCP. • **Medium**: The connection uses HTTPS/TLS. • **High**: The connection uses HTTPS/TLS. The server certificate store must contain the client identity certificate.
Network Type	Default = Public. This option is available when **System | Telephony | Telephony | Restrict Network Interconnect** is enabled. It allows you to configure trunks as either **Public** or **Private**. • The IP Office will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or the opposite. • The call restriction includes transfers, forwarding and conference calls. • Avaya does not recommended use of this feature on IP Office systems using any of the following features: multi-site networks, VPNremote, application telecommuter mode.
Include location specific information	Default = Off. Enabled when **Network Type** is set to **Private**. Set to **On** if the PBX on the other end of the trunk is toll compliant.
Telephone Number	Default = Blank. Used to remember the telephone number of this line. For information only.
Prefix	Default = Blank. The prefix is used in the following ways: • **For incoming calls** The ISDN messaging tags indicates the call type (National, International or Unknown). If the call type is unknown, then the number in the Prefix field is added to the ICLID. • **For outgoing calls** The prefix is not stripped, therefore any prefixes not suitable for external line presentation should be stripped using short codes.

Table continues…

Field	Description
Outgoing Group ID	Default = 1. Range 0 to 99999. When a short code specifies a number to dial, the IP Office will seize an available line from those available with a matching **Outgoing Group ID**. In a Server Edition/Select network, the **Outgoing Group ID** used for lines to a system must be unique within the network. **Reserved Group ID Numbers:** • **0** - In a Server Edition/Select network, the ID 0 cannot be used. • **90000 - 99999** - Reserved for system use (not enforced). - **96666** - Use for ACO lines. - **98888** - For IP Office deployed in an Enterprise Branch environment, reserved for the SM line. - **99001 - 99148** - In a Server Edition/Select network, reserved for the IP Office lines from the primary and secondary servers to each expansion system in the network. - **99998** - In a Server Edition/Select network, reserved for the IP Office lines to the secondary server. - **99999** - In a Server Edition/Select network, reserved for the IP Office lines to the primary server.
Number of Channels	Default = 20. Range 1 to 250; 1 to 500 for Select systems. Defines the number of operational channels that are available on this line.
Outgoing Channels	Default = 20, Range 0 to 250; 0 to 500 for Select systems. This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as Number of Channels field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls.

Gateway

Field	Description
Address	Default = Blank. Enter the IP address of the gateway device at the remote end. This address must not be shared by any other IP line (H.323, SIP, SES or IP DECT).
Location	Default = Cloud. You can set Location values for the IP Office system and for individual extensions and lines. Associating a line with a location: • Applies the location's call admission control (CAC) settings to the line • For SIP lines that support RFC4119/RFC5139, emergency calls using the line can include the location's address information.

Table continues…

Field	Description
Password **Confirm Password**	Default = Blank. The **Password** field is enabled when **Transport Type** is set to **WebSocket Server** or **WebSocket Client**. WebSockets are bi-directional HTTP or HTTPS communication pipes initiated from a client to a server. They permit clients behind local a firewall to traverse the internet to a server by using well known ports and protocols. A matching password must be set at each end of the line.
Port	When **Transport Type** is set to **Proprietary**, the default port is 1720 and cannot be changed. When **Transport Type** is set to **WebSocket Client**, the default port is 80. The **Port** field is not available when **Transport Type** is set to **WebSocket Server**. The HTTP and HTTPS receive ports are defined at the system level in the security settings **System Details** tab.

SCN Resiliency Options

These options are only available when the **Networking Level** option is set to **SCN**. The intention of this feature is to attempt to maintain a minimal level of operation while problems with the local system are resolved.

For information on the **SCN Resiliency Options**, refer to the IP Office Resilience Overview manual.

Field	Description
Supports Resiliency	Default = Off. These fields are available when **Networking Level** is set to **SCN**. When selected, all the available options are defaulted to **On**.

Table continues…

Field	Description
Backs up my IP Phones	Default = Off. When selected, the local system shares information about the registered phones and users on those phones with the backup system. If the local system is no longer visible to the phones, the phones will reregister with the backup system. When phones have registered with the backup system, they show an **R** on their display. Note that while IP Office line settings are mergeable, changed to this setting require the IP phones to be restarted in order to become aware of the change in their failover destination. If the setting **System Settings** > **System** > **Telephony** > **Phone Failback** is set to **Automatic**, and the phone's primary server has been up for more than 10 minutes, the backup system causes idle phones to perform a failback recovery to the original system. If using resilience backup to support Avaya IP phones, **Auto-create Extn** and **Auto-create User** should not be left enabled after initial configuration or any subsequent addition of new extensions and users. Leaving auto-create options enabled on a system that is a failover target may cause duplicate extension/user records on the multi-site network under multiple failure scenarios.
Backs up my Hunt Groups	Default = Off. This option is available only on the IP Office Line connecting the Server Edition Primary server to the Server Edition Secondary server. When selected, any hunt groups the local system is advertising to the network are advertised from the backup system when fallback is required. The trigger for this occurring is phones registered with the local system registering with the backup system, ie. **Backs up my IP Phones** above must also be enabled. When used, the only hunt group members that will be available are as follows: • If the group was a distributed hunt group, those members who were remote members on other systems are still visible within the network. • Any local members who have hot desked to another system still visible within the network. When the local system becomes visible to the backup system again, the groups will return to be advertised from the local system.
Backs up my Voicemail	Default = Off. This option can be used if the local system is hosting the Voicemail Pro server being used by the network. If selected, when the local system is no longer visible to the voicemail server, the backup system acts as host for the voicemail server. In a Server Edition network, this option is only available on the H.323 trunk from the Primary Server to the Secondary Server. It is assumed to be on and is automatically set by the Resilience Administration tool. The option requires the backup system to have licenses for the Voicemail Pro features that are required to operate during any fallback period.

Table continues…

Field	Description
Backs up my IP DECT Phones	Default = Off. This option is used for Avaya IP DECT phones registered with the system. When selected, it will share information about the registered phones and users on those phones with the backup system. If the local system is no longer visible to the phones, the phones will reregister with the backup system. The users who were currently on those phones will appear on the backup system as if they had hot desked. Note that when the local system is restored to the network, the phones will not automatically re-register with it. A phone reset via either a phone power cycle or using the System Status Application is required. When phones have registered with the backup system, they will show an **R** on their display. **Note:** Only one IP Office Line can have this configuration parameter set to On.
Backs up my one-X Portal	Default = Off. This option is available on Server Edition Select deployments and only on the IP Office Line connecting the Server Edition Primary server to the Server Edition Secondary server. When set to On, this setting enables one-X Portal resiliency and turns on the backup one-X Portal on the Server Edition Secondary server.
Backs up my Conferences	Default = Off This option is available on the line from the primary to secondary server in Linux-based networks. If enabled, the secondary server will provide hosting for system meet-me conferences if the primary is not available.

Related links

IP Office Line on page 335

IP Office Line Short Codes

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP Office Line** > **Short Codes**

Incoming calls on IP Office Lines are not routed using Incoming Call Route settings.

Short codes can be added and edited using the **Add**, **Remove** and **Edit** buttons. Alternatively you can right-click on the list of existing short code to add and edit short codes.

These settings can only be edited offline. Changes to these settings require a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Related links

IP Office Line on page 335

IP Office Line VoIP Settings

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP Office Line** > **VoIP Settings**

Configuration Settings

These settings can be edited Online. Changes to these settings do not require a reboot of the system.

Field	Description
Codec Selection	Default = System Default Set the supported codecs. Where possible, Avaya recommend that you use the same set of codecs for all IP Office systems, lines, and extensions. The options are: • **System Default** - Use the codec list set in the system settings. • **Custom** - Configure a list of codec preferences for the line. - You can move codecs between the **Unused** and **Selected** sets and change the order of the codecs. - The codecs available are set by **System Settings** > **System** > **VoIP**. The possible codecs are: • **OPUS** - Supported on Linux-based IP Office systems only. • **G.711 ALAW/G.711 ULAW** • **G.729** • **G.723.1** - Supported on IP500 V2 systems only. • **G.722 64K** - Supported by Linux-based IP Office systems and on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards.
Fax Transport Support	Default = None. If enabled, when the IP Office detects fax tone, it will renegotiate the call codec as configured below. • This option requires **Re-Invite Supported**. • IP Office systems in a network support fax relay for fax calls between systems. • IP500 V2 systems can terminate T38 fax calls. • Linux-based IP Office systems can route the calls between trunks/terminals with compatible fax types. The supported options are: • **None** - Do not support fax. • **G.711** - Use G.711 to send and receive faxes. • **T38** - Use T38 to send and receive faxes. • **T38 Fallback** - Use T38 to send and receive faxes. If the call destination does not support T38, the IP Office will send a re-invite to change the transport method to **G.711**.

Table continues…

Field	Description
Call Initiation Timeout (s)	Default = 4 seconds. Range = 1 to 99 seconds. Sets how long the IP Office system should wait for a response to an attempt to initiate a call before following the alternate routes set in an ARS form.
Media Security	Default = Same as System. Secure RTP (SRTP) can be used between IP Offices to add additional security. These settings control whether SRTP is used for this line and the settings used for the SRTP. The options are: • **Same as System**: Matches the system setting at **System Settings** > **System** > **VoIP Security**. • **Disabled**: Use RTP. • **Preferred**: Attempt to use SRTP. If SRTP call setup is unsuccessful, fall back to RTP. • **Enforced**: Use SRTP. If SRTP call setup is unsuccessful, the call fails. - For calls using **Dial Emergency**, the IP Office will switch to RTP if SRTP call setup fails.
Advanced Media Security Options	Default = Same as System. Sets the requirements for SRTP when enabled. • **Same as System**: Use the same settings as configured on **System Settings** > **System** > **VoIP Security**. • **Encryptions**: Default = RTP Sets which parts of a session SRTP protects using encryption. • **Authentication**: Default = RTP and RTCP Sets which parts of the session SRTP protects using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Not adjustable. The IP Office will accept authenticated packets that have a sequence number that is higher than or within 64 packets of the highest-numbered packet already received. • **Crypto Suites**: Default = *SRTP_AES_CM_128_SHA1_80*. Set the crypto suites SRTP uses for encryption. The options are *SRTP_AES_CM_128_SHA1_32* and *SRTP_AES_CM_128_SHA1_80*.
VoIP Silence Suppression	Default = Off When enabled, when the IP Office detects silence during an IP call, it does not send any audio data. • Lines between IP Office systems using G.711 ignore this feature. • On trunks between networked IP Office systems, you must enable the setting at both ends.

Table continues…

Field	Description
Out Of Band DTMF	Default = On. Out of Band DTMF is set to on and cannot be changed.
Allow Direct Media Path	Default = On This settings controls whether calls between IP endpoints and/or lines must go through the IP Office. • If disabled, calls go through the IP Office and use its resources. RTP relay allows calls between devices using the same audio codec to not require a voice compression channel. • If enabled, calls can take routes other than through the IP Office system. Both ends must support direct media and have matching VoIP settings. For example, both ends must use the same protocol (SIP or H.323), same addressing (IPv4 or IPv6), and so on. Otherwise, the call goes through the IP Office system. - For extensions, disabling **Requires DTMF** allows the extension to attempt direct media even if the other end has differing DTMF settings.

Related links

IP Office Line on page 335

T38 Fax

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP Office Line** > **T38 Fax**

The settings are available only on IP500 V2 since it can terminate T38 fax. On the **VoIP** settings for the line type, **Fax Transport Support** must be set to **T38** or **T38 Fallback**.

These settings are mergeable.

Field	Description
Use Default Values	Default = On. If selected, all the fields are set to their default values and greyed out.
T38 Fax Version	Default = 3. During fax relay, the two gateways will negotiate to use the highest version which they both support. The options are: **0**, **1**, **2**, **3**.
Transport	Default = UDPTL (fixed). Only **UDPTL** is supported. **TCP** and **RTP** transport are not supported. For **UDPTL**, redundancy error correction is supported. Forward Error Correction (FEC) is not supported.
Redundancy Redundancy sends additional fax packets in order to increase the reliability. However increased redundancy increases the bandwidth required for the fax transport.	

Table continues…

Field	Description
Low Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for low speed V.21 T.30 fax transmissions.
High Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for V.17, V.27 and V.28 fax transmissions.
TCF Method	Default = Trans TCF. TCF = Training Check Frame.
Max Bit Rate (bps)	Default = 14400. Lower rates can be selected if the current rate is not supported by the fax equipment or is found to not be reliable.
EFlag Start Timer (msecs)	Default = 2600.
EFlag Stop Timer (msecs)	Default = 2300.
Tx Network Timeout (secs)	Default = 150.
Scan Line Fix-up	Default = On.
TFOP Enhancement	Default = On.
Disable T30 ECM	Default = Off. When selected, disabled the T.30 Error Correction Mode used for fax transmission.
Disable EFlags For First DIS	Default = Off.
Disable T30 MR Compression	Default = Off.
NSF Override	Default = Off. If selected, the NSF (Non-Standard Facility) information sent by the T38 device can be overridden using the values in the fields below. **Country Code**: Default = 0. **Vendor Code**: Default = 0.

Related links

IP Office Line on page 335

Legacy SIP DECT Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **Legacy SIP DECT Line**

A **Legacy SIP DECT Line** can be added to connect to a D100 Base Station.

Related links

Line on page 303
SIP DECT Base on page 346
SIP DECT VoIP on page 347

SIP DECT Base

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **Legacy SIP DECT Line** > **SIP DECT Base**

The IP Office can support up to four D100 Base Stations. Each connects to the IP Office using a **Legacy SIP DECT Line**.

These settings are not mergeable. Changes to these settings requires a reboot of the system.

Field	Description
Line Number	Default = Blank. A unique line number associated with the SIP DECT Base Station.
Associated Extensions	Lists the SIP DECT extensions associated with the line through the extension's **SIP DECT Line** setting.
Base Name	Default = Blank. Maximum 16 characters. A name assigned to the base station. Each base station provisioned on the IP Office must have a unique name. The field cannot be blank. The format is an alphanumeric string with no special characters.
Base MAC Address	Default = Blank. The MAC Address of the base station. If only one base station is provisioned, the field can remain at the default value. If multiple base stations are provisioned, the MAC address for each base station must be entered.
Configure Base IP	
Configure Base IP	Default = Off. Set to **On** to configure IP address attributes for the base station. When enabled, the Configure Base IP settings are displayed.
DHCP Client	Default = On. When enabled, specifies that the base station operates as a DHCP client. When enabled, not other IP address attributes can be configured.
IP Address	Default = Blank. The IP address of the base station. The IP address must be on the same subnet as one of the LAN interfaces.
IP Mask	Default = Blank. IP address mask.
IP Gateway	Default = Blank. The default gateway address

Table continues…

Field	Description
Provisioning Server	Default = IP Office interface address. The server address from where the Base Station configuration files can be retrieved.
Description	Default = Blank. Maximum 31 characters. You can use this field to enter a description for the configuration entry. The description is not used elsewhere.

Related links

Legacy SIP DECT Line on page 345

SIP DECT VoIP

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **Legacy SIP DECT Line** > **VoIP**

This form is used to configure the VoIP setting applied to calls on a **Legacy SIP DECT Line**

These settings are not mergeable. Changes to these settings requires a reboot of the system.

Field	Description
IP Address	Default = Blank. The IP address of the SIP DECT extension.
Codec Selection	Default = Custom This field defines the codec or codecs offered during call setup. The codecs available to be used are set through **System Settings** > **System** > **VoIP**. The **Codec Selection** option allows specific configuration of the codec preferences to be different from the system **Default Selection** list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs. The D100 Base Station supports only G711 codecs.
TDM > **IP Gain**	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the system TDM interface to the IP connection. This field is not shown on Linux based platforms.
IP > **TDM Gain**	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the IP connection to the system TDM interface. This field is not shown on Linux based platforms.
DTMF Support	Default =RFC2833 The D100 Base Station supports only RFC2833.
VoIP Silence Suppression	Default = Off When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.

Table continues…

Field	Description
Local Hold Music	Default = Off
Allow Direct Media Path	Default = On This settings controls whether calls between IP endpoints and/or lines must go through the IP Office. • If disabled, calls go through the IP Office and use its resources. RTP relay allows calls between devices using the same audio codec to not require a voice compression channel. • If enabled, calls can take routes other than through the IP Office system. Both ends must support direct media and have matching VoIP settings. For example, both ends must use the same protocol (SIP or H.323), same addressing (IPv4 or IPv6), and so on. Otherwise, the call goes through the IP Office system. - For extensions, disabling **Requires DTMF** allows the extension to attempt direct media even if the other end has differing DTMF settings.
Reinvite Supported	Default = Off. When enabled, Re-Invite can be used during a session to change the characteristics of the session. For example when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk. Requires the ITSP to also support **Re-Invite**.

Related links

Legacy SIP DECT Line on page 345

MS Teams Line

IP Office can be configured as the telephony service for calls made to and from Microsoft Teams. The MS Teams Line settings uses a private SIP trunk connection with Session Border Controller (SBC).

Only one MS Teams line is supported, including for networked IP Office systems. For IP Office Server Edition and Select, the line should be configured on the primary server.

For details, see the Deploying MS Teams Direct Routing with IP Office manual.

Related links

Line on page 303
MS Teams on page 348
VoIP on page 351
Engineering on page 355

MS Teams

Navigation: **Line | MS Teams Line | MS Teams**

Additional configuration information

For additional information regarding the **Media Connection Preservation** setting, see Media Connection Preservation on page 743.

Configuration settings

These settings cannot be edited online. Changes to these settings require a reboot of the system.

Changing the **In Service** setting to **Disabled** (out of service) requires a system reboot. However, changing the **In Service** setting to **Enabled** is mergeable. Configuration changes made while the line is out of service are also mergeable.

Field	Description
Line Number	Default = Auto-filled. Range = 1 to 249 *(IP500 V2)*/349 *(Server Edition)*. The line number must be unique. On IP500 V2 systems, line numbers 1 to 16 are reserved for internal hardware. • Only one MS Teams line is supported, including for networked IP Office systems. For IP Office Server Edition and Select, the line should be configured on the primary server.
In Service	Default = Enabled This option can be used to administratively disable the MS Teams Line. It does not reflect the dynamic state of the line.
Calling Number Verification	Default = Clear These settings configure the SIP trunks use of STIR protocols for calling number verification. For more details, see SIP Calling Number Verification (STIR/SHAKEN) on page 959. • **Incoming Calls Handling**: Default = System. Sets the defaults for which calls are accepted by the system based on the authentication level of the call. This default can be overridden in the individual line configuration. - **Allow All** - Allow all calls regardless of authentication level. Note this can include calls with no authentication level. - **Allow Validated** - Only accept calls which are fully or semi-authenticated. - **Allow Not Failed** - Accept all calls expect those that specifically failed authentication. Note this can include calls with no authentication level.
Domain Name	Default = Blank. An IP address or SIP domain name as required by the service provider.

Table continues…

Field	Description
Local Domain Name	Default = Blank. An IP address or SIP domain name as required by the service provider. When configured, the **Local Domain Name** value is used in the following: • **From** and **Contact** headers • **PAI header**, when the setting **SIP Line** > **SIP Advanced** > **Use Domain for PAI** is checked • **Diversion** header If both the **ITSP Domain Name** and the **Local Domain Name** are configured, then **Local Domain** takes precedence. **Local Domain Name** is not used in the **Remote Party ID** header.
Proxy Address	Default- Blank Enter the proxy address to send the packet. Example: ms-teams.com
Outgoing Group ID	Default = 97777 This value is not changeable. It can be used by short codes to route calls to the line.
Prefix	Default = Blank This prefix is added to any source number received with incoming calls.
Max Calls	Default = 10 Sets the number of simultaneous calls allowed using this line.
URI Type	Default = SIP. When **SIP** or **SIP URI** is selected, the SIP URI format is used (for example, name@example.com). This affects the **From** field of outgoing calls. The **To** field for outgoing calls always uses the format specified by the short codes used for outgoing call routing. Recommendation: When SIP Secured URI is required, the **URI Type** should be set to **SIP URI**. **SIP URI** can be used only when **Layer 4 Protocol** is set to **TLS**.
Media Connection Preservation	Default = Enabled. When enabled, the system attempts to maintain established calls despite brief network failures. Call handling features are not available when a call is in a preserved state. When the **Media Connection Preservation** setting is enabled, it applies to Avaya H.323 phones that support connection preservation.
Location	

Table continues…

Field	Description
Network Configuration TLS connections support the following ciphers: • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA	
Layer 4 Protocol	Default = TCP.
Send Port	When **Layer 4 Protocol** is set to TLS, the default setting is 5061. When **Layer 4 Protocol** is set to TCP, the default setting is 5060.
Listen Port	When **Network Configuration** is set to TLS, the default setting is 5061. When **Network Configuration** is set to TCP, the default setting is 5060.
Use Network Topology Info	Default = None. This field associates the line with the LAN interface **System Settings** > **System** > **LAN1** > **Network Topology** settings. It also applies the **System Settings** > **System** > **LAN1** > **VoIP** > **DiffServ Settings** to the outgoing traffic on the line. If **None** is selected, STUN lookup is not applied and routing is determined by the system's routing tables. If no STUN server address is set for the interface, then the **System | LAN | Network Topology | Binding Refresh TimeSystem Settings** > **System** > **LAN1** > **Network Topology** > **Binding Refresh Time** is ignored by MS Teams Lines when calculating the periodic OPTIONS timing unless the **Firewall/NAT Type** is set to **Open Internet**.
Session Time (seconds)	Default = 1200. Range = 90 to 64800 This field specifies the session expiry time. At the halfway point of the expiry time, a session refresh message is sent. Setting the **Session Time (seconds)** to **On Demand** disables the session timer.
Description	Default = Blank. Maximum 31 characters. You can use this field to enter a description for the configuration entry. The description is not used elsewhere.

Related links

MS Teams Line on page 348

VoIP

Navigation: **Line | MS Teams Line | VoIP**

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. Note that the default order for G.711 codecs varies to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The codecs available in this form are set through the codec list and the System Default settings are on **System Settings** > **System** > **VoIP**. Within a network of systems, it is strongly recommended that all the systems and the lines connecting those systems use the same codecs. The options are: • **System Default** This is the default setting. When selected, the codec list below matches the codecs set in the system wide list. • **Custom** This option allows specific configuration of the codec preferences to be different from the system list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.
Fax Transport Support	Default = None. If enabled, when the IP Office detects fax tone, it will renegotiate the call codec as configured below. • This option requires **Re-Invite Supported**. • IP Office systems in a network support fax relay for fax calls between systems. • IP500 V2 systems can terminate T38 fax calls. • Linux-based IP Office systems can route the calls between trunks/terminals with compatible fax types. The supported options are: • **None** - Do not support fax. • **G.711** - Use G.711 to send and receive faxes. • **T38** - Use T38 to send and receive faxes. • **T38 Fallback** - Use T38 to send and receive faxes. If the call destination does not support T38, the IP Office will send a re-invite to change the transport method to **G.711**.
Call Initiation Timeout (s)	Default = 4 seconds. Range = 1 to 99 seconds. Sets how long the IP Office system should wait for a response to an attempt to initiate a call before following the alternate routes set in an ARS form.

Table continues…

Field	Description
DTMF Support	Default = RFC2833 (IP500 V2), RFC2833/RFC4733 (Linux-Based Server) Sets how the IP Office signals DTMF key press digits to the remote end. The options are: • **In Band** - Send digits as tones within the call audio. • **RFC2833** or **RFC2833/RF4733** - Send digits using a separate audio stream from the call audio. If not supported by the far end, the line reverts to using **In Band** signaling. • **Info** - Send the digits in SIP `INFO` packets.
Media Security	Default = Same as System. These setting controls and settings of SRTP that is used for the selected line. The options are: • **Same as System**: Matches the system setting at **System Settings** > **System** > **VoIP Security**. • **Disabled**: Use RTP. • **Preferred**: Attempt to use SRTP. If SRTP call setup is unsuccessful, fall back to RTP. • **Enforced**: Use SRTP. If SRTP call setup is unsuccessful, the call fails. - For calls using **Dial Emergency**, the IP Office will switch to RTP if SRTP call setup fails.
Advanced Media Security Options	Default = Same as System. Sets the requirements for SRTP when enabled. • **Same as System**: Use the same settings as configured on **System Settings** > **System** > **VoIP Security**. • **Encryptions**: Default = RTP Sets which parts of a session SRTP protects using encryption. • **Authentication**: Default = RTP and RTCP Sets which parts of the session SRTP protects using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Not adjustable. The IP Office will accept authenticated packets that have a sequence number that is higher than or within 64 packets of the highest-numbered packet already received. • **Crypto Suites**: Default = *SRTP_AES_CM_128_SHA1_80*. Set the crypto suites SRTP uses for encryption. The options are *SRTP_AES_CM_128_SHA1_32* and *SRTP_AES_CM_128_SHA1_80*.

Table continues…

Field	Description
VoIP Silence Suppression	Default = Off When enabled, when the IP Office detects silence during an IP call, it does not send any audio data. • Lines between IP Office systems using G.711 ignore this feature. • On trunks between networked IP Office systems, you must enable the setting at both ends.
Re-Invite Supported	Default = Off. When enabled, the IP Office can use `Re-Invite` during a call to change the characteristics of the call. For example, when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk. • Requires the ITSP to also support `Re-Invite`. • This setting must be enabled for video support.
Codec Lockdown	Default = Off. After making a SIP offer with a list of codecs, the IP Office expects an answer with a single codec selected from the list. User agents that send an answer with multiple codecs expect to switch to any of those codecs during the call without further negotiation, which the IP Office does not support. Instead, loss of speech occurs if the user agent changes codec without renegotiating. • If enabled, when the IP Office receives an answer with multiple codecs, the IP Office sends a `re-INVITE` and a SIP offer with just one codec. • This option requires **Re-Invite Supported** enabled.
Allow Direct Media Path	Default = On This settings controls whether calls between IP endpoints and/or lines must go through the IP Office. • If disabled, calls go through the IP Office and use its resources. RTP relay allows calls between devices using the same audio codec to not require a voice compression channel. • If enabled, calls can take routes other than through the IP Office system. Both ends must support direct media and have matching VoIP settings. For example, both ends must use the same protocol (SIP or H.323), same addressing (IPv4 or IPv6), and so on. Otherwise, the call goes through the IP Office system. - For extensions, disabling **Requires DTMF** allows the extension to attempt direct media even if the other end has differing DTMF settings.
Force direct media with phones	Default = On When enabled, if an Avaya IP phone dials digits during a direct media call, the IP Office changes the call to indirect media and sends the digits as RFC2833. 15-seconds after the last digit, the IP Office changes the call back to direct media. • This setting is requires the line to have **Re-Invite Supported** and **Allow Direct Media Path** enabled, and **DTMF Support** set to **RFC2833/RF4733**.

Table continues…

Field	Description
G.711 Fax ECAN	Default = Off When enabled, if the IP Office detects a fax call, it switches to G.711 with echo cancellation (ECAN) based on the 'G.711 Fax ECAN field, NLP disabled, a fixed jitter buffer, and silence suppression is disabled. You can use this to avoid an ECAN mismatch with the trunk provider. • This setting is only available on IP500 V2 systems when **Fax Transport Support** is set to **G.711** or **T38 Fallback**.

Related links

MS Teams Line on page 348

Engineering

Navigation: **Line | MS Teams Line | Engineering**

You can use this tab to enter commands that apply special features to the SIP line. The commands are called SIP Line Custom (SLIC) strings.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

reINVITE Codec Renegotiation

For R11.0 and higher, the IP Office supports codec renegotiation when a `reINVITE` is received. See Codec selection on page 950.

You can use the following command to retain the pre-R11.0 behavior of no renegotiation. Note: On existing IP Office systems upgraded to R11.0 or higher, this command is automatically added to all existing SIP lines.

- `SLIC_PREFER_EXISTING_CODEC`

Calling Number Validation

You can use the following commands to control calling number validation. See SIP Calling Number Verification (STIR/SHAKEN) on page 959.

- `SLIC_STIR_REJECT_CODE=<n>` where `<n>` is the response code sent for calls rejected by the IP Office.
- `SLIC_STIR_REJECT_STRING=<y>` where `<y>` is the response string sent for calls rejected by the IP Office.
- `SLIC_STIR_ATTEST="<w>"` where `<w>` is the name of the header the IP Office checks for a call's authorization level.
- `SLIC_STIR_CUSTOM=<z>` where `<z>` value enables or disables various call features.

Server Name Identification (SNI)

The following SLIC codes can be used for SIP trunks using TLS. When used:

- On outgoing connections, the IP Office adds Server Name Indication (SNI) information to the SAN field it sends.

- If the IP Office system's **Received certificate checks (Telephony endpoints)** settings is set to **Medium + Remote Checks** or **High + Remote Checks**, then the SLIC value is also used to validate the received certificates SAN.

The SLIC codes are:

- `SLI_ADD_SIP_SAN=<X>`

  Use a SNI set to `sip:<SNI>` where the `<SNI>` value is taken from the existing IP Office SIP line configuration based on the following values of `<X>` as below:

  - `D` = Use the value of the SIP line's **ITSP Domain Name** setting (**Line** > **SIP Line**). For example, for a SIP line with the **ITSP Domain Name** set to `ipo.example.com`, adding `SLIC_ADD_SIP_SAN=D` sets the SNI added to `sip:ipo.example.com`.
  - `P` = Use the value of the SIP line's configured **ITSP Proxy Address** setting (**Line** > **Transport** > **)**. This option is only supported for a **ITSP Proxy Address** set to a single address. For example: `SLI_ADD_SIP_SAN=P`

Keepalives

Supported with IP Office R11.1.3.1 and higher.

You can add `SLIC_HNT_EMPTY_PACKET` to have the SIP line send RTP packets with payload 20 (unassigned payload) and no data as keepalives. This overrides the default of send STUN packets for keepalives.

Related links

MS Teams Line on page 348

PRI Trunks

PRI trunks are provided by the installation of a PRI trunk card into the control unit. avThe IP500 PRI-U trunk card can be configured (see below) to one of those line types. The cards are also available with either 1 or 2 physical ports. The number of B-channels supported by each physical port depends on the line type of the card.

- **E1**: 30 B-channels and 1 D-channel per port.
- **T1**: 24 B-channels per port.
- **US PRI**: 23 B-channels and 1 D-channel per port.
- **E1-R2**: 30 B-channels and 1 D-channel per port.

IP500 PRI-U Trunk Card Line Type

The IP500 PRI-U card can be configured to support either E1, T1 or E1-R2 PRI line types. To select the line type required, right-click on the line in the group or navigation pane and select **Change Universal PRI Card Line Type**.

The control unit supports 8 B-channels on each IP500 PRI-U card fitted. Additional B-channels up to the full capacity of IP500 PRI-U ports installed require licenses added to the configuration. D-channels are not affected by licensing.

- For ETSI and QSIG trunks, license instances are consumed by the number of calls in progress on B-channels.
- For T1, E1R2 and ETSI CHI trunks, licenses instances are consumed by the channels set as in service.

Related links

Line on page 303

E1 Line

Related links

Line on page 303
E1 PRI Line on page 357
E1 Short Codes on page 363
E1 PRI Channels on page 363

E1 PRI Line

Navigation: **System Settings** > **Line** > **E1 PRI Line**

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Line Number	This parameter is not configurable; it is allocated by the system.
Line Sub Type	Select to match the particular line type provided by the line provider. The options are: • **ETSI** • **ETSI CHI** • **QSIG A** • **QSIG B** **ETSI CHI** is used to send the channel allocation ID (CHI) in the call setup signaling. This is a request to use a particular B-channel rather than use any B-channel allocated by the central office exchange. QSIG trunks are not supported on IP500 V2 systems without IP500 Voice Networking licenses.

Table continues…

Field	Description
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Network Type	Default = Public. This option is available when **System | Telephony | Telephony | Restrict Network Interconnect** is enabled. It allows you to configure trunks as either **Public** or **Private**. • The IP Office will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or the opposite. • The call restriction includes transfers, forwarding and conference calls. • Avaya does not recommended use of this feature on IP Office systems using any of the following features: multi-site networks, VPNremote, application telecommuter mode.
Telephone Number	Used to remember the external telephone number of this line to assist with loop-back testing. For information only.
Channel Allocation	Default = 30|1. For lines set to **ETSI CHI**, this option allows the system to select the default order in which channels should be used for outgoing calls. Typically this is set as the opposite of the default order in which the central office exchange uses channels for incoming calls. For lines set to the **Line Sub Type** of **ETSI CHI**, the **Incoming Group ID** is set as part of the individual channel settings.
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.

Table continues…

Field	Description
Outgoing Group ID	Default = 1. Range 0 to 99999. When a short code specifies a number to dial, the IP Office will seize an available line from those available with a matching **Outgoing Group ID**. In a Server Edition/Select network, the **Outgoing Group ID** used for lines to a system must be unique within the network. **Reserved Group ID Numbers:** • **0** - In a Server Edition/Select network, the ID 0 cannot be used. • **90000 - 99999** - Reserved for system use (not enforced). - **96666** - Use for ACO lines. - **98888** - For IP Office deployed in an Enterprise Branch environment, reserved for the SM line. - **99001 - 99148** - In a Server Edition/Select network, reserved for the IP Office lines from the primary and secondary servers to each expansion system in the network. - **99998** - In a Server Edition/Select network, reserved for the IP Office lines to the secondary server. - **99999** - In a Server Edition/Select network, reserved for the IP Office lines to the primary server.
Prefix	Default = Blank. The prefix is used in the following ways: • **For incoming calls** The ISDN messaging tags indicates the call type (National, International or Unknown). If the call type is unknown, then the number in the Prefix field is added to the ICLID. • **For outgoing calls** The prefix is not stripped, therefore any prefixes not suitable for external line presentation should be stripped using short codes.
National Prefix	Default = 0 This indicates the digits to be prefixed to a incoming national call. When a number is presented from ISDN as a "national number" this prefix is added. For example 1923000000 is converted to 01923000000.
International Prefix	Default = 00 This indicates the digits to be prefixed to an incoming international call. When a number is presented from ISDN as an "international number" this prefix is added. For example 441923000000 is converted to 00441923000000.
TEI	Default = 0 The Terminal Equipment Identifier. Used to identify each Control Unit connected to a particular ISDN line. For Point to Point lines this is typically (always) 0. It can also be 0 on a Point to Multi-Point line, however if multiple devices are sharing a Point to Multi-Point line it should be set to 127 which results in the exchange deciding on the TEI's to be used.

Table continues…

Field	Description
Number of Channels	Defines the number of operational channels that are available on this line. Up to 30 for E1 PRI, 23 for T1 PRI.
Outgoing Channels	This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as **Number of Channels** field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls. Only available when the **Line Sub Type** is set to **ETSI**.
Voice Channels	The number of channels available for voice use. Only available when the **Line Sub Type** is set to **ETSI**.
Data Channels	The number of channels available for data use. Only available when the **Line Sub Type** is set to **ETSI**.
CRC Checking	Default = On Switches CRC on or off.
Line Signalling	Default = CPE This option is not used for lines where the **Line SubType** is set to **QSIG**. Select either **CPE** (customer premises equipment) or **CO** (central office). The **CO** feature is intended to be used primarily as a testing aid. It allows PRI lines to be tested in a back-to-back configuration, using crossover cables. The CO feature operates on this line type by modifying the way in which incoming calls are disconnected for system configuration in Brazil and Argentina. In these locales, the CO setting uses Forced-Release instead of Clear-Back to disconnect incoming calls. The Brazilian Double-Seizure mechanism, used to police Collect calls, is also disabled in CO mode.
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available. • Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source. • In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.

Table continues…

Field	Description
Add 'Not-end-to-end ISDN' Information Element	Default = Never Sets whether the optional 'Not end-to-end ISDN' information element should be added to outgoing calls on the line. The options are: • **Never** • **Always** • **POTS**(only if the call was originated by an analog extension). The default is **Never** except for the following locales: • for Italy the default is **POTS**. • for New Zealand the default is **Always**.
Progress Replacement	Default = None. Progress messages are defined in the Q.931 ISDN connection control signaling protocol. Generally, if a progress message is sent, the caller does not get connected and so typically does not accrue call costs. Not all ISDN lines support Q.931 Progress messages. Use this setting to configure alternative signaling to the ISDN line for internally generated Progress messages. The options are: • **Alerting**: Map to Q.931 Alerting. The call is not connected. The caller does not hear the message and typically does not accrue call costs. • **Connect**: Map to Q.931 Connect. The caller hears the message and typically will accrue call costs.
Supports Partial Rerouting	Default = Off. Partial rerouting (PR) is an ISDN feature. It is supported on external (non-network and QSIG) ISDN exchange calls. When an external call is transferred to another external number, the transfer is performed by the ISDN exchange and the channels to the system are freed. Use of this service may need to be requested from the line provider and may incur a charge.
Force Number Plan to ISDN	Default = Off. This option is only configurable when **Support Partial Rerouting** is also enabled. When selected, the plan/type parameter for Partial Rerouting is changed from **Unknown/Unknown** to **ISDN/Unknown**.
Send Redirecting Number	Default = Off. This option can be used on ISDN trunks where the redirecting service is supported by the trunk provider. Where supported, on twinned calls the caller ID of the original call is passed through to the twinning destination. This option is only used for twinned calls.

Table continues…

Field	Description
Support Call Tracing	Default = Off. The system supports the triggering of malicious caller ID (MCID) tracing at the ISDN exchange. Use of this feature requires liaison with the ISDN service provider and the appropriate legal authorities to whom the call trace will be passed. The user will also need to be enabled for call tracing and be provider with either a short code or programmable button to activate MCID call trace. Refer to Malicious Call Tracing in the Telephone Features section for full details.
Active CCBS Support	Default = Off. Call completion to a busy subscriber (CCBS). It allows automatic callback to be used on outgoing ISDN calls when the destination is busy. This feature can only be used on point-to-point trunks. Use of this service may need to be requested from the line provider and may incur a charge.
Passive CCBS	Default = Off.
Cost Per Charging Unit	Advice of charge (AOC) information can be output in SMDR. The information is provided in the form of charge units. This setting is used to enter the call cost per charging unit set by the line provider. The values are 1/10,000th of a currency unit. For example if the call cost per unit is £1.07, a value of 10700 should be set on the line. See Advice of Charge on page 738.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.
Send original calling party for forwarded and twinning calls	Default = Off. Use the original calling party ID when forwarding calls or routing twinned calls. This setting applies to the following ISDN lines: • PRI24 with subtypes: PRI, QSIGA, QSIGB, ETSI, ETSI CHI. • PRI30 with subtypes: QSIGA, QSIGB, ETSI, ETSI CHI.
Originator number for forwarded and twinning calls	Default = blank. The number used as the calling party ID when forwarding calls or routing twinned calls. This field is grayed out when the **Send original calling party for forwarded and twinning calls** setting is enabled. This setting applies to the following ISDN lines: • PRI24 with subtypes: PRI, QSIGA, QSIGB, ETSI, ETSI CHI. • PRI30 with subtypes: QSIGA, QSIGB, ETSI, ETSI CHI.

The following fields are shown for a US T1 trunk card set to ETSI or QSIG operation. These cards have the same settings E1 PRI trunk cards set to ETSI or QSIG but only support 23 channels.

These settings are not mergeable. Changing these settings requires a system reboot.

Field	Description
CSU Operation	Check this field to enable the T1 line to respond to loop-back requests from the line.
Haul Length	Default = 0-115 feet Sets the line length to a specific distance.
Channel Unit	Default = Foreign Exchange This field should be set to match the channel signaling equipment provided by the Central Office. The options are Foreign Exchange, Special Access or Normal.

Related links

E1 Line on page 357

E1 Short Codes

Navigation: **System Settings** > **Line** > **E1 Short Codes**

For some types of line, Line short codes can be applied to any digits received with incoming calls.

The line Short Code tab is shown for the following trunk types which are treated as internal or private trunks: **QSIG** (T1, E1, H.323), **BRI S0**, **H.323**, **SCN**, **IP Office**. Incoming calls on those types of trunk are not routed using **Incoming Call Route** settings. Instead the digits received with incoming calls are checked for a match as follows:

Extension number (including remote numbers in a multi-site network).

- Line short codes (excluding ? short code).
- System short codes (excluding ? short code).
- Line ? short code.
- System ? short code.

Short codes can be added and edited using the **Add**, **Remove** and **Edit** buttons. Alternatively you can right-click on the list of existing short code to add and edit short codes.

These settings can be edited online.

Related links

E1 Line on page 357

E1 PRI Channels

Navigation: **System Settings** > **Line** > **E1 PRI Channels**

This tab allows settings for individual channels within the trunk to be adjusted. To edit a channel either double-click on it or click the channel and then select **Edit**.

To edit multiple channels at the same time, select the required channels using Ctrl or Shift and then click **Edit**. When editing multiple channels, fields that must be unique such as **Line Appearance ID** are not shown.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Line Appearance ID	Default = Auto-assigned. Range = 2 to 9 digits. Used for configuring Line Appearances with button programming. The line appearance ID must be unique and not match any extension number. Line appearance is not supported for trunks set to QSIG operation and is not recommended for trunks be used for DID. If the trunk **Line Sub Type** is set to **ETSI CHI**, outgoing line appearance calls must use the corresponding channel.

The following additional fields are shown for lines where the **Line Sub Type** is set to **ETSI CHI**.

Field	Description
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.
Outgoing Group ID	Default = 1. Range 0 to 99999. When a short code specifies a number to dial, the IP Office will seize an available line from those available with a matching **Outgoing Group ID**. In a Server Edition/Select network, the **Outgoing Group ID** used for lines to a system must be unique within the network. **Reserved Group ID Numbers:** • **0** - In a Server Edition/Select network, the ID 0 cannot be used. • **90000 - 99999** - Reserved for system use (not enforced). - **96666** - Use for ACO lines. - **98888** - For IP Office deployed in an Enterprise Branch environment, reserved for the SM line. - **99001 - 99148** - In a Server Edition/Select network, reserved for the IP Office lines from the primary and secondary servers to each expansion system in the network. - **99998** - In a Server Edition/Select network, reserved for the IP Office lines to the secondary server. - **99999** - In a Server Edition/Select network, reserved for the IP Office lines to the primary server.
Direction	Default = Bothways The direction of calls on the channel. The options are:**Incoming**, **Outgoing**, **Bothways**.
Bearer	Default = Any The type of traffic carried by the channel. The options are: **Voice**, **Data**, **Any**.

Table continues…

Field	Description
Admin	Default = Out of Service. This field can be used to indicate whether the channel is in use or not. On trunks where only a limited number of channels have been requested from the trunk provider (known as sub-equipped trunks), those channels not provided should be set as **Out of Service**. For channels that are available but are temporarily not being used select **Maintenance**.
Tx Gain	Default = 0dB. Range = -10dBb to +5dB. The transmit gain in dB.
Rx Gain	Default = 0dB. Range = -10dBb to +5dB. The receive gain in dB.

Related links

E1 Line on page 357

E1 R2 Line

Related links

Line on page 303
E1-R2 Options on page 365
E1-R2 Channels on page 367
E1–R2 MFC Group on page 369
E1-R2 Advanced on page 369

E1-R2 Options

Navigation: **System Settings** > **Line** > **E1–R2 Options**

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.

Table continues…

Field	Description
Network Type	Default = Public. This option is available when **System | Telephony | Telephony | Restrict Network Interconnect** is enabled. It allows you to configure trunks as either **Public** or **Private**. • The IP Office will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or the opposite. • The call restriction includes transfers, forwarding and conference calls. • Avaya does not recommended use of this feature on IP Office systems using any of the following features: multi-site networks, VPNremote, application telecommuter mode.
Line Number	Allocated by the system.
Line SubType	Default = E1-R2 The options are: • **E1-R2** • **ETSI** • **QSIGA** • **QSIGB** QSIG trunks trunks are not supported on IP500 V2 systems without IP500 Voice Networking licenses.
Channel Allocation	Default = 30 | 1 The order, **30 | 1** or **1 | 30**, in which channels are used.
Country (Locale)	Default = Mexico. Select the locale that matches the area of usage. Note that changing the locale will return the MFC Group settings to the defaults for the selected locale. Currently supported locales are: • **Argentina** • **Brazil** • **China** • **India** • **Korea** • **Mexico** • **None**

Table continues…

Field	Description
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected. The table at the base of the form displays the settings for the individual channels provided by the line. For details of the channel settings see the E1-R2 Channel form. To edit a channel, either double-click on it or right-click and select **Edit**. This will display the Edit Channel dialog box. To edit multiple channels at the same time select the channels whilst pressing the Shift or Ctrl key. Then right-click and select **Edit**.

Related links

E1 R2 Line on page 365

E1-R2 Channels

Navigation: **System Settings** > **Line** > **E1–R2 Channels**

The channel settings are split into two sub-tabs, **E1R2 Edit Channel** and **Timers**.

The **Timers** tab displays the various timers provided for E1-R2 channels. These should only be adjusted when required to match the line provider's settings.

This tab allows settings for individual channels within the trunk to be adjusted. To edit a channel, select the required channel or channels and click **Edit**.

The following settings are mergeable: **Incoming Group ID**, **Outgoing Group ID**, **Admin**.

The remaining settings are not mergeable. Changes to these settings require a system reboot.

Field	Descriptions
Channel	The channel or channels being edited.
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.

Table continues…

Field	Descriptions
Outgoing Group ID	Default = 1. Range 0 to 99999. When a short code specifies a number to dial, the IP Office will seize an available line from those available with a matching **Outgoing Group ID**. In a Server Edition/Select network, the **Outgoing Group ID** used for lines to a system must be unique within the network. **Reserved Group ID Numbers:** • **0** - In a Server Edition/Select network, the ID 0 cannot be used. • **90000 - 99999** - Reserved for system use (not enforced). - **96666** - Use for ACO lines. - **98888** - For IP Office deployed in an Enterprise Branch environment, reserved for the SM line. - **99001 - 99148** - In a Server Edition/Select network, reserved for the IP Office lines from the primary and secondary servers to each expansion system in the network. - **99998** - In a Server Edition/Select network, reserved for the IP Office lines to the secondary server. - **99999** - In a Server Edition/Select network, reserved for the IP Office lines to the primary server.
Direction	Default = Both Directions The direction of calls on the channel. The options are: **Incoming**, **Outgoing**, **Both Directions**.
Bearer	Default = Any The type of traffic carried by the channel. The options are: **Voice**, **Data**, **Any**.
Admin	Default = Out of Service. This field can be used to indicate whether the channel is in use or not. On trunks where only a limited number of channels have been requested from the trunk provider (known as sub-equipped trunks), those channels not provided should be set as **Out of Service**. For channels that are available but are temporarily not being used select **Maintenance**.

Table continues…

Field	Descriptions
Line Signaling Type	Default = R2 Loop Start The signaling type used by the channel. Current supported options are: • **R2 Loop Start** • **R2 DID** • **R2 DOD** • **R2 DIOD** • **Tie Immediate Start** • **Tie Wink Start** • **Tie Delay Dial** • **Tie Automatic** • **WAN Service** • **Out of Service**
Dial Type	Default = MFC Dialing The type of dialing supported by the channel. The options are: **MFC Dialing**, **Pulse Dialing**, **DTMF Dialing**.

Related links

E1 R2 Line on page 365

E1–R2 MFC Group

Navigation: **System Settings** > **Line** > **E1–R2 MFC Group**

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

These tabs show the parameter assigned to each signal in an MFC group. The defaults are set according to the Country (Locale) on the Line tab. All the values can be returned to default by the **Default All** button on the **Advanced** tab.

These settings are not mergeable. Changes to these settings will require a reboot of the system.

To change a setting either double-click on it or right-click and select **Edit**.

Related links

E1 R2 Line on page 365

E1-R2 Advanced

Navigation: **System Settings** > **Line** > **E1–R2 Advanced**

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Zero Suppression	Default = HDB3 Selects the method of zero suppression used (HDB3 or AMI).
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available. • Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source. • In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.
Line Signaling	Default = CPE The options are: • **CPE** • **CO** • **CO** The feature is intended to be used primarily as a testing aid. It allows T1 and E1 lines to be tested in a back-to-back configuration, using crossover (QSIG) cables. The CO feature operates by modifying the way in which incoming calls are disconnected for system configuration in Brazil and Argentina. In these locales, the CO setting uses Forced-Release instead of Clear-Back to disconnect incoming calls. The Brazilian Double-Seizure mechanism used to police Collect calls, is also disabled in CO mode.
Incoming Routing Digits	Default = 4 Sets the number of incoming digits used for incoming call routing.
CRC Checking	Default = On Switches CRC on or off.
Default All Group Settings	Default the MFC Group tab settings.
Line Signaling Timers	To edit one of these timers, either double-click on the timer or right-click on a timer and select the action required.

Related links

E1 R2 Line on page 365

T1 Line

Related links

Line on page 303
US T1 Line on page 371
T1 Channels on page 373

US T1 Line

Navigation: **System Settings** > **Line** > **US T1 Line**

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Line Number	Allocated by the system.
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Network Type	Default = Public. This option is available when **System | Telephony | Telephony | Restrict Network Interconnect** is enabled. It allows you to configure trunks as either **Public** or **Private**. • The IP Office will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or the opposite. • The call restriction includes transfers, forwarding and conference calls. • Avaya does not recommended use of this feature on IP Office systems using any of the following features: multi-site networks, VPNremote, application telecommuter mode.
Line Sub Type	Default = T1 Set to T1 for a T1 line.
Channel Allocation	Default = 24 | 1 The order, 24 to 1 or 1 to 24, in which channels are used.
Prefix	Default = Blank Enter the number to prefix to all incoming numbers for callback. This is useful if all users must dial a prefix to access an outside line. The prefix is automatically placed in front of all incoming numbers so that users can dial the number back.

Table continues…

Field	Description
Framing	Default = ESF Selects the type of signal framing used. The options are: • **ESF** • **D4**
Zero Suppression	Default = B8ZS Selects the method of zero suppression used. The options are: • **B8ZS** • **AMI ZCS**
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available. • Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source. • In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.
Haul Length	Default = 0-115 feet. Sets the line length to a specific distance.
Channel Unit	Default = Foreign Exchange This field should be set to match the channel signaling equipment provided by the Central Office. The options are: • **Foreign Exchange** • **Special Access** • **Normal**
CRC Checking	Default = On Turns CRC on or off.
Line Signaling	Default = CPE This field affects T1 channels set to Loop-Start or Ground-Start. The field can be set to either CPE (Customer Premises Equipment) or CO (Central Office). This field should normally be left at its default of CPE. The setting CO is normally only used in lab back-to-back testing.

Table continues…

Field	Description
Incoming Routing Digits	Default=0 (present call immediately) Sets the number of routing digits expected on incoming calls. This allows the line to present the call to the system once the expected digits have been received rather than waiting for the digits timeout to expire. This field only affects T1 line channels set to E&M Tie, E&M DID, E&M Switched 56K and Direct Inward Dial.
CSU Operation	Enable this field to enable the T1 line to respond to loop-back requests from the line.
Enhanced Called Party Number	Default = Off This option is not supported for systems set to the United States locale. Normally the dialed number length is limited to 15 digits. Selecting this option increases the allowed dialed number length to 30 digits.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.

Related links

T1 Line on page 371

T1 Channels

Navigation: **System Settings** > **Line** > **T1 Channels**

The settings for each channel can be edited. Users have the option of editing individual channels by double-clicking on the channel or selecting and editing multiple channels at the same time. Note that the Line Appearance ID cannot be updated when editing multiple channels.

When editing a channel or channels, the settings available are displayed on two sub-tabs; T1 Edit Channel and Timers.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Channel	Allocated by the system.
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.

Table continues…

Field	Description
Outgoing Group ID	Default = 1. Range 0 to 99999. When a short code specifies a number to dial, the IP Office will seize an available line from those available with a matching **Outgoing Group ID**. In a Server Edition/Select network, the **Outgoing Group ID** used for lines to a system must be unique within the network. **Reserved Group ID Numbers:** • **0** - In a Server Edition/Select network, the ID 0 cannot be used. • **90000 - 99999** - Reserved for system use (not enforced). - **96666** - Use for ACO lines. - **98888** - For IP Office deployed in an Enterprise Branch environment, reserved for the SM line. - **99001 - 99148** - In a Server Edition/Select network, reserved for the IP Office lines from the primary and secondary servers to each expansion system in the network. - **99998** - In a Server Edition/Select network, reserved for the IP Office lines to the secondary server. - **99999** - In a Server Edition/Select network, reserved for the IP Office lines to the primary server.
Line Appearance ID	Default = Auto-assigned. Range = 2 to 9 digits. Used for configuring Line Appearances with button programming. The line appearance ID must be unique and not match any extension number. Line appearance is not supported for trunks set to QSIG operation and is not recommended for trunks be used for DID.
Direction	Default = Bothway The direction of calls on the channel. The options are: • **Incoming** • **Outgoing** • **Bothway**
Bearer	Default = Any The type of traffic carried by the channel. The options are: **Voice**, **Data**, **Any**.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.

Table continues…

Field	Description
Type	Default = Loop-Start. The T1 emulates the following connections: • **Ground-Start** • **Loop-Start** • **E&M - TIE** • **E&M - DID** • **E&M Switched 56K** • **Direct Inward Dial** • **Clear Channel 64K** Trunks set to **E&M - DID** will only accept incoming calls. If **E&M - TIE** is selected and the **Outgoing Trunk Type** is set to **Automatic**, no secondary dial tone is provided for outgoing calls on this line/trunk.
Dial Type	Default = DTMF Dial Select the dialing method required. The options are: **DTMF Dial**, **Pulse Dial**.
Incoming Trunk Type	Default = Wink-Start Used for E&M types only. The handshake method for incoming calls. The options are
Outgoing Trunk Type	Default = Wink-Start Used for E&M types only. The handshake method for outgoing calls. The options are: **Automatic**, **Immediate**, **Delay Dial**, **Wink-Start**. If the line Type is set to **E&M-TIE** and the **Outgoing Trunk Type** is set to **Automatic**, no secondary dial tone is provided for outgoing calls on this line/trunk.
Tx Gain	Default = 0dB. The transmit gain in dB.
Rx Gain	Default = 0dB. The receive gain in dB.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.

Timer Settings

This sub-tab allows various timers relating to operation of an individual channel to be adjusted. These should only be adjusted to match the requirements of the line provider. The following is a list of the default values. To reset a value, click on the current value and then right click and select from the default, minimize and maximize options displayed.

Incoming Automatic Delay: 410.

Incoming Wink Delay: 100.

Wink Signal: 200.

Incoming Dial Guard: 50.

First Incoming Digit: 15000.

Incoming Inter Digit: 5000.

Maximum Inter Digit: 300.

Flash Hook Detect: 240.

Incoming Disconnect: 300.

Incoming Disconnect Guard: 800.

Disconnected Signal Error: 240000.

Outgoing Disconnect: 300.

Outgoing Disconnect Guard: 800.

Ring Verify Duration: 220.

Ring Abandon: 6300.

Ping Verify: 600.

Long Ring Time: 1100.

Silent Interval: 1100.

Outgoing Seizure: 10.

Wink Start: 5000.

Wink Validated: 80.

Wink End: 350.

Delay End: 5000.

Outgoing Dial Guard: 590.

Outgoing IMM Dial Guard: 1500.

Outgoing Pulse Dial Break: 60.

Outgoing Pulse Dial Make: 40.

Outgoing Pulse Dial Inter Digit: 720.

Outgoing Pulse Dial Pause: 1500.

Flash Hook Generation: 500.

Outgoing End of Dial: 1000.

Answer Supervision: 300.

Incoming Confirm: 20.

Related links

T1 Line on page 371

SIP Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line**

IP Office supports SIP voice calls through the addition of SIP lines to the system configuration. This approach allows users with non-SIP phones to make and receive SIP calls.

Deleting a SIP line requires a “merge with service disruption”. When the configuration file is sent to the system, the SIP trunk is restarted and all calls on the line are dropped.

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 806.

Related links

Line on page 303
SIP Line on page 377
SIP Line I Transport on page 381
Call Details on page 384
SIP Line VoIP on page 391

T.38 Fax on page 395
SIP Line Credentials on page 397
SIP Line Advanced on page 398
SIP Line Engineering on page 404

SIP Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Line**

Configuration Settings

These settings are mergeable with the exception of the **Line Number** setting. Changing the **Line Number** setting requires a “merge with service disruption”. When the configuration file is sent to the system, the SIP trunk is restarted and all calls on the line are dropped.

Offline editing is not required.

Field	Description
Line Number	Default = Auto-filled. Range = 1 to 249 *(IP500 V2)*/1 to 349 *(Server Edition)*. The line number must be unique for each line in the configuration. IP500 V2 systems reserved line numbers 1 to 16 for internal hardware.
ITSP Domain Name	Default = Blank. This field is used to specify the default host part of the SIP URI in the `From`, `To`, and `R-URI` fields for outgoing calls. For example, in the SIP URI `name@example.com`, the host part of the URI is `example.com`. When empty, the default host is provided by the **SIP Line** > **SIP Transport** > **ITSP Proxy Address** field value. If multiple addresses are defined in the **ITSP Proxy Address** field, then this field must be defined. For the user making the call, the user part of the From SIP URI is determined by the settings of the SIP URI channel record being used to route the call (see **SIP Line** > **SIP URI** > **Local URI**). This will use one of the following: • a specific name entered in Local URI field of the channel record. • or specify using the primary or secondary authentication name set for the line below. • or specify using the SIP Name set for the user making the call (**Call Management** > **Users** > **Add/Edit Users** > **SIP** > **SIP Name**). For the destination of the call, the user part of the To and R-URI fields are determined by dial short codes of the form 9N/N"@example.com” where N is the user part of the SIP URI and "@example.com" is optional and can be used to override the host part of the To and R-URI.

Table continues…

Field	Description
Local Domain Name	Default = Blank. An IP address or SIP domain name as required by the service provider. When configured, the **Local Domain Name** value is used in • the `From` and `Contact` headers • the `PAI` header, if **Line** > **SIP Advanced** is checked • the `Diversion` header If both the **ITSP Domain Name** and **Local Domain Name** are configured, **Local Domain** takes precedence. **Local Domain Name** is not used in the `Remote Party ID` header.
URI Type	Default = SIP URI. Set the format the IP Office uses for SIP URI entries in headers. • **SIP URI** - Use SIP URI format. For example, `display <sip:content@hostname>` • **Tel** - Use Tel URI format. For example, +1-425-555-4567. This affects the `From` field of outgoing calls. The `To` field for outgoing calls uses the format specified by the short codes used for outgoing call routing. • **SIPS** - Use SIPS format for all URIs. SIPS can be used only when **Layer 4 Protocol** is set to **TLS**.
Location	Default = Cloud. You can set Location values for the IP Office system and for individual extensions and lines. Associating a line with a location: • Applies the location's call admission control (CAC) settings to the line • For SIP lines that support RFC4119/RFC5139, emergency calls using the line can include the location's address information.
Prefix **National Prefix** **International Prefix** **Country Code**	The IP Office uses these values to adjust incoming numbers to match the format required for outgoing calls and used in system directory entries. 1. If the number starts with a + symbol, the symbol is replaced with the **International Prefix**. 2. If the **Country Code** has been set: a. If the number begins with the **Country Code**, or **International Prefix** plus **Country Code**, the IP Office replaces them with the **National Prefix**. b. If the number does not start with the **National Prefix** or **International Prefix**, the IP Office adds the **International Prefix**. 3. If the incoming number does not begin with the **National Prefix** or **International Prefix**, the IP Office adds the **Prefix**.

Table continues…

Field	Description
Name Priority	Default = System Default. For SIP trunks, the caller name displayed on an extension can either be that supplied by the trunk or one obtained by checking for a number match in the extension user's personal directory and the system directory. This setting determines which method is used by the line. The options are: • **System Default**: Use the system setting **System | Telephony | Telephony | Default Name Priority**. • **Favor Trunk**: Display the name provided by the trunk. For example, the trunk may be configured to provide the calling number or the name of the caller. The system should display the caller information as it is provided by the trunk. If the trunk does not provide a name, the system uses the **Favor Directory** method. • **Favor Directory**: Search for a number match in the extension user's personal directory and then in the system directory. The first match is used and overrides the name provided by the SIP line. If no match is found, the name provided by the line, if any, is used.
Description	Default = Blank. Maximum 31 characters. You can use this field to enter a description for the configuration entry. The description is not used elsewhere.
Network Type	Default = Public. This option is available when **System | Telephony | Telephony | Restrict Network Interconnect** is enabled. It allows you to configure trunks as either **Public** or **Private**. • The IP Office will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or the opposite. • The call restriction includes transfers, forwarding and conference calls. • Avaya does not recommended use of this feature on IP Office systems using any of the following features: multi-site networks, VPNremote, application telecommuter mode.
In Service	Default = On. When this field is not selected, the SIP trunk is unregistered and not available to incoming and outgoing calls.
Check OOS	Default = On. If enabled, the system will regularly check if the trunk is in service using the methods listed below. Checking that SIP trunks are in service ensures that outgoing call routing is not delayed waiting for response on a SIP trunk that is not currently usable. For UDP and TCP trunks, OPTIONS message are regularly sent. If no reply to an OPTIONS message is received the trunk is taken out of service. For trunks using DNS, if the IP address is not resolved or the DNS resolution has expired, the trunk is taken out of service.

Session Timers

Field	Description
Refresh Method	Default = Auto. The options are: **Auto**, **Reinvite** or **Update**. When **Auto** is selected, if UPDATE is in the Allow: header from the far SIP endpoint, then it is used. Otherwise INVITE is used.
Timer (seconds)	Default = On Demand. Range = 90 to 64800 This field specifies the session expiry time. At the half way point of the expiry time, a session refresh message is sent. When set to **On Demand**, IP Office will not send a session refresh message but will respond to them.

Redirect and Transfer

Redirection and blind transfer are configured separately. By default, they are disabled.

A supervised transfer occurs when a consultation call is made and the REFER contains a Replaces: header indicating the CallID of another call leg which the REFERing agent has already initiated with the REFER target.

Note:

- Do not change these settings unless directed to by the SIP service provider.

Field	Description
Incoming Supervised REFER	Default = Auto. Determines if IP Office will accept a REFER being sent by the far end. The options are: • **Always**: Always accepted. • **Auto**: If the far end does not advertise REFER support in the Allow: header of the OPTIONS responses, then IP Office will reject a REFER from that endpoint. • **Never**: Never accepted.
Outgoing Supervised REFER	Default = Auto. Determines if IP Office will attempt to use the REFER mechanism to transfer a party to a call leg which IP Office has already initiated so that it can include the CallID in a Replaces: header. The options are: • **Always**: Always use REFER. • **Auto**: Use the Allow: header of the OPTIONS response to determine if the endpoint supports REFER. • **Never**: Never use REFER.
Send 302 Moved Temporarily	Default = Off. A SIP response code used for redirecting an unanswered incoming call. It is a response to the INVITE, and cannot be used after the 200 OK has been sent as a response to the INVITE.

Table continues…

Field	Description
Outgoing Blind REFER	Default = Off. When enabled, a user, voicemail system or IVR can transfer a call by sending a REFER to an endpoint that has not set up a second call. In this case, there is no Replaces: header because there is no CallID to replace the current one. This directs the far end to perform the transfer by initiating the new call and release the current call with IP Office.

Related links

SIP Line on page 376

SIP Line I Transport

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Transport**

Behavior during Service unavailable

A proxy server is considered Active once the system has received a response to an INVITE, REGISTER or OPTIONS.

In the case of the proxy server responding with `503 - Service Unavailable`, it should be considered Active - In Maintenance. In this case, the following should occur:

- If the response `503 - Service Unavailable` was in response to an INVITE request:
  - If calls are tied to registrations (**Calls Route via Registrar** enabled) and there are other proxies available, the tied registrations should issue an Un-REGISTER and try to REGISTER with a different proxy. The call should fail with cause = Temporary Fail.
  - If calls are not tied, the INVITE should be immediately tried to a different proxy.
- If the response `503 - Service Unavailable` was in response to a REGISTER request:
  - If there are other proxies available, this registration only should issue an Un-REGISTER and try to REGISTER with a different proxy.
  - If **Explicit DNS Server(s)** are configured, a DNS request should be sent out to see whether the proxy server has disappeared from those being offered.

An `Active-InMaintenance` proxy server should not be used for a new transactions (INVITE or REGISTER) until:

- There is a change in DNS responses indicating the proxy has become active.
- The configuration does not leave any better option available. In this case, there should be a throttle so that no more than 5 failures (without successes) in 1 minute should be allowed.
- A configuration merge has occurred where the ITSP Proxy Address has been changed.
- 10 minutes has expired.

Behavior during Not Responding

A proxy server that is not-responding (UDP) is indicated when 3 requests are sent and no replies are received. This would normally occur during a single INVITE transaction.

Consideration should be given whether this is caused by a local network fault or is caused by the Proxy being out of service. Since it is likely to be local, no action should be taken unless traffic is

received from an alternative proxy while this proxy is actually not responding. The state should be "Possibly non responding".

If explicit DNS servers are configured, a DNS request should be sent out to see whether this Proxy server has disappeared from those being offered.

If possible, an alternative proxy should be stimulated simultaneously with stimulating the suspect server.

The server should be considered non-responding if it is persistently non-responding while other proxies are responding or if it is non-responding and has disappeared from the DNS advertisement.

While in the "possibly not responding" state, it would be better to send an INVITE to an alternative proxy while simultaneously sending any appropriate message to this proxy. This will help to resolve whether it is really not responding rather than there being local network problems. However, there is no requirement to blacklist the proxy.

Once in the "definitely not responding" state:

- If there are other proxies available: this registration only issues an Un-REGISTER, and try to REGISTER with a different proxy. Calls do not automatically clear.
- If a SIP message is received from it, the state should immediately go"Active".
- This proxy should be blacklisted unless there are no better options available. While blacklisted, only one transaction per 10 minutes is allowed.
- Even if not blacklisted, there should be a throttle so that no more than 5 failures (without successes) in 1 minute should be allowed.

Configuration settings

The **ITSP Proxy Address** and **Calls Route via Registrar** settings are mergeable. Changing the remaining settings requires a “merge with service disruption”. When the configuration file is sent to the system, the SIP trunk is restarted and all calls on the line are dropped.

Offline editing is not required.

Field	Description
ITSP Proxy Address	Default = Blank This is the SIP Proxy address used for outgoing SIP calls. The address can be specified in the following ways: • If left blank, the ITSP Domain Name is used and is resolved by DNS resolution in the same way as if a DNS address had been specified as below. • An IP address. • A list of up to 4 IP addresses, with each address separated by a comma or space. - The addresses can include an indication of the relative call weighting of each address compared to the others. This is done by adding a **w N** suffix to the address where **N** is the weighting value. For example, in the list 213.74.81.102w3 213.74.81.100w2, the weighting values assigns 1.5 times the weight of calls to the first address. The default weight if not specified is 1. A weight of 0 can be used to disable an address. Weight is only applied to outgoing calls. If there is more than one proxy defined, and no weight indication, then calls are only sent to the first in the list until there is a failure at which point the next proxy is used. - If the **Calls Route via Registrar** setting below is enabled, the weighting is applied to registrations rather than calls. • A DNS address, for example sbc.example.com. - The DNS response may return multiple proxy addresses (RFC 3263). If that is the case, the system will resolve the address to use based on priority, TTL and weighting information included with each address. - A load balancing suffix can be added to specify that multiple proxy results should be returned if possible, for example sbc.example.com(N). where **N** is the required number of addresses from 1 to 4. This field is mergeable. However, no more than 4 IP Addresses should be in use at any time. So, if the combined new and old address settings exceed 4, the new addresses are only phased into use as transactions in progress on the previous addresses are completed.
Network Configuration	
Layer 4 Protocol	Default = UDP. The options are: **TCP**, **UDP** or **TLS**. • TLS connections support the following ciphers: `TLS_RSA_WITH_AES_128_CBC_SHA`, `TLS_RSA_WITH_AES_256_CBC_SHA`, `TLS_DHE_RSA_WITH_AES_128_CBC_SHA`, and `TLS_DHE_RSA_WITH_AES_256_CBC_SHA`

Table continues…

Field	Description
Use Network Topology Info	Default = None. • **LAN1** - Associate the line with the **Network Topology** and **DiffServ Settings** settings of IP Office LAN1. - If no STUN server address is set for the LAN interface, then the **Binding Refresh Time** is ignored when calculating the timing for periodic `OPTIONS` messages unless the **Firewall/NAT Type** is set to **Open Internet**. • **LAN2** - As above but using the settings of IP Office LAN2. • **None** - If selected, the IP Office does not apply STUN lookup. The IP Office system IP routing tables determine routing for the line.
Send Port	When the **Layer 4 Protocol** is set to **TLS**, the default port is 5061. When set to **TCP** or **UDP**, the default port is 5060.
Listen Port	When the **Layer 4 Protocol** is set to **TLS**, the default port is 5061. When set to **TCP** or **UDP**, the default port is 5060.
Explicit DNS Server(s)	Default = 0.0.0.0 (Off) If specific DNS servers should be used for SIP trunk operation rather than the general DNS server specified or obtained for the system, the server addresses can be specified here. If exported or imported as part of a trunk template.
Calls Route via Registrar	Default = On If selected, all calls are routed via the same proxy as used for registration. If multiple ITSP proxy addresses have been specified, there is no load balancing of registrations.
Separate Registrar	Default = Blank This field allows the SIP registrar address to be specified if it is different from that of the SIP proxy. The address can be specified as an IP address or DNS name.

Related links

SIP Line on page 376

Call Details

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **Call Details**

These settings are used to control the incoming and outgoing calls that use the SIP line. They also set the SIP headers used on calls and the source for values within those headers.

	Description
SIP URIs	These settings are used for general incoming and outgoing calls on the SIP line.
SIP Line Appearances	These settings allow the emulation of line appearance operation by the SIP line.

For details of how these are used as part of call routing, see Outgoing SIP Call Routing on page 934.

Related links

SIP Line on page 376
SIP URIs on page 385
SIP Line Appearances on page 388

SIP URIs

For the IP Office, each SIP URI acts as a set of trunk channels. It also sets the content of various SIP headers and how that content is used.

- For outgoing calls, the IP Office maps internal calling or called numbers to headers to match the ITSPs requirements. Outgoing calls are routed to a SIP URI by short codes that match the URIs **Outgoing Group** setting. See SIP Outgoing Call Routing on page 934.
- For incoming calls, headers in the SIP message are used for call routing. Incoming calls are routed to incoming call routes that match the URI's **Incoming Group** setting. See SIP Incoming Call Routing on page 942.
- The IP Office supports up to 150 SIP URIs on each SIP line.

General Settings

Name	Description
URI	This field is for information only and cannot be edited.
Incoming Group	Default = 0, Range 0 to 99999. This value is used to match incoming to the **Line Group ID** of an incoming call route entry.
Outgoing Group	Default = 0, Range 0 to 99999. Short codes that specify a number to dial to a line specify a **Line Group ID**. This is used to match to lines with the same **Outgoing Group** value.
Max Sessions	Default =10 This field sets the maximum number of simultaneous calls that can use the URI before the system returns busy to any further calls.
Credentials	Default = 0:<None> This field is used to select from a list of the account credentials configured on the line's **SIP Credentials** tab.

The remaining sections are arranged as a table of values. These set which SIP headers are used for calls routed by the SIP URI entry.

The table also sets the source of the values used in the SIP URI values in those headers. A typical SIP URI takes the following form: `display <sip:content@hostname>` where:

- `display` is the displayed name value for the caller/called party.
- `content` is the call target name or number.
- `hostname` is the host from/to which the calls are sent. For details of how the hostname used by the IP Office system is set. See Setting the SIP URI Host on page 930.

Headers

The first column indicates the headers used for calls matched to this SIP URI entry.

Name	Description
Local URI	Default = Auto This field sets the `From` field for outgoing SIP calls using this URI.
Contact	Default = Auto This field sets the `From` field for outgoing SIP calls using this URI.
P Asserted ID	Default = Disabled When selected, identity information is provided in `P-Asserted-Identity` (PAI) headers.
P Preferred ID	Default = Disabled When selected, identity information is provided in a `P-Preferred-Identity` header.
Diversion Header	Default = Disabled When selected, information from the `Diversion Header` is provided in the SIP messages.
Remote Party ID	Default = Disabled When selected, `Remote Party ID` header are provided with calls.

Display

This column sets the source for the `display` part of the SIP URI used in the selected headers.

Setting	Description
Auto	If **Auto** is selected, the system automatically determines the appropriate value to use. It uses external numbers when forwarding incoming calls, and internal extension numbers for calls made by a local user. • On incoming calls, the system looks for matches against extension numbers and system short codes. • On outgoing calls, the system allows short code manipulation of the caller number and name. For example: **S** to explicitly set the caller number, **W** to set withheld, **A** to allow (override any previous withhold setting), **Z** to set the caller name.
Use Internal Data	Use the SIP settings of the user (**User** > **SIP**), group (**Group** > **SIP**) or voicemail services (**System** > **Voicemail** > **SIP**) making or receiving the call: • Use the **SIP Display Name (Alias)** setting. • If the Anonymous is selected, use that value instead.
Manual Entry	If required, you can manually type in a value to use. The value is then used by other fields configured as **Explicit**. This is typically used to set the DDI to be associated with SIP line appearances.

Table continues…

Setting	Description
Credential Values	If a **Credentials** entry has been selected above, then the **User name**, **Authentication Name** and **Contact** values from the selected credentials entry can be selected as values. The value is then used by other fields configured as **Explicit**. • URI values should only be set using credentials when required by the line provider. For example, some line providers require the `From` header to always contains the credentials used for registration, whilst other headers are used to convey information about the caller ID.

Content

This column sets the source for the `content` part of the SIP URI used in the selected headers.

Setting	Description
Auto	If **Auto** is selected, the system automatically determines the appropriate value to use. It uses external numbers when forwarding incoming calls, and internal extension numbers for calls made by a local user. • On incoming calls, the system looks for matches against extension numbers and system short codes. • On outgoing calls, the system allows short code manipulation of the caller number and name. For example: **S** to explicitly set the caller number, **W** to set withheld, **A** to allow (override any previous withhold setting), **Z** to set the caller name.
Use Internal Data	Use the SIP settings of the user (**User** > **SIP**), group (**Group** > **SIP**) or voicemail services (**System** > **Voicemail** > **SIP**) making or receiving the call: • Use the **SIP Display Name (Alias)** setting. • If the Anonymous is selected, use that value instead.
Manual Entry	If required, you can manually type in a value to use. The value is then used by other fields configured as **Explicit**. This is typically used to set the DDI to be associated with SIP line appearances.
Credential Values	If a **Credentials** entry has been selected above, then the **User name**, **Authentication Name** and **Contact** values from the selected credentials entry can be selected as values. The value is then used by other fields configured as **Explicit**. • URI values should only be set using credentials when required by the line provider. For example, some line providers require the `From` header to always contains the credentials used for registration, whilst other headers are used to convey information about the caller ID.

Field Meaning

These values are used to set the source or value for headers based on the call direction.

Field	Description
Outgoing Calls	Set the source for URI header information on outgoing external calls.
Forwarding/ Twinning	Set the source for URI header information on calls being forwarded externally.
Incoming Calls	Set the source for URI header information on incoming external calls.

The following values can be selected for the different fields.

Field	Description
Caller	Use the values associated with the calling party. For forwarded calls, use the values associated with the party forwarding the call.
Original Caller	For forwarded calls, use the value associated with the original caller.
Called	Use the values associated with the called party.
Explicit	Use the manual entered values from the header **Display** and **Content** fields, or the credentials values selected from those drop-downs.
None	Do not send the header.

Related links

Call Details on page 384

SIP Line Appearances

These settings allow the SIP line to emulate the use of line appearances on phones that support line appearance buttons. Those buttons can then be used to make or receive calls. For details, see SIP Line Appearances on page 957.

SIP line appearances are not supported over a multi-site network/SCN or in resiliency.

General Settings

Name	Description
SIP Line Appearances	Default = Disabled When enabled, SIP line appearances can be configured. Note, if you disable this setting and save the configuration, all configured SIP line appearance values are removed.
Incoming Group	Default = 0, Range 0 to 99999. This value is used to match incoming to the **Line Group ID** of an incoming call route entry.
Outgoing Group	Default = 0, Range 0 to 99999. Short codes that specify a number to dial to a line specify a **Line Group ID**. This is used to match to lines with the same **Outgoing Group** value.
Credentials	Default = 0:<None> This field is used to select from a list of the account credentials configured on the line's **SIP Credentials** tab.
Max Sessions	Default =10 This field sets the maximum number of simultaneous calls that can use the URI before the system returns busy to any further calls.
Incoming Sessions	Default = 3 The maximum number of incoming call sessions.
Outgoing Sessions	Default = 3 The maximum number of outgoing call sessions. .

The remaining sections are arranged as a table of values. These set which SIP headers are used for calls routed by the SIP URI entry.

The table also sets the source of the values used in the SIP URI values in those headers. A typical SIP URI takes the following form: `display <sip:content@hostname>` where:

- `display` is the displayed name value for the caller/called party.
- `content` is the call target name or number.
- `hostname` is the host from/to which the calls are sent. For details of how the hostname used by the IP Office system is set, see Setting the SIP URI Host on page 930.

Headers

The first column indicates the headers used for calls matched to this SIP URI entry.

Name	Description
Local URI	Default = Auto This field sets the `From` field for outgoing SIP calls using this URI.
Contact	Default = Auto This field sets the `From` field for outgoing SIP calls using this URI.
P Asserted ID	Default = Disabled When selected, identity information is provided in `P-Asserted-Identity` (PAI) headers.
P Preferred ID	Default = Disabled When selected, identity information is provided in a `P-Preferred-Identity` header.
Diversion Header	Default = Disabled When selected, information from the `Diversion Header` is provided in the SIP messages.
Remote Party ID	Default = Disabled When selected, `Remote Party ID` header are provided with calls.

Display

This column sets the source for the `display` part of the SIP URI used in the selected headers.

Setting	Description
Auto	If **Auto** is selected, the system automatically determines the appropriate value to use. It uses external numbers when forwarding incoming calls, and internal extension numbers for calls made by a local user. • On incoming calls, the system looks for matches against extension numbers and system short codes. • On outgoing calls, the system allows short code manipulation of the caller number and name. For example: **S** to explicitly set the caller number, **W** to set withheld, **A** to allow (override any previous withhold setting), **Z** to set the caller name.

Table continues…

Setting	Description
Use Internal Data	Use the SIP settings of the user (**User** > **SIP**), group (**Group** > **SIP**) or voicemail services (**System** > **Voicemail** > **SIP**) making or receiving the call: • Use the **SIP Display Name (Alias)** setting. • If the Anonymous is selected, use that value instead.
Manual Entry	If required, you can manually type in a value to use. The value is then used by other fields configured as **Explicit**. This is typically used to set the DDI to be associated with SIP line appearances.
Credential Values	If a **Credentials** entry has been selected above, then the **User name**, **Authentication Name** and **Contact** values from the selected credentials entry can be selected as values. The value is then used by other fields configured as **Explicit**. • URI values should only be set using credentials when required by the line provider. For example, some line providers require the `From` header to always contains the credentials used for registration, whilst other headers are used to convey information about the caller ID.

Content

This column sets the source for the `content` part of the SIP URI used in the selected headers.

Setting	Description
Auto	If **Auto** is selected, the system automatically determines the appropriate value to use. It uses external numbers when forwarding incoming calls, and internal extension numbers for calls made by a local user. • On incoming calls, the system looks for matches against extension numbers and system short codes. • On outgoing calls, the system allows short code manipulation of the caller number and name. For example: **S** to explicitly set the caller number, **W** to set withheld, **A** to allow (override any previous withhold setting), **Z** to set the caller name.
Use Internal Data	Use the SIP settings of the user (**User** > **SIP**), group (**Group** > **SIP**) or voicemail services (**System** > **Voicemail** > **SIP**) making or receiving the call: • Use the **SIP Display Name (Alias)** setting. • If the Anonymous is selected, use that value instead.
Manual Entry	If required, you can manually type in a value to use. The value is then used by other fields configured as **Explicit**. This is typically used to set the DDI to be associated with SIP line appearances.
Credential Values	If a **Credentials** entry has been selected above, then the **User name**, **Authentication Name** and **Contact** values from the selected credentials entry can be selected as values. The value is then used by other fields configured as **Explicit**. • URI values should only be set using credentials when required by the line provider. For example, some line providers require the `From` header to always contains the credentials used for registration, whilst other headers are used to convey information about the caller ID.

Field Meaning

These values are used to set the source or value for headers based on the call direction.

Field	Description
Outgoing Calls	Set the source for URI header information on outgoing external calls.
Incoming Calls	Set the source for URI header information on incoming external calls.

The following values can be selected for the different fields.

Field	Description
Explicit	Use the manual entered values from the header **Display** and **Content** fields, or the credentials values selected from those drop-downs.
None	Do not send the header.

Related links

Call Details on page 384

SIP Line VoIP

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP VoIP**

This form is used to configure the VoIP settings applied to calls on the SIP trunk.

Configuration Settings

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Codec Selection	Default = System Default Set the supported codecs. Where possible, Avaya recommend that you use the same set of codecs for all IP Office systems, lines, and extensions. The options are: • **System Default** - Use the codec list set in the system settings. • **Custom** - Configure a list of codec preferences for the line. - You can move codecs between the **Unused** and **Selected** sets and change the order of the codecs. - The codecs available are set by **System Settings** > **System** > **VoIP**. The possible codecs are: • **OPUS** - Supported on Linux-based IP Office systems only. • **G.711 ALAW/G.711 ULAW** • **G.729** • **G.723.1** - Supported on IP500 V2 systems only. • **G.722 64K** - Supported by Linux-based IP Office systems and on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards.
Fax Transport Support	Default = None. If enabled, when the IP Office detects fax tone, it will renegotiate the call codec as configured below. • This option requires **Re-Invite Supported**. • IP Office systems in a network support fax relay for fax calls between systems. • IP500 V2 systems can terminate T38 fax calls. • Linux-based IP Office systems can route the calls between trunks/terminals with compatible fax types. The supported options are: • **None** - Do not support fax. • **G.711** - Use G.711 to send and receive faxes. • **T38** - Use T38 to send and receive faxes. • **T38 Fallback** - Use T38 to send and receive faxes. If the call destination does not support T38, the IP Office will send a re-invite to change the transport method to **G.711**.

Table continues…

Field	Description
DTMF Support	Default = RFC2833 (IP500 V2), RFC2833/RFC4733 (Linux-Based Server) Sets how the IP Office signals DTMF key press digits to the remote end. The options are: • **In Band** - Send digits as tones within the call audio. • **RFC2833** or **RFC2833/RF4733** - Send digits using a separate audio stream from the call audio. If not supported by the far end, the line reverts to using **In Band** signaling. • **Info** - Send the digits in SIP `INFO` packets.
Media Security	Default = Disabled. These setting control whether SRTP is used for this line and the settings used for the SRTP. The options are: • **Same as System**: Matches the system setting at **System Settings** > **System** > **VoIP Security**. • **Disabled**: Use RTP. • **Preferred**: Attempt to use SRTP. If SRTP call setup is unsuccessful, fall back to RTP. • **Enforced**: Use SRTP. If SRTP call setup is unsuccessful, the call fails. - For calls using **Dial Emergency**, the IP Office will switch to RTP if SRTP call setup fails.
Advanced Media Security Options	Default = Same as System. Sets the requirements for SRTP when enabled. • **Same as System**: Use the same settings as configured on **System Settings** > **System** > **VoIP Security**. • **Encryptions**: Default = RTP Sets which parts of a session SRTP protects using encryption. • **Authentication**: Default = RTP and RTCP Sets which parts of the session SRTP protects using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Not adjustable. The IP Office will accept authenticated packets that have a sequence number that is higher than or within 64 packets of the highest-numbered packet already received. • **Crypto Suites**: Default = *SRTP_AES_CM_128_SHA1_80*. Set the crypto suites SRTP uses for encryption. The options are *SRTP_AES_CM_128_SHA1_32* and *SRTP_AES_CM_128_SHA1_80*.

Table continues…

Field	Description
VoIP Silence Suppression	Default = Off When enabled, when the IP Office detects silence during an IP call, it does not send any audio data. • Lines between IP Office systems using G.711 ignore this feature. • On trunks between networked IP Office systems, you must enable the setting at both ends.
Local Hold Music	Default = Off. When enabled, if the far end puts the call on HOLD, the system plays music received from far end (SIP Line) to the other end. RTCP reports are sent towards SIP Line. When disabled, the system plays local music to the other endpoint and no RTCP packets are sent to SIP trunk.
Re-Invite Supported	Default = Off. When enabled, the IP Office can use `Re-Invite` during a call to change the characteristics of the call. For example, when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk. • Requires the ITSP to also support `Re-Invite`. • This setting must be enabled for video support.
Codec Lockdown	Default = Off. After making a SIP offer with a list of codecs, the IP Office expects an answer with a single codec selected from the list. User agents that send an answer with multiple codecs expect to switch to any of those codecs during the call without further negotiation, which the IP Office does not support. Instead, loss of speech occurs if the user agent changes codec without renegotiating. • If enabled, when the IP Office receives an answer with multiple codecs, the IP Office sends a `re-INVITE` and a SIP offer with just one codec. • This option requires **Re-Invite Supported** enabled.
Allow Direct Media Path	Default = On This settings controls whether calls between IP endpoints and/or lines must go through the IP Office. • If disabled, calls go through the IP Office and use its resources. RTP relay allows calls between devices using the same audio codec to not require a voice compression channel. • If enabled, calls can take routes other than through the IP Office system. Both ends must support direct media and have matching VoIP settings. For example, both ends must use the same protocol (SIP or H.323), same addressing (IPv4 or IPv6), and so on. Otherwise, the call goes through the IP Office system. - For extensions, disabling **Requires DTMF** allows the extension to attempt direct media even if the other end has differing DTMF settings.

Table continues…

Field	Description
PRACK/100rel Supported	Default = Off. When selected, supports Provisional Reliable Acknowledgment (PRACK) on SIP trunks. Enable this parameter when you want to ensure that provisional responses, such as announcement messages, have been delivered. Provisional responses provide information on the progress of the request that is in process. For example, while a cell phone call is being connected, there may be a delay while the cell phone is located; an announcement such as “please wait while we attempt to reach the subscriber” provides provisional information to the caller while the request is in process. PRACK, which is defined in RFC 3262, provides a mechanism to ensure the delivery of these provisional responses.
Force direct media with phones	Default = On When enabled, if an Avaya IP phone dials digits during a direct media call, the IP Office changes the call to indirect media and sends the digits as RFC2833. 15-seconds after the last digit, the IP Office changes the call back to direct media. • This setting is requires the line to have **Re-Invite Supported** and **Allow Direct Media Path** enabled, and **DTMF Support** set to **RFC2833/RF4733**.
G.711 Fax ECAN	Default = Off When enabled, if the IP Office detects a fax call, it switches to G.711 with echo cancellation (ECAN) based on the 'G.711 Fax ECAN field, NLP disabled, a fixed jitter buffer, and silence suppression is disabled. You can use this to avoid an ECAN mismatch with the trunk provider. • This setting is only available on IP500 V2 systems when **Fax Transport Support** is set to **G.711** or **T38 Fallback**.

Related links

SIP Line on page 376

T.38 Fax

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP T38 Fax**

The settings are available only on IP500 V2 since it can terminate T38 fax. On the **VoIP** settings for the line type, **Fax Transport Support** must be set to **T38** or **T38 Fallback**.

These settings are mergeable.

Field	Description
Use Default Values	Default = On. If selected, all the fields are set to their default values and greyed out.
T38 Fax Version	Default = 3. During fax relay, the two gateways will negotiate to use the highest version which they both support. The options are: **0**, **1**, **2**, **3**.

Table continues…

Field	Description
Transport	Default = UDPTL (fixed). Only **UDPTL** is supported. **TCP** and **RTP** transport are not supported. For **UDPTL**, redundancy error correction is supported. Forward Error Correction (FEC) is not supported.
Redundancy Redundancy sends additional fax packets in order to increase the reliability. However increased redundancy increases the bandwidth required for the fax transport.	
Low Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for low speed V.21 T.30 fax transmissions.
High Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for V.17, V.27 and V.28 fax transmissions.
TCF Method	Default = Trans TCF. TCF = Training Check Frame.
Max Bit Rate (bps)	Default = 14400. Lower rates can be selected if the current rate is not supported by the fax equipment or is found to not be reliable.
EFlag Start Timer (msecs)	Default = 2600.
EFlag Stop Timer (msecs)	Default = 2300.
Tx Network Timeout (secs)	Default = 150.
Scan Line Fix-up	Default = On.
TFOP Enhancement	Default = On.
Disable T30 ECM	Default = Off. When selected, disabled the T.30 Error Correction Mode used for fax transmission.
Disable EFlags For First DIS	Default = Off.
Disable T30 MR Compression	Default = Off.
NSF Override	Default = Off. If selected, the NSF (Non-Standard Facility) information sent by the T38 device can be overridden using the values in the fields below. **Country Code**: Default = 0. **Vendor Code**: Default = 0.

Related links

SIP Line on page 376

SIP Line Credentials

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Credentials**

These settings in the **SIP Credentials** tab are used to enter the ITSP username and password for the SIP account with the ITSP. If you have several SIP accounts going to the same ITSP IP address or domain name, you can enter up to 30 sets of ITSP account names and passwords on this tab.

Use the **Add**, **Remove**, and **Edit** buttons to manage the set of credentials for the SIP trunk accounts.

Configuration Settings

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Descriptions
Index	This number is assigned automatically and cannot be edited. If the **From** field on the SIP URI being used for the call is set to **Use Authentication Name** , the registration field of the SIP URI indicates the index number of the SIP credentials to use for calls by that SIP URI.
User Name	This name must be unique and is used to identify the trunk. The name can include the domain if necessary.
Authentication Name	Default = Blank. This field can be blank but must be completed if a **Password** is also specified. This value is provided by the SIP ITSP. Depending on the settings on the **Local URI** tab associated with the SIP call, it may also be used as the user part of the SIP URI. The name can include the domain if necessary.
Contact	Default = Blank. This field is used to enter a contact and can include the domain if necessary.
Password	Default = Blank. This value is provided by the SIP ITSP. If a password is specified, the matching **Authentication Name** must also be set.
Expiration (mins)	Default = 60 minutes. This setting defines how often registration with the SIP ITSP is required following any previous registration.
Registration Required	Default = On. If selected, the fields above above are used for registration when making calls. If exported or imported as part of a trunk template.

Related links

SIP Line on page 376

SIP Line Advanced

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Advanced**

Additional configuration information

For additional information regarding the **Media Connection Preservation** setting, see Media Connection Preservation on page 743.

Configuration settings

These settings are mergeable, with the exception of the **Media Connection Preservation** setting.

- Changing the **Media Connection Preservation** setting requires a “merge with service disruption”. When the configuration file is sent to the system, the SIP trunk is restarted and all calls on the line are dropped.

Offline editing is not required.

Call Control

Field	Description
Call Initiation Timeout (s)	Default = 4 seconds. Range = 1 to 99 seconds. Sets how long the IP Office system should wait for a response to an attempt to initiate a call before following the alternate routes set in an ARS form.
Call Queuing Timeout (m)	Default = 5 minutes. • For incoming calls, this sets how many minutes the IP Office waits before dropping a call that is waiting for VCM resources or has remained in the unanswered state. • For outgoing calls, this sets how many minutes the IP Office waits for a call to be answered after receiving a provisional response.
Service Busy Response	Default = 486 - Busy Here (503 - Service Unavailable for the France2 locale). For calls that result in a busy response from IP Office, this setting determines the response code. The options are: • **486 - Busy Here** • **503 - Service Unavailable**
on No User Responding Send	Default = 408-Request Timeout. Specifies the cause to be used when releasing incoming calls from SIP trunks, when the cause of releasing is that user did not respond. The options are 408-Request Timeout or 480 Temporarily Unavailable.
Action on CAC Location Limit	Default = Allow Voicemail When set to **Allow Voicemail**, the call is allowed to go to a user's voicemail when the user's location call limit has been reached. When set to **Reject Call**, the call is rejected with the failure response code configured in the **Service Busy Response** field.

Table continues…

Field	Description
Suppress Q.850 Reason Header	Default = Off. When SIP calls are released by sending BYE and CANCEL, a release reason header is added to the message. When set to On, the Q.850 reason header is not included.
Emulate NOTIFY for REFER	Default = Off. Use for SIP providers that do not send NOTIFY messages. When set to On, after IP Office issues a REFER, and the provider responds with 202 ACCEPTED, IP Office will assume the transfer is complete and issue a BYE.
No REFER if using Diversion	Default = Off. When enabled, REFER is not sent on the trunk if the forwarding was done with 'Send Caller ID = Diversion Header'. Applies to Forwards and Twinning.

Media

Field	Description
Allow Empty INVITE	Default = Off. When set to On, allows 3pcc devices to initiate calls to IP Office by sending an INVITE without SDP.
Send Empty re-INVITE	Default = Off. This option is only available if **SIP Line** > **SIP VoIP** > **Reinvite Supported** is selected. If set to On, when connecting a call between two endpoints, IP Office sends an INVITE without SDP in order to solicit the full media capabilities of both parties.
Allow To Tag Change	Default = Off. When set to On, allows the IP Office to change media parameters when connecting a call to a different party than that which was advertised in the media parameters of provisional responses, such as 183 Session Progress.
P-Early-Media Support	Default = None. The options are: • **None**: IP Office will not advertise support of this SIP header and will always take incoming early media into account regardless of presence of this header • **Receive**: IP Office will advertise support of this SIP header and will discard incoming early media unless this header is present in the SIP message. • **All**: IP Office will advertise support of this SIP header, will discard incoming early media unless this header is present in the SIP message and will include this SIP header when providing early media.
Send SilenceSupp=off	Default = Off. Used for the G711 codec. When checked, the silence suppression off attribute is sent in SDP on this trunk.

Table continues…

Field	Description
Force Early Direct Media	Default = Off. When set to On, allows the direct connection of early media streams to IP endpoints rather than anchoring it at the IP Office.
Media Connection Preservation	Default = Disabled. When enabled, allows established calls to continue despite brief network failures. Call handling features are no longer available when a call is in a preserved state. Preservation on public SIP trunks is not supported until tested with a specific service provider.
Indicate HOLD	Default = Off. When enabled, the system sends a HOLD INVITE to the SIP trunk endpoint.
Media Security	Default = Off When enabled, the IP Office advertises support of this SIP header, to indicate that audio is configured to be secure and is enforced to use SRTP only. This supports the SIP security header defined by RFC3329. This option is available only when: • TLS is being used. • **Line | SIP Line | VoIP** > **Media Security** is selected and set to **Enforced**. • **Line | SIP Line | VoIP** > **Fax Transport Support** is not set to **T38** or **T38 Fallback**. When the configuration file is sent to the system, the SIP trunk is restarted and all calls on the line are dropped.

Calling Number Verification

These settings configure the SIP trunks use of STIR protocols for calling number verification.

For more details, see SIP Calling Number Verification (STIR/SHAKEN) on page 959.

Field	Description
Calling Number Verification	Default = Off Sets whether the line uses calling number verification.
Incoming Calls Handling	Default = **Allow Not Failed** Set which calls are accepted by the system based on the attestation level of the call. • **System** - Use the default system setting (**System VoIP** > **VoIP Security** > **Calling Number Verification**). • **Allow All** - Allow all calls regardless of calling number verification. • **Allow Validated** - Only accept verified calls with full or partial attestation. • **Allow Not Failed** - Accept all calls expect those that specifically failed verification. Note this can include calls with no reported verification result.

Identity

Field	Description
Use Phone Context	Default = Off. When enabled, signals SIP enabled PBXs that the call routing identifier is a telephone number.
Add user=phone	Default = Off. This setting is available when **Use Phone Context** is enabled. When enabled, this setting adds the SIP parameter **User** with value **Phone** to the *From* and *To* SIP headers of outgoing calls.
Use + for International	Default = Off. When enabled, outgoing international calls use E.164/International format with + followed by the country code and then the telephone number.
Use PAI for Privacy	Default = Off. When enabled, if the caller ID is withheld: • The SIP message *From* header is made anonymous • The caller identity is inserted into the *P-Asserted-Identity* header. This should only be used in a trusted network and must be stripped out of the SIP message before it is forwarded outside the trusted domain.
Use Domain for PAI	Default = Off. • When disabled, the DNS resolved IP address of the ITSP Proxy is used for the host part in the *P-Asserted-Identity* header. • When enabled, the Domain is used.
Caller ID FROM Header	Default = Off. Incoming calls can include caller ID information in both the *From* field and in the *PAI* fields. When this option is enabled, the caller ID information in the *From* field is used rather than that in the *PAI* fields.
Send From In Clear	Default = Off. When enabled, the user ID of the caller is included in the `From` field. This applies even if the caller has selected to be or is configured to be anonymous. However, their anonymous state is still honored in other fields used to display the caller identity.
Cache Auth Credentials	Default = On. When enabled, credentials challenge and response information from a registration transaction is cached by the IP Office and automatically inserted into later SIP messages without waiting for a subsequent challenge. This speeds up connections but must be supported by the other end of the connection.
Add UUI header	Default = Off. When enabled, the User-to-User Information (UUI) is passed in SIP headers to applications.

Table continues…

Field	Description
Add UUI header to redirected calls	Default = Off. When enabled, the UUI is passed in SIP headers for calls that are redirected. For example, on forwarded and twinned calls. This field can be enabled if **Add UUI header** is enabled.
User-Agent and Server Headers	Default = Blank (Use system type and software level). The value set in this field is used as the *User-Agent* and *Server* value included in SIP request headers made the line. • If blank, the type of IP Office system and its software level are used. • Setting a unique value can be useful in call diagnostics when the IP Office has multiple SIP trunks.
Send Location Info	Default = Never. This option is useable with SIP ISPs that support RFC 4119/RFC 5139. When enabled, emergency calls send the address information associated with the dialing extension's location. See Configuration for Emergency Calls on page 772. The options are: • **Never**: Do not send location information. • **Emergency Calls**: For **Dial Emergency** calls, send the address information configured for the dialing extension's location.

Association Method

When the IP Office receives an incoming SIP call, it needs to match the call to one of its SIP line.

- Lines are checked for a match in **Line Number** order until a match occurs.
- The method used to check for a match on a line uses the line's **Association Method**.
- If no match occurs on any line, the request is ignored.

This process enables support of multiple SIP lines with the same address settings. For example, for scenarios that require support of multiple SIP lines from the same ITSP. That can occur when the same ITSP supports different call plans on separate lines, or where all outgoing SIP lines are routed from the system through an additional on-site system.

Field	Description
By Source IP Address	Uses the source IP address and port of the incoming request for association. The match is against the configured remote end of the SIP line, using either an IP address/port or resolution of an FQDN. For UDP calls, the local **Listen Port** is also used for the match. • For TCP/TLS connections, the IP Office establishes a connection to the remote address and port specified on the SIP line. • For UDP, non-call dialogs and call starting dialogs must use the remote address and port specified on the SIP line. It is recommended that the remote end does not change these value as that may prevent NAT traversal.
"From" header hostpart against ITSP domain	Uses the host part of the `From` header in the incoming SIP request for association. • The match is against the **Line** > **SIP Line** > **ITSP Domain Name**.
R-URI hostpart against ITSP domain	Uses the host part of the `Request-URI` header in the incoming SIP request for association. • The match is against the **Line** > **SIP Line** > **ITSP Domain Name**.
"To" header hostpart against ITSP domain	Uses the host part of the `To` header in the incoming SIP request for association. • The match is against the **Line** > **SIP Line** > **ITSP Domain Name**.
"From" header hostpart against DNS-resolved ITSP domain	Uses the host part of the `From` header in the incoming SIP request for association. • The match is found by comparing the `From` header against the IP address resolution of the **Line** > **SIP Line** > **ITSP Domain Name** or, if set, the **Line** > **SIP Transport** > **ITSP Proxy Address** setting.
"Via" header hostpart against DNS-resolved ITSP domain	Uses the host part of the `VIA` header in the incoming SIP request for association. • The match is found by comparing the `VIA` header against the IP address resolution of the **Line** > **SIP Line** > **ITSP Domain Name** or, if set, the **Line** > **SIP Transport** > **ITSP Proxy Address** setting.
"From" header hostpart against ITSP proxy	Uses the host part of the `From` header in the incoming SIP request for association. • The match is against the **Line** > **SIP Transport** > **ITSP Proxy Address** setting.
"To" header hostpart against ITSP proxy	Uses the host part of the `From` header in the incoming SIP request for association. • The match is against the **Line** > **SIP Transport** > **ITSP Proxy Address** setting.
R-URI hostpart against ITSP proxy	Uses the host part of the `Request-URI` in the incoming SIP request for association. • The match is against the **Line** > **SIP Transport** > **ITSP Proxy Address** setting.

Addressing

Field	Description
Call Routing Method	Default = Request URI. This field selects which incoming SIP information is used for incoming number matching by the IP Office to route incoming calls. The options are to match the **Request URI** or the **To Header** element provided with the incoming call.
Use P-Called-Party	Default = Off. When enabled, IP Office reads the `P-Called-Party ID` header if present in the SIP message and routes the incoming SIP calls based on it. The feature can be enabled on public SIP trunk interfaces. If enabled and the header is not present in the SIP message, the IP Office uses the header configured in the **Call Routing Method** for incoming call routing.
Suppress DNS SRV Lookups	Default = Off. Controls whether to send SRV queries for this endpoint, or just NAPTR and A record queries.

Related links

SIP Line on page 376

SIP Line Engineering

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Engineering**

You can use this tab to enter commands that apply special features to the SIP line. The commands are called SIP Line Custom (SLIC) strings.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

reINVITE Codec Renegotiation

For R11.0 and higher, the IP Office supports codec renegotiation when a `reINVITE` is received. See Codec selection on page 950.

You can use the following command to retain the pre-R11.0 behavior of no renegotiation. Note: On existing IP Office systems upgraded to R11.0 or higher, this command is automatically added to all existing SIP lines.

- `SLIC_PREFER_EXISTING_CODEC`

Calling Number Validation

You can use the following commands to control calling number validation. See SIP Calling Number Verification (STIR/SHAKEN) on page 959.

- `SLIC_STIR_REJECT_CODE=<n>` where `<n>` is the response code sent for calls rejected by the IP Office.
- `SLIC_STIR_REJECT_STRING=<y>` where `<y>` is the response string sent for calls rejected by the IP Office.

- SLIC_STIR_ATTEST="<w>" where <w> is the name of the header the IP Office checks for a call's authorization level.
- SLIC_STIR_CUSTOM=<z> where <z> value enables or disables various call features.

Server Name Identification (SNI)

The following SLIC codes can be used for SIP trunks using TLS. When used:

- On outgoing connections, the IP Office adds Server Name Indication (SNI) information to the SAN field it sends.
- If the IP Office system's **Received certificate checks (Telephony endpoints)** settings is set to **Medium + Remote Checks** or **High + Remote Checks**, then the SLIC value is also used to validate the received certificates SAN.

The SLIC codes are:

- SLI_ADD_SIP_SAN=<X>

  Use a SNI set to sip:<SNI> where the <SNI> value is taken from the existing IP Office SIP line configuration based on the following values of <X> as below:

  - D = Use the value of the SIP line's **ITSP Domain Name** setting (**Line** > **SIP Line**). For example, for a SIP line with the **ITSP Domain Name** set to ipo.example.com, adding SLIC_ADD_SIP_SAN=D sets the SNI added to sip:ipo.example.com.
  - P = Use the value of the SIP line's configured **ITSP Proxy Address** setting (**Line** > **Transport** > **)**. This option is only supported for a **ITSP Proxy Address** set to a single address. For example: SLI_ADD_SIP_SAN=P

Keepalives

Supported with IP Office R11.1.3.1 and higher.

You can add SLIC_HNT_EMPTY_PACKET to have the SIP line send RTP packets with payload 20 (unassigned payload) and no data as keepalives. This overrides the default of send STUN packets for keepalives.

Related links

SIP Line on page 376

T1 PRI Line

Related links

Line on page 303
T1 ISDN on page 406
T1 ISDN Channels on page 409
T1 ISDN TNS on page 411
T1 ISDN Special on page 412
Call By Call (US PRI) on page 412

T1 ISDN

Navigation: **System Settings** > **Line** > **T1 ISDN Line**

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Variable	Description
Line Number	Allocated by the system.
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Network Type	Default = Public. This option is available when **System | Telephony | Telephony | Restrict Network Interconnect** is enabled. It allows you to configure trunks as either **Public** or **Private**. • The IP Office will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or the opposite. • The call restriction includes transfers, forwarding and conference calls. • Avaya does not recommended use of this feature on IP Office systems using any of the following features: multi-site networks, VPNremote, application telecommuter mode.
Line Sub Type	: Default = PRI Set to **PRI**. If set to T1 see Line Form (T1). If set to **ETSI**, **ETSI CHI**, **QSIG A** or **QSIG B** see Line (E1). QSIG trunks trunks are not supported on IP500 V2 systems without IP500 Voice Networking licenses.
Channel Allocation	Default = 23 | 1 The order, 23 to 1 or 1 to 23, in which channels are used.
Switch Type	Default = NI2 The options are: **4ESS**, **5ESS**, **DMS100**, **NI2**.
Provider	Default = Local Telco Select the PSTN service provider (**AT&T**, **Sprint**, **WorldCom** or **Local Telco**).
Prefix	Default = Blank Enter the number to prefix to all incoming numbers for callback. This is useful if all users must dial a prefix to access an outside line. The prefix is automatically placed in front of all incoming numbers so that users can dial the number back.

Table continues…

Variable	Description
Add 'Not-end-to-end ISDN' Information Element	Default = Never*. Sets whether the optional 'Not end-to-end ISDN' information element should be added to outgoing calls on the line. The options are: **Never**, **Always**, **POTS** (only if the call was originated by an analog extension). *The default is **Never** except for the following locales; for Italy the default is **POTS**, for New Zealand the default is **Always**.
Progress Replacement	Default = None. Progress messages are defined in the Q.931 ISDN connection control signaling protocol. Generally, if a progress message is sent, the caller does not get connected and so typically does not accrue call costs. Not all ISDN lines support Q.931 Progress messages. Use this setting to configure alternative signaling to the ISDN line for internally generated Progress messages. The options are: • **Alerting**: Map to Q.931 Alerting. The call is not connected. The caller does not hear the message and typically does not accrue call costs. • **Connect**: Map to Q.931 Connect. The caller hears the message and typically will accrue call costs.
Send Redirecting Number	Default = Off. This option can be used on ISDN trunks where the redirecting service is supported by the trunk provider. Where supported, on twinned calls the caller ID of the original call is passed through to the twinning destination. This option is only used for twinned calls.
Send Names	This option is available when the **Switch Type** above is set to **DMS100**. If set, names are sent in the display field. The **Z** shortcode character can be used to specify the name to be used.
Names Length	Set the allowable length for names, up to 15 characters, when **Send Names** is set above.
Test Number	Used to remember the external telephone number of this line to assist with loop-back testing. For information only.
Framing	Default = ESF Selects the type of signal framing used (ESF or D4).
Zero Suppression	Default = B8ZS Selects the method of zero suppression used (B8ZS or AMI ZCS).

Table continues…

Variable	Description
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available. • Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source. • In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.
CSU Operation	Tick this field to enable the T1 line to respond to loop-back requests from the line.
Haul Length	Default = 0-115 feet Sets the line length to a specific distance.
Channel Unit	Default = Foreign Exchange This field should be set to match the channel signaling equipment provided by the Central Office. The options are: **Foreign Exchange**, **Special Access**, **Normal**.
CRC Checking	Default = On Turns CRC on or off.
Line Signaling	The field can be set to either **CPE** (Customer Premises Equipment) or **CO** (Central Office). This field should normally be left at its default of **CPE**. The setting **CO** is normally only used in lab back-to-back testing.
Incoming Routing Digits	Default=0 (present call immediately) Sets the number of routing digits expected on incoming calls. This allows the line to present the call to the system once the expected digits have been received rather than waiting for the digits timeout to expire. This field only affects T1 line channels set to **E&M Tie**, **E&M DID**, **E&M Switched 56K** and **Direct Inward Dial**.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.
Send original calling party for forwarded and twinning calls	Default = Off. Use the original calling party ID when forwarding calls or routing twinned calls. This setting applies to the following ISDN lines: • PRI24 with subtypes: PRI, QSIGA, QSIGB, ETSI, ETSI CHI. • PRI30 with subtypes: QSIGA, QSIGB, ETSI, ETSI CHI.

Table continues…

Variable	Description
Originator number for forwarded and twinning calls	Default = blank. The number used as the calling party ID when forwarding calls or routing twinned calls. This field is grayed out when the **Send original calling party for forwarded and twinning calls** setting is enabled. This setting applies to the following ISDN lines: • PRI24 with subtypes: PRI, QSIGA, QSIGB, ETSI, ETSI CHI. • PRI30 with subtypes: QSIGA, QSIGB, ETSI, ETSI CHI.

Related links

T1 PRI Line on page 405

T1 ISDN Channels

Navigation: **System Settings** > **Line** > **T1 ISDN Channels**

This tab allows settings for individual channels within the trunk to be adjusted. This tab is not available for trunks sets to ETSI or QSIG mode.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Channel	Allocated by the system.
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.

Table continues…

Field	Description
Outgoing Group ID	Default = 1. Range 0 to 99999. When a short code specifies a number to dial, the IP Office will seize an available line from those available with a matching **Outgoing Group ID**. In a Server Edition/Select network, the **Outgoing Group ID** used for lines to a system must be unique within the network. **Reserved Group ID Numbers:** • **0** - In a Server Edition/Select network, the ID 0 cannot be used. • **90000 - 99999** - Reserved for system use (not enforced). - **96666** - Use for ACO lines. - **98888** - For IP Office deployed in an Enterprise Branch environment, reserved for the SM line. - **99001 - 99148** - In a Server Edition/Select network, reserved for the IP Office lines from the primary and secondary servers to each expansion system in the network. - **99998** - In a Server Edition/Select network, reserved for the IP Office lines to the secondary server. - **99999** - In a Server Edition/Select network, reserved for the IP Office lines to the primary server.
Line Appearance ID	Default = Auto-assigned. Range = 2 to 9 digits. Used for configuring Line Appearances with button programming. The line appearance ID must be unique and not match any extension number.
Direction	Default = Both Directions The direction of calls on the channel. The options are: **Incoming**, **Outgoing**, **Both Directions**.
Bearer	Default = Any The type of traffic carried by the channel. The options are: **Voice**, **Data**, **Any**.

Table continues…

Field	Description
Service	Default = None. If the line provider is set to AT&T, select the type of service provided by the channel. The options are: • **Call by Call** • **SDN (inc GSDN)** • **MegaCom 800** • **MegaCom** • **Wats** • **Accunet** • **ILDS** • **I800** • **ETN** • **Private Line** • **AT&T Multiquest** For other providers, the service options are **None** or **No Service**.
Admin	Default = Out of Service Used to indicate the channel status. The options are: **In Service**, **Out of Service**, **Maintenance**.
Tx Gain	Default = 0dB The transmit gain in dB
Rx Gain	Default = 0dB The receive gain in dB.

Related links

T1 PRI Line on page 405

T1 ISDN TNS

Navigation: **System Settings** > **Line** > **T1 ISDN TNS**

This tab is shown when the line Provider is set to AT&T. It allows the entry of the Network Selection settings. These are prefixes for alternative long distance carriers. When a number dialed matches an entry in the table, that pattern is stripped from the number before being sent out. This table is used to set field in the TNS (Transit Network Selection) information element for 4ESS and 5ESS exchanges. It is also used to set fields in the NSF information element.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
TNS Code	The pattern for the alternate long distance carrier. For example: The pattern 10XXX is added to this tab. If 10288 is dialed, 10 is removed and 288 is placed in the TNS and NSF information.

Related links

T1 PRI Line on page 405

T1 ISDN Special

Navigation: **System Settings** > **Line** > **T1 ISDN Special**

This tab is shown when the line Provider is set to AT&T. This table is used to set additional fields in the NSF information element after initial number parsing by the TNS tab. These are used to indicate the services required by the call. If the channel is set to Call by Call, then further parsing is done using the records in the Call by Call tab.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Short code	The number which results from the application of the rules specified in the User or System Short code tables and the Network Selection table and the Call-by-call table to the number dialed by the user.
Number	The number to be dialed to line.
Special	Default = No Operator. The options are: **No Operator**, **Local Operator** or **Presubscribed Operator**.
Plan	Default = National. The options are: **National** or **International**.

Typical values are:

Short Code	Number	Service
011N	N	No Operator, International
010N	N	Local Operator, International
01N	N	Local Operator, National
00N	N	Presubscribed Operator, National
0N	N	Presubscribed Operator, National
1N	1N	No operator, National

Related links

T1 PRI Line on page 405

Call By Call (US PRI)

Navigation: **System Settings** > **Line** > **T1 ISDN Call by Call**

This tab is shown when the line Provider is set to AT&T. Settings in this tab are only used when calls are routed via a channel which has its **Service** set to **Call by Call**.

It allows short codes to be created to route calls to a different services according to the number dialed. Call By Call reduces the costs and maximizes the use of facilities. Call By Call chooses the optimal service for a particular call by including the Bearer capability in the routing decision. This is particularly useful when there are limited resources.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Short Code	The number which results from the application of the rules specified in the User or System Short code tables and the Network Selection table to the number dialed by the user.
Number	The number to be dialed to line.
Bearer	Default = Any The type of traffic carried by the channel. The options are: • **Voice** • **Data** • **Any**
Service	Default = AT&T The service required by the call. The options are: • **Call by Call** • **SDN (inc GSDN)** • **MegaCom 800** • **MegaCom** • **Wats** • **Accunet** • **ILDS** • **I800** • **ETN** • **Private Line** • **AT&T Multiquest**

Related links

T1 PRI Line on page 405

SM Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SM Line**

This type of line is used to create a SIP connection between an IP Office and an Avaya Aura® Session Manager. The other end of the SIP connection must be configured on the Session Manager as a SIP Entity Link.

An SM Line can only be added to IP Office system Standard Mode or Server Edition configurations. It is typically used in IP Office Standard mode in Enterprise Branch deployments connected to the Avaya Aura® network. For more details about IP Office Enterprise Branch deployments refer to Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager.

An SM Line can also be used in IP Office Server Edition to connect to an Avaya Aura® Session Manager. Through the SM Line, IP Office Server Edition supports interoperability with Avaya Aura® Session Manager. It also supports interoperability, via the Avaya Aura® Session Manager, with Avaya Aura® Communication Manager systems and with CS 1000 systems. Note that IP Office Server Edition is not used as an enterprise branch product and does not support some of the IP Office enterprise branch functionality, such as management by Avaya Aura® System Manager, WebLM licensing, Centralized Users or voicemail over the SM Line.

If the Avaya Aura® network has multiple Avaya Aura® Session Managers to provide redundancy, two SM lines can be added, one configured for each Avaya Aura® Session Manager.

Related links

Line on page 303
SM Line Session Manager on page 414
SM Line VoIP on page 417
SM Line T38 Fax on page 421

SM Line Session Manager

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SM Line** > **Session Manager**

Additional configuration information

For additional information regarding the **Media Connection Preservation** setting, see Media Connection Preservation on page 743.

Configuration settings

These settings cannot be edited online. Changes to these settings require a reboot of the system.

Changing the **In Service** setting to **Disabled** (out of service) requires a system reboot. However, changing the **In Service** setting to **Enabled** is mergeable. Configuration changes made while the line is out of service are also mergeable.

Field	Description
Line Number	Default = Auto-filled. Range = 1 to 249 *(IP500 V2)*/349 *(Server Edition)*. Enter the line number that you wish. Note that this must be unique. On IP500 V2 systems, line numbers 1 to 16 are reserved for internal hardware. • **Session Manager line prioritization**: Up to two Session Manager lines can be configured. The two Session Manager lines are prioritized based on the line number. The lower line number is considered the primary Session Manager line. For example, if the first Session Manager line is configured as line number 17 and the second Session Manager line is configured as line 18, then line number 17 is considered the primary Session Manager line. If you want to designate the second Session Manager line (line 18 in this example) as the primary Session Manager line, you must change one or both of the line numbers so that the second Session Manager line is configured with a lower number than the current primary line. • **Session Manager line redundancy**: Based on the priority of the Session Manager lines designated by the line number, the active line to which the IP Office> sends all calls will always be the highest priority Session Manager line in service. That is, if the primary Session Manager line is in service, it will be the active line for sending calls. If the connection to the primary Session Manager line is lost, causing the IP Office to switch to the secondary Session Manager line, then when the primary line comes back up later, the IP Office reverts back to the primary Session Manager line.
In Service	Default = Enabled This option can be used to administratively disable the SM Line. It does not reflect the dynamic state of the line. If an SM Line is administratively disabled it is not equivalent to being in the dynamic out of service state.
SM Domain Name	This should match a SIP domain defined in the Session Manager system's SIP Domains table. Unless there are reasons to do otherwise, all the Enterprise Branch systems in the Avaya Aura® network can share the same domain.
SM Address	Enter the IP address of the Session Manager the line should use in the Avaya Aura network. The same Session Manager should be used for the matching **Entity Link** record in the Avaya Aura® configuration.
Outgoing Group ID	Default = 98888 This value is not changeable. However note the value as it is used in Enterprise Branch short codes used to route calls to the Session Manager.
Prefix	Default = Blank This prefix will be added to any source number received with incoming calls.
Max Calls	Default = 10 Sets the number of simultaneous calls allowed between the Enterprise Branch and Session Manager using this connection. Each call will use one of the available licenses that are shared by all SIP trunks configured in the system.

Table continues…

Field	Description
Network Type	Default = Public. This option is available when **System | Telephony | Telephony | Restrict Network Interconnect** is enabled. It allows you to configure trunks as either **Public** or **Private**. • The IP Office will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or the opposite. • The call restriction includes transfers, forwarding and conference calls. • Avaya does not recommended use of this feature on IP Office systems using any of the following features: multi-site networks, VPNremote, application telecommuter mode.
Include location specific information	Default = Off. Enabled when **Network Type** is set to **Private**. Set to **On** if the PBX on the other end of the trunk is toll compliant.
URI Type	Default = SIP. When **SIP** or **SIPS** is selected in the drop-down box, the SIP URI format is used (for example, name@example.com). This affects the **From** field of outgoing calls. The **To** field for outgoing calls will always use the format specified by the short codes used for outgoing call routing. Recommendation: When SIP Secured URI is required, the URI Type should be set to **SIPS**. **SIPS** can be used only when Layer 4 Protocol is set to TLS.
Media Connection Preservation	Default = Enabled. When enabled, attempts to maintain established calls despite brief network failures. Call handling features are no longer available when a call is in a preserved state. When enabled, Media Connection Preservation applies to Avaya H.323 phones that support connection preservation.
Location	
Network Configuration TLS connections support the following ciphers: • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA	
Layer 4 Protocol	Default = TCP.
Send Port	When Network Configuration is set to TLS, the default setting is 5061. When Network Configuration is set to TCP, the default setting is 5060.
Listen Port	When Network Configuration is set to TLS, the default setting is 5061. When Network Configuration is set to TCP, the default setting is 5060.

Table continues…

Field	Description
Session Timer	Default = 1200. Range = 90 to 64800 This field specifies the session expiry time. At the half way point of the expiry time, a session refresh message is sent. Setting the field to **On Demand** disables the session timer. Communication Manager supports SIP session refresh via UPDATE in Communicaton Manger release 6.2 SP1 and later. If using an earlier release of Communication Manager, then the **Session Timer** parameter must be set to **On Demand**.
Description	Default = Blank. Maximum 31 characters. You can use this field to enter a description for the configuration entry. The description is not used elsewhere.

Related links

SM Line on page 414

SM Line VoIP

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SM Line** > **VoIP**

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Codec Selection	Default = System Default Set the supported codecs. Where possible, Avaya recommend that you use the same set of codecs for all IP Office systems, lines, and extensions. The options are: • **System Default** - Use the codec list set in the system settings. • **Custom** - Configure a list of codec preferences for the line. - You can move codecs between the **Unused** and **Selected** sets and change the order of the codecs. - The codecs available are set by **System Settings** > **System** > **VoIP**. The possible codecs are: • **OPUS** - Supported on Linux-based IP Office systems only. • **G.711 ALAW/G.711 ULAW** • **G.729** • **G.723.1** - Supported on IP500 V2 systems only. • **G.722 64K** - Supported by Linux-based IP Office systems and on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards.

Table continues…

Field	Description
Fax Transport Support	Default = None. If enabled, when the IP Office detects fax tone, it will renegotiate the call codec as configured below. • This option requires **Re-Invite Supported**. • IP Office systems in a network support fax relay for fax calls between systems. • IP500 V2 systems can terminate T38 fax calls. • Linux-based IP Office systems can route the calls between trunks/terminals with compatible fax types. The supported options are: • **None** - Do not support fax. • **G.711** - Use G.711 to send and receive faxes. • **T38** - Use T38 to send and receive faxes. • **T38 Fallback** - Use T38 to send and receive faxes. If the call destination does not support T38, the IP Office will send a re-invite to change the transport method to **G.711**.
Call Initiation Timeout (s)	Default = 4 seconds. Range = 1 to 99 seconds. Sets how long the IP Office system should wait for a response to an attempt to initiate a call before following the alternate routes set in an ARS form.
DTMF Support	Default = RFC2833 (IP500 V2), RFC2833/RFC4733 (Linux-Based Server) Sets how the IP Office signals DTMF key press digits to the remote end. The options are: • **In Band** - Send digits as tones within the call audio. • **RFC2833** or **RFC2833/RF4733** - Send digits using a separate audio stream from the call audio. If not supported by the far end, the line reverts to using **In Band** signaling. • **Info** - Send the digits in SIP `INFO` packets.

Table continues…

Field	Description
Media Security	Default = Same as System. These setting control whether SRTP is used for this line and the settings used for the SRTP. The options are: • **Same as System**: Matches the system setting at **System Settings** > **System** > **VoIP Security**. • **Disabled**: Use RTP. • **Preferred**: Attempt to use SRTP. If SRTP call setup is unsuccessful, fall back to RTP. • **Enforced**: Use SRTP. If SRTP call setup is unsuccessful, the call fails. - For calls using **Dial Emergency**, the IP Office will switch to RTP if SRTP call setup fails.
Advanced Media Security Options	Default = Same as System. Sets the requirements for SRTP when enabled. • **Same as System**: Use the same settings as configured on **System Settings** > **System** > **VoIP Security**. • **Encryptions**: Default = RTP Sets which parts of a session SRTP protects using encryption. • **Authentication**: Default = RTP and RTCP Sets which parts of the session SRTP protects using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Not adjustable. The IP Office will accept authenticated packets that have a sequence number that is higher than or within 64 packets of the highest-numbered packet already received. • **Crypto Suites**: Default = *SRTP_AES_CM_128_SHA1_80*. Set the crypto suites SRTP uses for encryption. The options are *SRTP_AES_CM_128_SHA1_32* and *SRTP_AES_CM_128_SHA1_80*.
VoIP Silence Suppression	Default = Off When enabled, when the IP Office detects silence during an IP call, it does not send any audio data. • Lines between IP Office systems using G.711 ignore this feature. • On trunks between networked IP Office systems, you must enable the setting at both ends.

Table continues…

Field	Description
Allow Direct Media Path	Default = On This settings controls whether calls between IP endpoints and/or lines must go through the IP Office. • If disabled, calls go through the IP Office and use its resources. RTP relay allows calls between devices using the same audio codec to not require a voice compression channel. • If enabled, calls can take routes other than through the IP Office system. Both ends must support direct media and have matching VoIP settings. For example, both ends must use the same protocol (SIP or H.323), same addressing (IPv4 or IPv6), and so on. Otherwise, the call goes through the IP Office system. - For extensions, disabling **Requires DTMF** allows the extension to attempt direct media even if the other end has differing DTMF settings.
Re-Invite Supported	Default = Off. When enabled, the IP Office can use `Re-Invite` during a call to change the characteristics of the call. For example, when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk. • Requires the ITSP to also support `Re-Invite`. • This setting must be enabled for video support.
Codec Lockdown	Default = Off. After making a SIP offer with a list of codecs, the IP Office expects an answer with a single codec selected from the list. User agents that send an answer with multiple codecs expect to switch to any of those codecs during the call without further negotiation, which the IP Office does not support. Instead, loss of speech occurs if the user agent changes codec without renegotiating. • If enabled, when the IP Office receives an answer with multiple codecs, the IP Office sends a `re-INVITE` and a SIP offer with just one codec. • This option requires **Re-Invite Supported** enabled.
Force direct media with phones	Default = On When enabled, if an Avaya IP phone dials digits during a direct media call, the IP Office changes the call to indirect media and sends the digits as RFC2833. 15-seconds after the last digit, the IP Office changes the call back to direct media. • This setting is requires the line to have **Re-Invite Supported** and **Allow Direct Media Path** enabled, and **DTMF Support** set to **RFC2833/RF4733**.

Table continues…

Field	Description
G.711 Fax ECAN	Default = Off When enabled, if the IP Office detects a fax call, it switches to G.711 with echo cancellation (ECAN) based on the 'G.711 Fax ECAN field, NLP disabled, a fixed jitter buffer, and silence suppression is disabled. You can use this to avoid an ECAN mismatch with the trunk provider. • This setting is only available on IP500 V2 systems when **Fax Transport Support** is set to **G.711** or **T38 Fallback**.

Related links

SM Line on page 414

SM Line T38 Fax

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SM Line** > **SM Line T38 Fax**

The settings are available only on IP500 V2 since it can terminate T38 fax. On the **VoIP** settings for the line type, **Fax Transport Support** must be set to **T38** or **T38 Fallback**.

These settings are mergeable.

Field	Description
Use Default Values	Default = On. If selected, all the fields are set to their default values and greyed out.
T38 Fax Version	Default = 3. During fax relay, the two gateways will negotiate to use the highest version which they both support. The options are: **0**, **1**, **2**, **3**.
Transport	Default = UDPTL (fixed). Only **UDPTL** is supported. **TCP** and **RTP** transport are not supported. For **UDPTL**, redundancy error correction is supported. Forward Error Correction (FEC) is not supported.
Redundancy Redundancy sends additional fax packets in order to increase the reliability. However increased redundancy increases the bandwidth required for the fax transport.	
Low Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for low speed V.21 T.30 fax transmissions.
High Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for V.17, V.27 and V.28 fax transmissions.
TCF Method	Default = Trans TCF. TCF = Training Check Frame.

Table continues…

Field	Description
Max Bit Rate (bps)	Default = 14400. Lower rates can be selected if the current rate is not supported by the fax equipment or is found to not be reliable.
EFlag Start Timer (msecs)	Default = 2600.
EFlag Stop Timer (msecs)	Default = 2300.
Tx Network Timeout (secs)	Default = 150.
Scan Line Fix-up	Default = On.
TFOP Enhancement	Default = On.
Disable T30 ECM	Default = Off. When selected, disabled the T.30 Error Correction Mode used for fax transmission.
Disable EFlags For First DIS	Default = Off.
Disable T30 MR Compression	Default = Off.
NSF Override	Default = Off. If selected, the NSF (Non-Standard Facility) information sent by the T38 device can be overridden using the values in the fields below. **Country Code**: Default = 0. **Vendor Code**: Default = 0.

Related links

SM Line on page 414

Chapter 28: Locations

System Settings > **Locations**

Location records can be used to identify where particular extensions are physically located and to apply settings that need to differ from that location.

- When **Locations** have been defined, you must configure the system with one of those locations.

For additional configuration information, see:

- Emergency Call on page 772
- Configuring Call Access Control on page 827
- Preventing Toll Bypass on page 825

Defaults

By default, new lines and extensions are assigned the same location as set for their host IP Office system. However, their location setting can be changed individually. For IP extensions, the location can also be set to automatically by matching the IP extension's current IP address to the address settings of an existing location.

Networked Configurations

In networked IP Office configurations, each location entry and its settings are automatically replicated in the configuration of all IP Office systems in the network. The exception is the **Emergency ARS** setting which can be configured separately for the same location entry on each system.

Related links

Location on page 423
Address on page 426

Location

Navigation: **System Settings** > **Locations** > **Add/Edit Location** > **Locations**

You can use locations to apply a range of common settings to IP Office systems, extensions, and IP lines in the same physical location. For example, each location can define the timezone settings applied to extensions in that location. See Using Locations on page 739.

- When you have defined any **Location** entries, you must assign locations to each IP Office system in the network.

Settings

You can edit these settings online without needing to reboot the IP Office.

Field	Description
Location Name	Default = Blank. Use this field to set a name that identifies the location. • System alarms for emergency calls include the location name. • J189 phones with an emergency view button display the location name.
Location ID	Default = Automatically assigned. Read-only. For Avaya Wireless DECT, you can enter the value into the configuration of a base station. That associates emergency calls made by extensions using that base station with the location's emergency ARS and address settings. See the Deploying Avaya Wireless DECT with IP Office manual.
Subnet Address	Default = Blank (Not used) The IPv4 address associated with this location. • The value must be unique for each location. If there are overlapping IP address ranges, extensions will use the first match found which may not be the correct location.
Subnet Mask	Default = Blank. The subnet mask for the IPv4 address above.
Subnet Address (IPv6)	Default = Blank (Not used) The IPv6 subnet address for extensions in the location. • The value must be unique for each location. If there are overlapping IP address ranges, extensions will use the first match found which may not be the correct location. • If also using IPv4 **Subnet Address** and **Subnet Mask** to match extensions to a location, you need to create a separate location entry for IPv6 **Subnet Address (IPv6)**/**Prefix** extension IP address matching. • Supported on Linux-based IP Office R12.1 systems only. To enable IPv6 support, select **LAN1** > **LAN Setting (IPv6)** > **IPv6** and/or **LAN2** > **LAN Setting (IPv6)** > **IPv6**.
Prefix	Default = 64. Range 1 to 128. The prefix for the IPv6 sub-net address above.
Emergency ARS	Default = None. This setting sets which ARS entry the IP Office should use to route emergency calls made from the location. Refer to the IP Office Emergency Call Configuration manual. When the dialing on an extension associated with the location matches a **Dial Emergency** short code, this setting overrides the **Line Group ID** setting of the short code.
Fallback System	Default = No override. The list contains all configured IP Office lines and the associated IP Office system. The group of extensions associated with this location can fallback to the selected IP Office system.

Call Admission Control

The call admission control (CAC) settings allow you to control the number of IP trunk calls between locations. See Configuring Call Admission Control on page 827.

Field	Description
Total Maximum Calls	Default = Unlimited. Range = 1 - 99, Unlimited. Limit of all calls to or from other configured locations and the cloud.
External Maximum Calls	Default = Unlimited. Range = 1 - 99, Unlimited. Limit of calls to or from the cloud in this location.
Internal Maximum Calls	Default = Unlimited. Range = 1 - 99, Unlimited. Limit of calls to or from other configured locations in this location.
Parent Location for CAC	Default = None. The options are **None**, **Cloud** or the name of another configured location. • When set to **Cloud**, the IP Office treats the parent location as external to the IP Office network. The IP Office counts calls to this location from other locations as external, but does not apply any CAC limits to the location.

Time Settings

The IP Office supports location-based time on 1100, 1200, 1600, 9600 and J100 Series phones.

Field	Description
Time Zone	Default = Same as System Select a time zone from the list. • If set to **Same as System**, the location uses the same time zone as configured for the IP Office system: - For IP500 V2 systems, the time zone is set through the **System** > **System** menu. - For Linux-based servers, the time zone is set through the server's **Platform View** menus. • When set to a specific time zone, you can use the settings below to adjust the time.

Field	Description
Local Time Offset from UTC	Default = Based on the selected locale and time zone. See Avaya IP Office Locale Settings. Sets the local time difference from the UTC time value obtained using SNTP. For example, if the system or location is 5 hours behind UTC, set this field as **-05:00**. • You can adjust the offset in 15-minute increments. • Use this offset for the standard time. To apply any additional offset for daylight-saving time periods, using the settings below.

Table continues…

Field	Description
Automatic DST	Default = Based on the selected locale and time zone. See Avaya IP Office Locale Settings. When enabled, the system automatically corrects for daylight-saving time (DST) changes using the settings below.
Clock Forward/ Back Settings	Default = Based on the selected locale and time zone. See Avaya IP Office Locale Settings. This field displays entries for when the IP Office should apply and remove a daylight-saving time offset in addition to the **Local Time Offset from UTC**. You can configure up to 10 entries (20 for IP Office R11.1.3.2 and higher). • To edit an entry, select it and then click **Edit**. • To delete an entry, select it and click **Delete**. • To add a new entry, click **Add New Entry** at the bottom of the list. If necessary, delete an existing entry before adding a new one. Each entry has the following settings:

Field	Description
DST Offset	The number of hours to shift the local time for DST.
Clock Forward/Back	Select **Clock Forward** to see and edit when the clock will move forward to start daylight saving. Select **Clock Back** to see and edit when the clock will move backward to end daylight saving.
Local Time To Go Forward	The time of day to move the clock forward to start daylight saving.
Local Time To Go Back	The time of day to move the clock backward to end daylight saving.
Date for Clock Forward/Back	The date for moving the clock forwards or backwards. Select the date by double-clicking on it in the calendar.

Related links

Locations on page 423

Address

Navigation: **System Settings** > **Locations** > **Add/Edit Location** > **Address**

This information is used for SIP lines to an E911 service supporting RFC 4119 and RFC 5139. On emergency calls, the address information is included in the INVITE message.

To use the information, the **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Advanced** > **Send Location Info** settings must be enabled.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description	Example
Country Code	The country is identified by the two letter ISO 3166 code.	US
A1	National subdivisions (state, region, province, prefecture).	New York
A2	County, parish, gun (JP), district (IN).	King's County
A3	City, township, shi (JP).	New York
A4	City division, borough, city district, ward, chou (JP).	Manhattan
A5	Neighborhood, block.	Morningside Heights
A6	Street.	Broadway
RD	Primary road or street	Broadway
RDSEC	Trailing street suffix.	SW
RDBR	Road branch.	Lane 7
RDSUBBR	Road sub-branch.	Alley 8
PRD	Leading street direction.	N
POD	Trailing street suffix.	NE
STS	Street suffix.	Avenue, Platz, Street
PRM	Road pre-modifier.	Old
POM	Road post-modifier.	Extended
HNO	House number, numeric part only.	123
HNS	House number suffix.	A, 1/2
LMK	Landmark or vanity address.	Low Library
BLD	Building (structure).	Hope Theatre
LOC	Additional location information.	Room 543
PLC	Place type.	Office
FLR	Floor.	5
UNIT	Unit (apartment, suite).	12a
ROOM	Room.	450F
SEAT	Seat (desk, cubicle, workstation).	WS 181
NAM	Name (residence, business, or office occupant).	Joe's Barbershop
ADDCODE	Additional Code	13203000003
PCN	Postal community name.	Leonia
PC	Postal code.	10027-0401
POBOX	Post office box (P.O. box)	U40

Related links

Locations on page 423

Chapter 29: RAS

System Settings > **RAS**

A Remote Access Server (RAS) is a piece of computer hardware which sits on a corporate LAN and into which employees dial on the public switched telephone network to get access to their email and to software and data on the corporate LAN.

Click **Add/Edit RAS**to open the **RAS** page where you can provision a **RAS**. When you click **Add/Edit RAS**, you are prompted to specify the server where the **RAS** will be added.

- This type of configuration record is not available on subscription mode systems.

Related links

Add RAS on page 429

Add RAS

Navigation: **System Settings** > **RAS**

RAS

A Remote Access Server (RAS) is a piece of computer hardware which sits on a corporate LAN and into which employees dial on the public switched telephone network to get access to their email and to software and data on the corporate LAN.

This form is used to create a RAS service that the system offers Dial In users. A RAS service is needed when configuring modem dial in access, digital (ISDN) dial in access and a WAN link. Some systems may only require one RAS service since the incoming call type can be automatically sensed.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

Field	Description
Name	A textual name for this service. If **Encrypted Password** below is used, this name must match the **Account Name** entered in the Service form.
Extension	Enter an extension number if this service is to be accessed internally.
COM Port	For future use.

Table continues…

Field	Description
TA Enable	Default = Off Select to enable or disable - if enabled RAS will pass the call onto a TA port for external handling.
Encrypted Password	Default = Off This option is used to define whether Dial In users are asked to use PAP or CHAP during their initial log in to the RAS Service. If the Encrypted Password box is checked then Dial In users are sent a CHAP challenge, if the box is unchecked PAP is used as the Dial In Authorization method.

PPP

PPP (Point-to-Point Protocol) is a Protocol for communication between two computers using a Serial interface, typically a personal computer connected by phone line to a server.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

Field	Description
CHAP Challenge Interval (secs)	Default = 0 (disabled). Range = 0 to 99999 seconds. The period between successive CHAP challenges. Blank or 0 disables repeated challenges.
Header Compression	Default = Off Enables the negotiation and use of IP Header Compression as per RFC2507, RFC2508 and RFC2509.
PPP Compression Mode	Default = MPPC This option is used to negotiate compression (or not) using CCP. If set to MPPC or StacLZS the system will try to negotiate this mode with the remote Control Unit. If set to Disable CCP is not negotiated. The options are: • **Disable** Do not use or attempt to use compression. • **StacLZS** Attempt to use and negotiate STAC compression (the standard, Mode 3) • **MPPC** Attempt to use and negotiate MPPC (Microsoft) compression. Useful for dialing into NT Servers.

Table continues…

Field	Description
PPP Callback Mode	Default = Disable The options are: • **Disable**: Callback is not enabled • **LCP**: (Link Control Protocol) After authentication the incoming call is dropped and an outgoing call to the number configured in the Service will be made to reestablish the link. • **Callback CP**: (Microsoft's Callback Control Protocol) After acceptance from both ends the incoming call is dropped and an outgoing call to the number configured in the Service is made to reestablish the link. • **Extended CBCP**: (Extended Callback Control Protocol) Similar to Callback CP however the Microsoft application at the remote end will prompt for a telephone number. An outgoing call will then be made to that number to reestablish the link.
Data Pkt. Size	Default = 0. Range = 0 to 2048. This is the number of data bytes contained in a Data Packet.
BACP	Default = Off Allows negotiation of the BACP/BCP protocols. These are used to control the addition of additional B channels to simultaneously improve data throughput.
Multilink	Default = Off When enabled the system attempts to negotiate the use of the Multilink protocol (MPPC) on the link(s) into this Service. Multilink must be enabled if the more than one channel is allowed to be Bundled/Multilinked to this RAS Service.

Related links

RAS on page 429

Chapter 30: Services

Navigation Path: **System Settings** > **Services**

Services are used to configure the settings required when a user or device on the LAN needs to connect to a off-switch data service such as the Internet or another network. Services can be used when making data connections via trunk or WAN interfaces.

After creating a service, it can be used as the destination for an IP Route record. One service can also be set as the **Default Service**. That service will then be used for any data traffic received by the system for which no IP Route is specified.

The system supports the following types of service:

Service	Description
Remote Support Services	This type of tunnel is used by subscription mode IP Office systems for RSS connections routed to the system through COM. For details, refer to Using Customer Operations Manager for IP Office Subscription Systems.
Normal Service	This type of service should be selected when for example, connecting to an ISP.
WAN Service	This type of service is used when creating a WAN link. A User and RAS Service will also be created with the same name. These three records are automatically linked and each open the same form. Note however, that this type of Service cannot be used if the Encrypted Password option is checked. In this case, the RAS Service name must match the Account Name. Therefore either create each record manually or create an Intranet Service.
Intranet Service	This type of service can be selected to automatically create a User with the same name at the same time. These two records are linked and will each open the same form. The User's password is entered in the Incoming Password field at the bottom on the Service tab. An Intranet Services shares the same configuration tabs as those available to the WAN Service.
SSL VPN	The SSL VPN service provides secure tunneling between the Avaya IP Office hardware installed at a customer site and a remote Avaya VPN Gateway (AVG). This secure tunnel allows support personnel to offer remote management services to customers, such as fault management, monitoring, and administration. Refer to the Deploying Avaya IP Office™ Platform SSL VPN Services manual.

Related links

Normal, WAN, or Internet Service on page 433
SSL VPN Service on page 441
Remote Support Services on page 444

Normal, WAN, or Internet Service

Navigation: **System Settings** > **Services** > **Add/Edit Service** > **Normal / WAN / Internet**

Additional configuration information

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 806.

Configuration settings

Services are used to configure the settings required when a user or device on the LAN needs to connect to a off-switch data service such as the Internet or another network. Services can be used when making data connections via trunk or WAN interfaces.

After creating a service, it can be used as the destination for an IP Route record. One service can also be set as the **Default Service**. That service will then be used for any data traffic received by the system for which no IP Route is specified.

The system supports the following types of service:

Service	Description
Remote Support Services	This type of tunnel is used by subscription mode IP Office systems for RSS connections routed to the system through COM. For details, refer to Using Customer Operations Manager for IP Office Subscription Systems.
Normal Service	This type of service should be selected when for example, connecting to an ISP.
WAN Service	This type of service is used when creating a WAN link. A User and RAS Service will also be created with the same name. These three records are automatically linked and each open the same form. Note however, that this type of Service cannot be used if the Encrypted Password option is checked. In this case, the RAS Service name must match the Account Name. Therefore either create each record manually or create an Intranet Service.
Intranet Service	This type of service can be selected to automatically create a User with the same name at the same time. These two records are linked and will each open the same form. The User's password is entered in the Incoming Password field at the bottom on the Service tab. An Intranet Services shares the same configuration tabs as those available to the WAN Service.
SSL VPN	The SSL VPN service provides secure tunneling between the Avaya IP Office hardware installed at a customer site and a remote Avaya VPN Gateway (AVG). This secure tunnel allows support personnel to offer remote management services to customers, such as fault management, monitoring, and administration. Refer to the Deploying Avaya IP Office™ Platform SSL VPN Services manual.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Service Name	The name of the service. It is recommended that only alphanumeric characters be used.

Table continues…

Field	Description
Account Name	The user name that is used to authenticate the connection. This is provided by the ISP or remote system.
Password	Default = Blank Enter the password that is used to authenticate the connection. This is provided by the ISP or remote system.
Telephone Number	Default = Blank If the connection is to be made via ISDN enter the telephone number to be dialed. This is provided by the ISP or remote system.
Firewall Profile	Default = Internet01 if present, otherwise <None> From the list box select the Firewall Profile that is used to allow/disallow protocols through this Service.
Encrypted Password	Default = Off When enabled the password is authenticated via CHAP (this must also be supported at the remote end). If disabled, PAP is used as the authentication method.
Default Route	Default = Off When enabled this Service is the default route for data packets unless a blank IP Route has been defined in the system IP Routes. A green arrow appears to the left of the Service in the Configuration Tree. Only one Service can be the default route. If disabled, a route must be created under IP Route.
Incoming Password	Default = Blank Shown on WAN and Intranet services. Enter the password that will be used to authenticate the connection from the remote Control Unit. (If this field has appeared because you have created a Service and User of the same name, this is the password you entered in the User's Password field).

Bandwidth

These options give the ability to make ISDN calls between sites only when there is data to be sent or sufficient data to warrant an additional call. The calls are made automatically without the users being aware of when calls begin or end. Using ISDN it is possible to establish a data call and be passing data in less that a second.

Note:

The system will check **Minimum Call Time** first, then **Idle Period**, then the **Active Idle Period**.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Minimum No of Channels	Default = 1. Range = 1 to 30. Defines the number of channels used to connect for an outgoing connection. The initial channel must be established and stable, before further calls are made.

Table continues…

Field	Description
Maximum No of Channels	Default = 1. Range = 1 to 30. Defines the maximum number of channels to can be used. This field should contain a value equal to or greater than the Minimum Channels field.
Extra BW Threshold	Default = 50%. Range = 0 to 100%. Defines the utilization threshold at which extra channels are connected. The value entered is a %. The % utilization is calculated over the total number of channels in use at any time, which may be one, two etc. For example, if **Minimum Channels** set to 1, **Maximum Channels** set to 2 and **Extra Bandwidth** set to 50 - once 50% of first channel has been used the second channel is connected.
Reduce BW Threshold	Default = 10%. Range = 0 to 100%. Defines the utilization threshold at which additional channels are disconnected. The value entered is a %. Additional calls are only dropped when the % utilization, calculated over the total number of channels in use, falls below the % value set for a time period defined by the Service-Idle Time. The last call (calls - if Minimum Calls is greater than 1) to the Service is only dropped if the % utilization falls to 0, for a time period defined by the Service-Idle Time. Only used when 2 or more channels are set above. For example, if Minimum Channels set to 1, Maximum Channels set to 2 and Reduce Bandwidth is set to 10 - once the usage of the 2 channels drops to 10% the number of channels used is 1.
Callback Telephone Number	Default = Blank The number that is given to the remote service, via BAP, which the remote Control Unit then dials to allow the bandwidth to be increased. Incoming Call routing and RAS Services must be appropriately configured.
Idle Period (secs)	Default = 10 seconds. Range = 0 to 999999 seconds. The time period, in seconds, required to expire after the line has gone idle. At this point the call is considered inactive and is completely closed. For example, the 'Idle Period' is set to X seconds. X seconds before the 'Active Idle Period' timeouts the Control Unit checks the packets being transmitted/received, if there is nothing then at the end of the 'Active Idle Period' the session is closed & the line is dropped. If there are some packets being transmitted or received then the line stays up. After the 'Active Idle Period' has timed out the system performs the same check every X seconds, until there are no packets being transferred and the session is closed and the line dropped.

Table continues…

Field	Description
Active Idle Period (secs):	Default = 180 seconds. Range = 0 to 999999 seconds. Sets the time period during which time the line has gone idle but there are still active sessions in progress (for example an FTP is in process, but not actually passing data at the moment). Only after this timeout will call be dropped. For example, you are downloading a file from your PC and for some reason the other end has stopped responding, (the remote site may have a problem etc.) the line is idle, not down, no data is being transmitted/ received but the file download session is still active. After the set time period of being in this state the line will drop and the sessions close. You may receive a remote server timeout error on your PC in the Browser/FTP client you were using.
Minimum Call Time (secs):	Default = 60 seconds. Range = 0 to 999999 seconds. Sets the minimum time that a call is held up after initial connection. This is useful if you pay a minimum call charge every time a call is made, no matter the actual length of the call. The minimum call time should be set to match that provided by the line provider.
Extra Bandwidth Mode	Default = Incoming Outgoing Defines the mode of operation used to increases bandwidth to the initial call to the remote Service. The options are: • **Outgoing Only** Bandwidth is added by making outgoing calls. • **Incoming Only** Bandwidth is added by the remote service calling back on the BACP number (assuming that BACP is successfully negotiated). • **Outgoing Incoming** Uses both methods but bandwidth is first added using outgoing calls. • **Incoming Outgoing** Uses both methods but bandwidth is first added using incoming BACP calls.

IP

The fields in this tab are used to configure network addressing for the services you are running. Depending on how your network is configured, the use of Network Address Translation (NAT) may be required.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
IP Address	Default = 0.0.0.0 (address assigned by ISP) An address should only be entered here if a specific IP address and mask have been provided by the Service Provider. Note that if the address is in a different domain from the system then NAT is automatically enabled
IP Mask	Default = 0.0.0.0 (use NAT) Enter the IP Mask associated with the IP Address if an address is entered.

Table continues…

Field	Description
Primary Transfer IP Address	Default = 0.0.0.0 (No transfer) This address acts as a primary address for incoming IP traffic. All incoming IP packets without a session are translated to this address. This would normally be set to the local mail or web server address. For control units supporting a LAN1 and LAN2, the primary transfer address for each LAN can be set through the **System Settings** > **System** > **LAN1** and **System Settings** > **System** > **LAN2** tabs.
RIP Mode	Default = None Routing Information Protocol (RIP) is a method by which network routers can exchange information about device locations and routes. RIP can be used within small networks to allow dynamic route configuration as opposed to static configuration using. The options are: • **None** The LAN does not listen to or send RIP messages. • **Listen Only (Passive)** Listen to RIP-1 and RIP-2 messages in order to learn RIP routes on the network. • **RIP1** Listen to RIP-1 and RIP-2 messages and send RIP-1 responses as a sub-network broadcast. • **RIP2 Broadcast (RIP1 Compatibility)** Listen to RIP-1 and RIP-2 messages and send RIP-2 responses as a sub-network broadcast. • **RIP2 Multicast** Listen to RIP-1 and RIP-2 messages and send RIP-2 responses to the RIP-2 multicast address.
Request DNS	Default = Off. When selected, DNS information is obtained from the service provider. To use this, the DNS Server addresses set in the system configuration (System | DNS) should be blank. The PC making the DNS request should have the system set as its DNS Server. For DHCP clients the system will provide its own address as the DNS server.
Forward Multicast Messages	Default = On. By default this option is on. Multicasting allows WAN bandwidth to be maximized through the reduction of traffic that needs to be passed between sites.

Autoconnect

These settings enable you to set up automatic connections to the specified Service.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Auto Connect Interval (mins):	Default = 0 (disabled). Range = 0 to 99999 minutes. This field defines how often this Service will automatically be called ("polled"). For example setting 60 means the system will call this Service every hour in the absence of any normally generated call (this timer is reset for every call; therefore if the service is already connected, then no additional calls are made). This is ideal for SMTP Mail polling from Internet Service Providers.
Auto Connect Time Profile	Default = <None> Allows the selection of any configured Time Profiles. The selected profile controls the time period during which automatic connections to the service are made. It does NOT mean that connection to that service is barred outside of these hours. For example, if a time profile called "Working Hours" is selected, where the profile is defined to be 9:00AM to 6:00PM Monday to Friday, then automatic connection to the service will not be made unless its within the defined profile. If there is an existing connection to the service at 9:00AM, then the connection will continue. If there is no connection, then an automatic connection will be made at 9:00AM.

Quota

Quotas are associated with outgoing calls, they place a time limit on calls to a particular IP Service. This avoids excessive call charges when perhaps something changes on your network and call frequency increases unintentionally.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Quota Time (mins)	Default = 240 minutes. Range = 0 to 99999 minutes. Defines the number of minutes used in the quota. When the quota time is used up no further data can be passed to this service. This feature is useful to stop things like an internet game keeping a call to your ISP open for a long period. **Warning:** Setting a value here without selecting a Quota period below will stop all further calls after the Quota Time has expired.
Quota:	Default = Daily. Range = None, Daily, Weekly or Monthly Sets the period during which the quota is applied. For example, if the **Quota Time** is 60 minutes and the **Quota** is set to **Daily**, then the maximum total connect time during any day is 60 minutes. Any time beyond this will cause the system to close the service and prevent any further calls to this service. To disable quotas select **None** and set a **Quota Time** of zero. **Note:** The ClearQuota feature can be used to create short codes to refresh the quota time.

PPP

These settings enable you to configure Point to Point Protocol (PPP) in relation to this particular service. PPP is a protocol for communication between two computers using a Serial interface.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Chap Challenge Interval (secs)	Default = 0 (disabled). Range = 0 to 99999 seconds. The period between CHAP challenges. Blank or 0 disables repeated challenges.
Bi-Directional Chap	Default =Off.
Header Compression	Default = None selected Enables the negotiation and use of IP Header Compression. Supported modes are IPHC and VJ. IPHC should be used on WAN links.
PPP Compression Mode	Default = MPPC Enables the negotiate and use of compression. Do not use on VoIP WAN links. The options are: • **Disable** Do not use or attempt to use compression. • **StacLZS** Attempt to use STAC compression (Mode 3, sequence check mode). • **MPPC** Attempt to use MPPC compression. Useful for NT Servers.
PPP Callback Mode	Default = Disabled. The options are: • **Disable** Callback is not enabled • **LCP** (Link Control Protocol) After authentication the incoming call is dropped and an outgoing call to the number configured in the Service is made to re-establish the link. • **Callback CP** (Microsoft's Callback Control Protocol) After acceptance from both ends the incoming call is dropped and an outgoing call to the number configured in the Service is made to re-establish the link. • **Extended CBCP** (Extended Callback Control Protocol) Similar to Callback CP except the Microsoft application at the remote end prompts for a telephone number. An outgoing call is then made to that number to re-establish the link.

Table continues…

Field	Description
PPP Access Mode	Default = Digital64 Sets the protocol, line speed and connection request type used when making outgoing calls. Incoming calls are automatically handled (see RAS services). The options are: • **Digital64** Protocol set to Sync PPP, rate 64000 bps, call presented to local exchange as a "Data Call". • **Digital56** As above but rate 56000 bps. • **Voice56** As above but call is presented to local exchange as a "Voice Call". • **V120** Protocol set to Async PPP, rate V.120, call presented to local exchange as a "Data Call". This mode runs at up to 64K per channel but has a higher Protocol overhead than pure 64K operation. Used for some bulletin board systems as it allows the destination end to run at a different asynchronous speed to the calling end. • **V110** Protocol is set to Async PPP, rate V.110. This runs at 9600 bps, call is presented to local exchange as a "Data Call". It is ideal for some bulletin boards. • **Modem** Allows Asynchronous PPP to run over an auto-adapting Modem to a service provider (requires a Modem2 card in the main unit)
Data Pkt. Size	Default = 0. Range = 0 to 2048. Sets the size limit for the Maximum Transmissible Unit.
BACP	Default = Off. Enables the negotiation and use of BACP/BCP protocols. These are used to control the addition of B channels to increase bandwidth.
Incoming traffic does not keep link up	Default = On. When enabled, the link is not kept up for incoming traffic only.
Multilink/QoS	Default = Off. Enables the negotiation and use of Multilink protocol (MPPC) on links into this Service. Multilink must be enabled if there is more than one channel that is allowed to be Bundled/ Multilinked to this RAS Service.

Fallback

These settings allow you to set up a fallback for the Service. For example, you may wish to connect to your ISP during working hours and at other times take advantage of varying call charges from an alternative carrier. You could therefore set up one Service to connect during peak times and another to act as fallback during the cheaper period.

You need to create an additional Service to be used during the cheaper period and select this service from the Fallback Service list box (open the Service form and select the Fallback tab).

If the original Service is to be used during specific hours and the Fallback Service to be used outside of these hours, a Time Profile can be created. Select this Time Profile from the Time Profile list box. At the set time the original Service goes into Fallback and the Fallback Service is used.

A Service can also be put into Fallback manually using short codes, for example:

Put the service "Internet" into fallback:

- **Short Code**: *85
- **Telephone Number**: "Internet"
- **Line Group ID**: 0
- **Feature**: SetHuntGroupNightService

Take the service "Internet" out of fallback:

- **Short Code**: *86
- **Telephone Number**: "Internet"
- **Line Group ID**: 0
- **Feature**: ClearHuntGroupNightService

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
In Fallback	Default = Off. This option indicates whether the Service is in Fallback or not. A service can be set into fallback using this setting. Alternatively a service can be set into fallback using a time profile or short codes.
Time profile	Default = <None> (No automatic fallback) Select the time profile you wish to use for the service. The time profile should be set up for the hours that you wish this service to be operational, out of these hours the Fallback Service is used.
Fallback Service	Default = <None> Select the service that is used when this service is in fallback.

Dial In

Only available for WAN and Intranet Services. This tab is used to define a WAN connection.

To define a WAN connection, click Add and enter `WAN` if the service is being routed via a WAN port on a WAN3 expansion module.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Related links

Services on page 432

SSL VPN Service

Navigation: **System Settings** > **Services** > **Add/Edit Service** > **SSL VPN**

The SSL VPN service provides secure tunneling between the Avaya IP Office hardware installed at a customer site and a remote Avaya VPN Gateway (AVG). This secure tunnel allows support

personnel to offer remote management services to customers, such as fault management, monitoring, and administration.

For full details on how to configure and administer SSL VPN services, refer to the Deploying Avaya IP Office™ Platform SSL VPN Services manual.

For Server Edition, this type of configuration record can be saved as a template and new records created from a template.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Service Name	Enter a name for the SSL VPN service.
Account Name	Enter the SSL VPN service account name. This account name is used for authenticating the SSL VPN service when connecting with the Avaya VPN Gateway (AVG).
Account Password	Enter the password for the SSL VPN service account.
Confirm Password	Confirm the password for the SSL VPN service account.
Server Address	Enter the address of the VPN gateway. The address can be a fully qualified domain name or an IPv4 address
Server Type	Default = AVG. This field is fixed to **AVG** (Avaya VPN Gateway).
Server Port Number	Default = 443. Select a port number.

Session

Field	Description
Session Mode	Default = Always On. This setting is greyed out and cannot be adjusted.
Preferred Data Transport Protocol	Default = UDP. This is the protocol used by the SSL VPN service for data transport. Only **TCP** is supported. If you select **UDP** as the protocol when you configure the connection, UDP displays in this field but the SSL VPN service falls back to TCP.
Heartbeat Interval	Default = 30 seconds. Range = 1 to 600 seconds. Enter the length of the interval between heartbeat messages, in seconds. The default value is 30 seconds.
Heartbeat Retries	Default = 4. Range = 1 to 10. Enter the number of unacknowledged heartbeat messages that IP Office sends to AVG before determining that AVG is not responsive. When this number of consecutive heartbeat messages is reached and AVG has not acknowledged them, IP Office ends the connection.
Keepalive Interval	Default = 10 seconds. Range = 0 (Disabled) to 600 seconds. Not used for **TCP** connections. Keepalive messages are sent over the UDP data transport channel to prevent sessions in network routers from timing out.

Table continues…

Field	Description
Reconnection Interval on Failure	Default = 60 seconds. Range = 1 to 600 seconds. The interval the system waits attempting to re-establish a connection with the AVG. The interval begins when the SSL VPN tunnel is in-service and makes an unsuccessful attempt to connect with the AVG, or when the connection with the AVG is lost. The default is 60 seconds.

NAPT

The Network Address Port Translation (NAPT) rules are part of SSL VPN configuration. NAPT rules allow a support service provider to remotely access LAN devices located on a private IP Office network. You can configure each SSL VPN service instance with a unique set of NAPT rules. You can configure up to 64 rules.

Field	Description		
Application	Default = Blank Defines the communication application used to connect to the LAN device through the SSL VPN tunnel. When you select an application, the **Protocol** and **Port Number** fields are filled with the default values. The drop-down **Application** selector options and the associated default values are:		
	Application	**Protocol**	**External and Internal Port Number**
	Custom	TCP	0
	VMPro	TCP	50791
	OneXPortal	TCP	8080
	SSH	TCP	22
	TELNET	TCP	23
	RDP	TCP	3389
	WebControl	TCP	7070
Protocol	Default = TCP The protocol used by the application. The options are **TCP** and **UDP**.		
External Port Number	Default = the default port number for the application. Range = 0 to 65535 Defines the port number used by the application to connect from the external network to the LAN device in the customer private network.		
Internal IP address	Default = Blank. The IP address of the LAN device in the customer network.		
Internal Port Number	Default = the default port number for the application. Range = 0 to 65535 Defines the port number used by the application to connect to the LAN device in the customer private network.		

Fallback

Field	Description
In Fallback	Default = Off. This setting is used to indicate whether the SSL VPN service is in use or not. • To configure the service without establishing an SSL VPN connection, or to disable an SSL VPN connection, select this option. • To enable the service and establish an SSL VPN connection, de-select this option. • The **Set Hunt Group Night Service** and **Clear Hunt Group Night Service** short code and button features can be used to switch an SSL VPN service off or on respectively. The service is indicated by setting the service name as the telephone number or action data. Do not use quotation marks.

Related links

Services on page 432

Remote Support Services

Navigation: **System Settings** > **System** > **Services** > **Remote Support Services**

This type of tunnel is used by subscription mode IP Office systems for RSS connections routed to the system through COM. For details, refer to Using Customer Operations Manager for IP Office Subscription Systems.

TCP Tunnels

These settings are used to configure allowed TCP tunnel connections.

Field	Description
Application	Default = Blank You can use the drop-down menu to select from a range of services (**OneXPortal**, **SSH**, **Telnet**, **RDP**, **WebControl**). The **Protocol** and **Server Port Number** fields are then pre-filled with the defaults for the selected application. For other services, select **Custom**.
Protocol	Default = Blank Only **TCP** is supported.
Server IP Address	Default = Blank The address of the server to which the RSS tunnel connects.
Server Port Number	Default = Blank The server port for the tunnel connection.

Related links

Services on page 432

Chapter 31: Short Codes

System Settings > **Short Codes**

Dialing by users on the system can be compared to short codes. When a match occurs, the matching short code sets what should happen. This may be the triggering of some feature, changing a system setting, or changing the dialed number.

For additional configuration information, see Short Code Features on page 993.

Main content pane

The **Short Codes** main content pane lists provisioned short codes. The contents of the list depends on the filter option selected. Click the icons beside a short code to edit or delete.

Bulk delete: You can delete multiple records. Select the check box to the right of each record you want to delete and click **Delete**. You receive a prompt to confirm the deletion.

Click **Add/Edit Short Code** to open the Add Short Code window where you can provision a user. When you click **Add/Edit Short Code**, you are prompted to specify if the short code will be a global object or specific to a server.

Related links

Add Short Code on page 445

Add Short Code

Navigation: **System Settings** > **Short Codes** > **Add/Edit Short Code**

These settings are used to create System Short Codes. System short codes can be dialed by all system users. However the system short code is ignored if the user dialing matches a user or user rights short code.

Warning:

User dialing of emergency numbers must not be blocked. If short codes are edited, the users ability to dial emergency numbers must be tested and maintained.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

- For systems using record consolidation, you can only add and edit this type of record at the solution level. The record is then automatically copied to each IP Office system in the network.

Field	Description
Code	The dialing digits used to trigger the short code. Maximum length 31 characters. For details of the characters that you can use, see Short Code Characters on page 975.
Feature	Select the action to be performed by the short code. For descriptions of the features, see Short Code Features on page 993.
Telephone Number	The number dialed by the short code or parameters for the short code feature. This field can contain numbers and characters. For example, it can contain Voicemail Pro start point names, user names, hunt group names and telephone numbers (including those with special characters). Maximum length 31 characters. See Short Code Characters on page 975. The majority of North-American telephony services and SIP trunks use 'en-bloc' dialing. That is, they expect to receive the routing digits for a call as a single simultaneous set. Therefore, the use of a ; is recommended at the end of all dialing short codes that use an **N**. This is also recommended for all dialing where secondary dial tone short codes are being used.
Line Group ID	Default = 0. For short codes that result in the dialing of a number, that is short codes with a **Dial** feature, this field is used to enter the initially routing destination of the call. The drop down can be used to select the following from the displayed list: • **Outgoing Group ID**: The Outgoing Group ID's current setup within the system configuration are listed. If an **Outgoing Group ID** is selected, the call will be routed to the first available line or channel within that group. • **ARS**: The ARS records currently configured in the system are listed. If an ARS record is selected, the call will be routed by the setting within that ARS record. Refer to ARS Overview. • For calls matching **Dial Emergency** short codes, this setting is overridden by the **Emergency ARS** settings of the dialing extension's location.
Locale	Default = Blank. For short codes that route calls to voicemail, this field can be used to set the prompts locale that should be used if available on the voicemail server.
Force Account Code	Default = Off. For short codes that result in the dialing of a number, this field trigger the user being prompted to enter a valid account code before the call is allowed to continue.
Force Authorization Code	Default = Off. This option is only shown on systems where authorization codes have been enabled. If selected, then for short codes that result in the dialing of a number, the user is required to enter a valid authorization code in order to continue the call.

Related links

Short Codes on page 445

Chapter 32: Subscription

System Settings > **Subscription**

Subscriptions are monthly paid entitlements used by subscription mode systems. They can be divided into two main groups; per-user per-month user subscriptions and per-month application subscriptions. For more information, see Subscriptions on page 726.

Subscription are ordered from the Avaya Channel Marketplace, using the unique ID number of the system. Once ordered, details of the customer number and address of the subscription server are supplied in an email. Those details are then used during the initial system configuration.

Field	Descriptions
System ID	The unique number used for validation of subscriptions. • For IP500 V2 systems, this is the System SD card's PLDS ID as printed on the card. For older cards with 10-digits ID, the number is prefixed with 11. • For other systems, the ID is a unique value based on elements of the system hardware at the time of system installation.
Customer ID	This number is supplied in the email provided when the **System ID** is subscribed with Avaya.
Customer Name	The customer name used when the **System ID** was subscribed.
License Server	This address is supplied in the email provided when the **System ID** is subscribed with Avaya.

Available Subscriptions

The following subscriptions can be ordered for an IP Office Subscription system.

Table 1: User Subscriptions

Subscription	Description
Telephony User	Enables a user with telephony functions using a deskphone.
Telephony Plus User	Enable a user with telephony functions using an deskphone and or a softphone client on a PC.
UC User	Enable a user with the full range of telephony functions.

Table 2: Application Subscriptions

Subscription	Description
Receptionist Console	Enables use of the IP Office SoftConsole application to answer and redirect calls. The number of subscriptions allows the matching number of users to be configured as **Receptionist** users. Those users still require a user subscriptions for their telephone connection (IP Office SoftConsole is not a softphone).
Media Manager	This subscription enables support for Media Manager. This uses Voicemail Pro to perform call recording. Media Manager then collects and stores those recordings. Media Manager can be provided as a local or centralized service as follows: • Run locally on the same server as the Voicemail Pro service and storing the recordings on an additional hard disk installed in that server. This option is not supported if using a Unified Communications Module. • Run centralized and storing the recordings on the cloud-based servers providing the system's subscriptions. In this case, the number of subscriptions also controls the maximum number of recordings supported: 1. 150,000 2. 300,000 3. 500,000 4. 750,000 5. 1,000,000
Third-Party CTI	This subscription enables support for CTI connections by third-party applications. This includes DevLink, DevLink3, 3rd-party TAPI and TAPI WAV.
Avaya Contact Center Select	This subscription enables support the Avaya Contact Center Select (ACCS) service hosted on a separate server.
Avaya Call Reporter	This subscription enables support for the Avaya Call Reporter application, hosted on a separate server.

Chapter 33: System Directory

System Settings > **System Directory**

The system directory contains records for external contacts, that is their names and numbers. These can be displayed on phones in order to make outgoing calls. They can also be used to match a name to the number on incoming calls.

For additional configuration information, see Centralized System Directory on page 734.

Main content pane

The **System Directory** main content pane lists provisioned directory records. Click the icons beside a record to edit or delete.

Click **Add/Edit Directory Entry** to open the Add Directory window and configure a directory record.

Related links

Add Directory Entry on page 449

Add Directory Entry

Navigation: **System Settings** > **System Directory** > **Add/Edit Directory Entry**

Additional configuration information

For additional configuration information, see Centralized System Directory on page 734.

Configuration settings

Use these settings to create directory records that are stored in the system's configuration. Directory records can also be manually imported from a CSV file. The system can also use Directory Services to automatically import directory records from an LDAP server at regular intervals.

A system can also automatically import directory records from another system. Automatically imported records are used as part of the system directory but are not part of the editable configuration. Automatically imported records cannot override manually entered records.

For a Server Edition network, these settings can only be configured at the network level and they are stored in the configuration of the Primary Server. All other systems in the network are configured to share the directory settings of the Primary Server through their Manager settings at **System | Directory Services | HTTP**.

Directory Special Characters

The following characters are supported in directory records. They are supported in both system configuration records and in imported records.

- **? = Any Digit** Directory records containing a **?** are only used for name matching against the dialed or received digits on outgoing or incoming calls. They are excluded from the dialable directory. In the following example, any calls where the dialed or received number that starts 9732555 will have the display name Homdel associated with them.
  - **Name**: Holmdel
  - **Number**: 9732555?
- **( ) = Optional Digits** Brackets can be used to enclose an optional portion of a number, typically the area code. Only one pair of brackets are supported in a number. Records containing digits inside ( ) brackets are only used for user dialling. The full string is dialed with the ( ) brackets removed.
- **- Characters** Directory records can also contain **-** characters. Records containing **-** characters are only used for user dialing. The full string is dialed with the **-** character removed.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Index	Range = 000 to 999 or None. This value is used with system speed dials dialed from M and T-Series phones. The value can be changed but each value can only be applied to one directory record at any time. Setting the value to **None** makes the speed dial inaccessible from M and T-Series phones, however it may still be accessible from the directory functions of other phone types and applications. The Speed Dial short code feature can be used to create short codes to dial the number stored with a specific index value.
Name	Enter the text, to be used to identify the number. Names should not begin with numbers.
Number	Enter the number to be matched with the above name. The number is processed against the applicable user and system short codes. Note that if the system has been configured to use an external dialing prefix, that prefix should be added to directory numbers.

Related links

System Directory on page 449

Chapter 34: System

System Settings > **System**

This menu gives access to a set of sub-menus for settings that control system-wide behavior.

The System page lists all the systems in the IP Office Server Edition solution. There is one System record for each system being managed. Click on the icon to the right of the record to open the system configuration pages.

Related links

System on page 451
Voicemail on page 461
System Events on page 469
SMTP on page 476
DNS on page 477
SMDR on page 478
LAN1 on page 479
LAN2 on page 501
VoIP on page 501
Directory Services on page 506
Telephony on page 512
Contact Center on page 532
Avaya Cloud Services on page 532
Avaya Push Notification Services on page 535
Remote Operations on page 536

System

Navigation: **System Settings** > **System** > **System**

Additional configuration information

For additional information on time settings, see System Date and Time on page 783.

Configuration settings

These settings can be edited online except **Locale** and **Favor RIP Routes over Static Routes**. Those settings must be edited offline and requires a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Name	Default = System MAC Address. A name to identify this system. This is typically used to identify the configuration by the location or customer's company name. Some features such as H.323 Gatekeeper require the system to have a name. • This field is case sensitive and within any network of systems must be unique. • Do not use <, >, |, \0, :, *, ?, . or /.
Contact Information	Default = Blank. This field is only be edited by service user with administrator rights. If a value is entered, it sets the system under 'special control'. If the contact information is set using a standalone version of Manager, warnings that "`This configuration is under special control`" are given when the configuration is opened again. This can be used to warn other users of Manager that the system is being monitored for some specific reason and provide them with contact details of the person doing that monitoring.
Locale	Sets default telephony and language settings based on the selection. It also sets various external line settings and so must be set correctly to ensure correct operation of the system. See Avaya IP Office Locale Settings. • For individual users, the system settings can be overridden through their own locale setting Select **Call Management** > **Users** > **Add/Edit Users** > **User** > **Local**.
Location	Default = None. Specify a **Location** entry for the system. This location is then used as the default **Location** settings for all the system's extensions and lines unless they are specifically configured with a different location. See Using Locations on page 739. • When you have defined any **Location** entries, you must assign locations to each IP Office system in the network.
IPv6	Default = Disabled Supported on Linux-based IP Office systems only. When enabled, the IP Office system supports IPv6 features.
Device ID	Server Edition only. Displays the value set for **Device ID** on the **System** > **System Events** > **Configuration** tab. If SSL VPN is configured, Avaya recommends that the **Device ID** matches an SSL VPN service Account Name. Each SSL VPN service account name has an associated SSL VPN tunnel IP address. Having the displayed Device ID match an SSL VPN service account name helps identify a particular SSL VPN tunnel IP address to use for remotely managing the IP Office.

Table continues…

Field	Description
TFTP Server IP Address	Default = 0.0.0.0 (Disabled). On Server Edition Systems, the default on Secondary and Expansion servers is the Primary Server address.) If the **Phone File Server Type** below is set to **Custom**, this address is included as the TFTP file server address sent in the system's DHCP response to phones. • You can use the address `255.255.255.255` to broadcast for the first available TFTP server on the network. • IP Office Manager can act as a TFTP server to provide files from its configured binaries directory. This requires the IP Office Manager setting **File** > **Preferences** > **Preferences** > **Enable BootP and TFTP Servers** enabled. • On IP500 V2 systems, you can enter the LAN1 IP Address to use the system's own memory card as the TFTP file source. This requires the security setting **Unsecured Interfaces** > **Applications Controls** > **TFTP Directory Read** enabled.
HTTP Server IP Address	Default = 0.0.0.0 (Disabled). This address, if set, is used in a number of scenarios: • **DHCP Responses**: If the **Phone File Server Type** below is set to **Custom**, this address is included as the HTTP file server address sent in the system's DHCP response to phones. • **HTTP Redirection**: Redirect phone firmware file requests. See below. • **B199/H175 Phones/Vantage Phones**: Phone firmware file requests sent to the system from these types of phone are always redirected to this address (B199 phones running R1.0 FP6 or higher).
HTTP Server IP Address (IPV6)	Default = Blank (Disabled) Similar to **HTTP Server IP Address** above but for devices connected using IPv6. Requires • The IP Office supports IPv6 addresses in the following formats: - Full address: For example, `2001:0000:040F:0000:0000:0000:805B:001B`. - Replace one series of `:0000:` parts with `::`. For example, `2001:0000:040F::805B:001B`. - Replace any individual `:0000:` parts with `:0:`. For example, `2001:0:040F::805B:001B`. - Remove leading `0` zeros after any `:` colon. For example, `2001:0:40F::805B:1B`.
HTTP Server URI	Default = Value provided by the deployment's Customer Operations Manager. Used by subscription mode systems. • If set, software file requests from Avaya Workplace Client and Vantage phones are redirected to this address. • If not set, then the Avaya Workplace Client and Vantage phones use the **HTTP Server IP Address** setting.

Table continues…

Field	Description
Phone File Server Type	Default = Memory Card (IP500 V2)/Disk (Linux system). For IP phones (H.323 and SIP) using the system as their DHCP server, the DHCP response can include the address of a file server from which the phone should request files. The setting of this field controls which address is used in the DHCP response. The options are: • **Custom** The DHCP response the system provides to phones contains the addresses set in the **TFTP Server IP Address** and **HTTP Server IP Address** fields. • **Disk**: *(Linux systems only)* The system uses its hard disk for file requests from phones. The DHCP response the system provides to phones contains its the LAN address as the TFTP and HTTP file server address. • **Memory Card**: *(IP500 V2 only)* The system uses it memory card for file requests from phones. The DHCP response the system provides to phones contains its the LAN address as the TFTP and HTTP file server address. This is supported for up to 50 IP phones total. • **Manager**: *(IP500 V2 only)* The system forwards phone file requests to the configured **Manager PC IP Address** set below. The DHCP response the system provides to phones contains the system's LAN address as the HTTP file server address. - HTTP-TFTP Relay is support when using IP Office Manager as the TFTP server (not supported by Linux based systems). This is done by setting the **TFTP Server IP Address** to the address of the IP Office Manager PC and the **HTTP Server IP Address** to the control unit IP address. This method is supported for up to 5 IP phones total.
HTTP Redirection	Default = Off. Some phones allow the file server from which they request files, in this case the IP Office, to redirect the request to another file server. This is useful when the firmware files are large or to enable multiple IP Office systems to share a common firmware file server. • When enabled, for phones that support redirection, the IP Office redirects firmware file to the address set by the **HTTP Server IP Address** or **HTTP Server IP Address (IPV6)** settings. The fields are available when the **Phone File Server Type** is set to **Memory Card** or **Disk**. The IP Office supports HTTP redirection for the following phones: • 9600 Series and J100 Series phones. • B199, H175 and Vantage phone firmware requests are always redirected regardless of the **HTTP Redirection** and **Phone File Server Type** settings.
Manager PC IP Address	Default = 0.0.0.0 (Broadcast). This address is used when the **Phone File Server Type** is set to **Manager**.

Table continues…

Field	Description
Avaya HTTP Clients Only	Default = Off. When selected, the IP Office only responds to HTTP requests from another IP Office system, Avaya phone, or Avaya application.
Enable SoftPhone HTTP Provisioning	Default = Off. This option must be enabled if the IP Office Video Softphone is being supported.
Use Preferred Phone Ports	Default = Off Set the ports indicated in the auto-generated `46xxsettings.txt` file requested by phones. • **When not enabled:** IP Office addresses in the auto-generated `46xxsettings.txt` file use ports 80 (HTTP) and 443 (HTTPS). • **When enabled:** IP Office addresses in the auto-generated `46xxsettings.txt` file uses ports 8411 (HTTP) and 411 (HTTPS). Regardless of the setting, the IP Office will accept requests on HTTP 80 and HTTPS 443. This is required for legacy phones that do not use the `46xxsettings.txt` file settings and to redirect existing phones to the preferred phone ports.
Favor RIP Routes over static routes	Default = Off Supported on IP500 V2 IP Office systems. You can enabled RIP on the **LAN1**, **LAN2**, and on specific **Services**. This setting controls how the IP Office system uses a RIP route when it has a static route to the same destinations configured in the **IP Routes** settings. • **When enabled:** RIP routes to a destination override any static route to the same destination. This applies even if the RIP route has a higher metric. - The exception is RIP routes with a metric of 16 which are always ignored. - If a learned RIP route fails, the IP Office applies a metric of 16 for five minutes after the failure. • **When disabled:** RIP routes to destinations which have static routes configured are ignored.
Automatic Backup	Default = On. This command is available with IP500 V2 systems. When selected, as part of its daily backup process, the system automatically copies the folders and files from the **System SD** card's `/primary` folder to its `/backup` folder. Any matching files and folders already present in the **/backup** folder are overwritten. • On subscription mode systems, COM supports a separate daily backup of configuration settings.

Table continues…

Field	Description
Media Archival Solution	For subscription mode systems, this field sets with application is used as the voice recording library (VRL) application for call recordings: • **Local Media Manager** Use the media manager service running locally on the same server as the voicemail service. Refer to the Administering Avaya IP Office™ Platform Media Manager. • **Centralized Media Manager** Use the media manager service provided by the same cloud based services providing the system subscriptions.
Messaging Server	This field sets which service is used as the instant messaging server for Avaya applications. The following options are supported: • **one-X Portal** Use the system's Avaya one-X® Portal for IP Office server for instant messaging between IP Office clients, including Avaya Workplace Client. - This method is not supported for Avaya Workplace Client users who log in using SSO or email. User's must register directly to the IP Office system. • **Avaya Spaces** Use Avaya Cloud Services for instant messaging between Avaya Workplace Client users. - This requires the IP Office to be configure to support Avaya Cloud Services. See the IP Office Avaya Workplace Client Installation Notes manual. - This method does not support sending push notifications for instant messages. The iOS Avaya Workplace Client does not receive instant messages when suspended or in the background. - Avaya Cloud Services is not supported for Avaya Workplace Client extensions using IPv6.
Provider	Default = Not visible. This field is visible if the system has been branded by addition of a special license for a specific equipment provider. • The branding is fixed, that is it remains even if the license is subsequently removed. • The number shown is a unique reference to the particular equipment provider for whom the system has been branded. • When branded, the equipment provider's name is displayed on idle phone displays and other provider related features are enabled.

Table continues…

Field	Description
Reseller	This field is shown on subscription mode systems. The value is automatically set when the system is first subscribes. **Warning:** • Do not change the value except under guidance from Avaya. Changing the value can cause lose of the system's subscriptions and remote management services through COM.
Time Setting Config Source	Time and date settings are only shown for IP500 V2 based systems. The time and date for Linux-based servers are set through the server's **Platform View** menus. **Important:** An accurate time source and settings are vital to many functions, including any services that use certificates. Avaya recommend that you use SNTP and a reliable source such as `time.google.com`. • **SNTP** Use a list of SNTP servers to obtain the UTC time. The IP Office tries the listed servers in order until it receives a response. The IP Office makes a request following a reboot and every hour afterwards. - In a network, other IP Office servers can use the primary IP Office as their SNTP server. • **Voicemail Pro/Manager** *(Obsolete)* Both Windows-based Voicemail Pro and IP Office Manager can act as RFC868 Time servers for the IP Office. Use of other RFC868 server sources is not supported. They provide both the UTC time value and the local time as set on the PC. The system makes a request to the specified address following a reboot and every 8 hours afterwards. • **None** Enable users with **System Phone Rights** (**User** > **User**) to set the time and date from their own extension. The IP Office can still apply daylight saving settings to the manually set time.
File Writer IP Address	Default = 0.0.0.0 (Disabled) This field set the address of the PC allowed to send files to the System SD card installed in the system using HTTP or TFTP methods other than embedded file management. • On non-Linux based systems, this field sets the address of the PC allowed to send files to the memory card using HTTP or TFTP methods other than embedded file management. • For Linux based systems it is applied to non-embedded file management access to the `/opt/ipoffice` folder on the server. An address of 255.255.255.255 allows access from any address. If embedded file management is used, this address is overwritten by the address of the PC using embedded file management (unless set to 255.255.255.255).

Table continues…

Field	Description
Dongle Serial Number	Displayed ony for pre-Release 10.0 IP500 V2 systems using ADI licensing. For system's using PLDS licensing, see the **PLDS Host ID** (**License** > **License**). This field is for information only. It shows the serial number of the feature key dongle against which the system last validated its licenses. **Local** is shown for a serial port, Smart Card or System SD feature key plugged directly into the control unit. **Remote** is shown for a parallel or USB feature key connected to a feature Key Server PC. The serial number is printed on the System SD card and prefixed with **FK**.
System Identification	Displayed for Linux based systems. This field is for information only. This is the unique system reference that is used to validate licenses issued for this particular system. For a physical server this is a unique value based on the server hardware. For a virtual server this value is based on several factors including the LAN1 and LAN2 IP addresses, the host name and the time zone. If any of those are changed, the System ID changes and any existing licenses become invalid.
AVPP IP Address	Default = 0.0.0.0 (Disabled) Where Avaya 3600 Series SpectraLink wireless handsets are being used with the system, this field is used to specify the IP address of the Avaya Voice Priority Processor (AVPP)

Customize Locale Settings

The **Customize** locale matches the Saudi Arabia locale but with the following additional controls shown below. For other locales, these are set on .

Field	Description
Tone Plan	Default = Tone Plan 1 The tone plan control tones and ringing patterns. The options are: • **Tone Plan 1**: United States. • **Tone Plan 2**: United Kingdom. • **Tone Plan 3**: France. • **Tone Plan 4**: Germany. • **Tone Plan 5**: Spain.
CLI Type	Used to set the CLI detection used for incoming analog trunks. The options are: **DTMF**, **FSK BELL202**, and **FSK V23**.

Time Setting Config Source = None/SNTP

These settings are shown for IP500 V2 based systems where the **Time Setting Config Source** has been set to **None** or **SNTP**. The time, date and timezone for Linux-based servers are set through the server **Platform View** menus.

- If **Location** entries have been defined, a location must be assigned to the system. The location's time settings (other than time source) override the settings below unless set to **Same as System**.

Field	Description
Time Server Address	Default = Blank Displayed when the **Time Setting Config Source** is set to **SNTP**. For the SNTP servers, enter a list of IP addresses, host names, or fully-qualified domain names (FQDN). Separate each record with a space. The use of broadcast addresses is not supported. • The list is used in order of the records until a response is received. • In a network, other IP Office servers can use the primary IP Office as their SNTP server.
Time Zone	Select a time zone from the list. This sets the default time offset and DST to match the chosen time zone.

Field	Description
Local Time Offset from UTC	Default = Based on the selected locale and time zone. See Avaya IP Office Locale Settings. Sets the local time difference from the UTC time value obtained using SNTP. For example, if the system or location is 5 hours behind UTC, set this field as **-05:00**. • You can adjust the offset in 15-minute increments. • Use this offset for the standard time. To apply any additional offset for daylight-saving time periods, using the settings below.
Automatic DST	Default = Based on the selected locale and time zone. See Avaya IP Office Locale Settings. When enabled, the system automatically corrects for daylight-saving time (DST) changes using the settings below.

Table continues…

Field	Description
Clock Forward/ Back Settings	Default = Based on the selected locale and time zone. See Avaya IP Office Locale Settings. This field displays entries for when the IP Office should apply and remove a daylight-saving time offset in addition to the **Local Time Offset from UTC**. You can configure up to 10 entries (20 for IP Office R11.1.3.2 and higher). • To edit an entry, select it and then click **Edit**. • To delete an entry, select it and click **Delete**. • To add a new entry, click **Add New Entry** at the bottom of the list. If necessary, delete an existing entry before adding a new one. Each entry has the following settings:

Field	Description
DST Offset	The number of hours to shift the local time for DST.
Clock Forward/Back	Select **Clock Forward** to see and edit when the clock will move forward to start daylight saving. Select **Clock Back** to see and edit when the clock will move backward to end daylight saving.
Local Time To Go Forward	The time of day to move the clock forward to start daylight saving.
Local Time To Go Back	The time of day to move the clock backward to end daylight saving.
Date for Clock Forward/Back	The date for moving the clock forwards or backwards. Select the date by double-clicking on it in the calendar.

Time Setting Config Source = Voicemail Pro/Manager

These settings are shown for IP500 V2 based systems where the **Time Setting Config Source** has been set to **Voicemail Pro/Manager**.

Field	Description
IP Address	Default = 0.0.0.0 The address to which the IP Office should send time requests. This must be the address of an server running Voicemail Pro or IP Office Manager. • When set to 0.0.0.0, following a reboot the IP Office first makes the request to the **Voicemail Server IP** address if set and, if it receives no reply, then makes a broadcast request. • For Windows-based Voicemail Pro servers, if IP Office Manager is already running on the server when the voicemail service starts, voicemail will not act as a time server. • You can stop IP Office Manager acting as an RFC868 time server by deselecting the **Enable Time Server** option (**File** > **Preferences** > **Preferences**).

Table continues…

Field	Description
Time Offset	Default = 00:00. This value is not normally set as the IP Office matches any time changes, including daylight savings, that occur on the time source PC.

Related links

System on page 451

Voicemail

Navigation: **System Settings** > **System** > **Voicemail**

Additional configuration information

For information on the **SCN Resiliency Options**, refer to the IP Office Resilience Overview manual.

Configuration settings

The following settings are used to set the system's voicemail server type and location. Fields are enabled or grayed out as appropriate to the selected voicemail type. Refer to the appropriate voicemail installation manual for full details.

These settings can be edited online with the exception of **Voicemail Type** and **Voicemail IP Address**. These settings must be edited offline and requires a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Voicemail Type

Field	Description
Voicemail Type Sets the type of voicemail service used by the IP Office server.	
None	No voicemail operation.
Analogue Trunk MWI	Select this option to support receiving a message waiting indicator (MWI) signal from analog trunks terminating on the ATM4U-V2 card. MWI is a telephone feature that turns on a visual indicator on a telephone when there are recorded messages.

Table continues…

Field	Description
Avaya Aura Messaging	Select this option if you want to configure the system to use Avaya Aura Messaging as the central voicemail system. If you choose this option, you are still able to use Embedded Voicemail or Voicemail Pro at each branch to provide auto-attendant operation and announcements for waiting calls. When selected, access to voicemail is routed via an SM line to the numbers specified in the **AAM Number** field. The optional **AAM PSTN Number** can be configured for use when the SM Line is not in service. For a setup where the voicemail box numbers configured on Avaya Aura Messaging or Modular Messaging are same as the caller's DID, the short code to route the PSTN call should be such that the caller-id is withheld ("W" in the telephone-number of the shortcode). This is to make sure that, during rainy day - the voicemail system does not automatically go to the voicemail box of the caller based on the caller id.
Call Pilot	Select this option if you want to configure the system to use CallPilot over SIP as the central voicemail system. If you choose this option, you are still able to use **Embedded Voicemail** or Voicemail Pro at each branch to provide auto-attendant operation and announcements for waiting calls. When selected, access to voicemail is routed via SM line to the numbers specified in the **CallPilot Number** field. • The **CallPilot PSTN Number** field and associated **Enable Voicemail Instructions Using DTMF** check box are not supported. IP Office cannot access the CallPilot system over the PSTN when the Session Manager line is down. • Users can access their CallPilot voicemail by dialing the Voicemail Collect short code. Access to CallPilot voicemail from Auto Attendant cannot be enabled by setting a Normal Transfer action to point to the Voicemail Collect short code. If desired, it can be enabled by setting a Normal Transfer action to point to the CallPilot number.
Centralized Voicemail	Select this option when using a Voicemail Pro system installed and licensed on another system in a multi-site network. The outgoing line group of the IP Office line connection to the system with the Voicemail Pro is entered as the **Voicemail Destination**. In a Server Edition network this option is used on the Secondary Server and expansion systems to indicate that they use the Primary Server for as their voicemail server.
Distributed Voicemail	This option can be used when additional Voicemail Pro voicemail servers are installed in a SCN network and configured to exchange messages with the central voicemail server using email. This option is used if this system should use one of the additional servers for its voicemail services rather than the central server. This option is not supported by Server Edition systems. When selected: • The **Voicemail Destination** field is used for the outgoing H.323 IP line to the central system. • The **Voicemail IP Address** is used for the IP address of the distributed voicemail server the system should use.
Embedded Voicemail	IP500 V2 systems can store voicemail messages and prompts on the system's own memory card. It also supports internal auto-attendant configuration. For details, refer to IP Office Embedded Voicemail Installation.

Table continues…

Field	Description
Group Voicemail	This option is used to support third-party voicemail systems attached by extension ports in the group specified as the **Voicemail Destination**. Not supported by Server Edition systems.
Modular Messaging over SIP	Select this option if you want to configure the system to use Modular Messaging over SIP as the central voicemail system. • When selected, access to voicemail is routed via an SM line to the numbers specified in the **MM Number** field. • The optional **MM PSTN Number** can be configured for use when the SM Line is not in service.
Remote Audix Voicemail	Select this option if using a remote Avaya Intuity Audix or MultiMessage voicemail system. Requires entry of an **Audix Voicemail** license. This option is not supported by Server Edition systems.
Voicemail Lite/Pro	Select this option when using Voicemail Pro. The IP address of the PC being used should be set as the **Voicemail IP Address**. In a Server Edition network this option is used on the Primary Server. It can also be used on the Secondary Server if the Secondary server includes its own voice mail server. Use of Voicemail Pro requires licenses for the number of simultaneous calls to be supported.

Field	Description
Voicemail Mode	Default = IP Office Mode. This field is only shown here for **Embedded Voicemail**. For systems using Voicemail Pro, it can be changed using the **Default Telephony Interface** setting shown in IP Office Web Manager and the Voicemail Pro client. Voicemail provided by the IP Office system can use either **IP Office Mode** or **Intuity Mode** key presses for mailbox functions. End users should be provided with the appropriate mailbox user guide for the mode selected. You can switch between modes without losing user data, such as passwords, greetings, or messages. The following user guides are available from the Avaya support web site: • Using IP Office Embedded Voicemail Intuity Mode • Using IP Office Embedded Voicemail IP Office Mode • Using a Voicemail Pro Intuity Mode Mailbox • Using a Voicemail Pro IP Office Mode Mailbox

Table continues…

Field	Description
Voicemail Destination	Defaults: Non-Server Edition = Blank, Server Edition = IP trunk connection to the Primary Server. • When the **Voicemail Type** is set to **Remote Audix Voicemail**, **Centralized Voicemail** or **Distributed Voicemail**, this setting is used to enter the outgoing line group of the line configured for connection to the phone system hosting the central voicemail server. • When the **Voicemail Type** is set to **Group Voicemail**, this setting is used to specify the group whose user extensions are connected to the 3rd party voicemail system. • When the **Voicemail Type** is set to **Analogue Trunk MWI**, this setting is used to specify the phone number of the message center. All analogue trunks configured for **Analogue Trunk MWI** must have the same destination.
Voicemail IP Address	Defaults: Non-Server Edition = 255.255.255.255, Primary Server = Primary Server IP Address. This setting is used when the **Voicemail Type** is set to **Voicemail Pro** or **Distributed Voicemail**. It is the IP address of the PC running the voicemail server that the system should use for its voicemail services. • If the system is fitted with a UCM hosting Voicemail Pro, the field should be set to 169.254.0.2. • If set as 255.255.255.255, the control unit broadcasts on the LAN for a response from a voicemail server. If set to a specific IP address, the system connects only to the voicemail server running at that address.
Backup Voicemail IP Address	Defaults: Primary Server = Secondary Server IP Address, All others = 0.0.0.0 (Off). This option is supported with Voicemail Pro. An additional voicemail server can be setup but left unused. If contact to the voicemail server specified by the **Voicemail IP Address** is lost, responsibility for voicemail services is temporarily transferred to this backup server address.
Maximum Record Time	Default = 120 seconds. Range = 30 to 180 seconds. This field is only available when **Embedded Voicemail** is selected as the **Voicemail Type**. The value sets the maximum record time for messages and prompts.
Messages Button Goes to Visual Voice	Default = On. Visual Voice allows phone users to check their voicemail mailboxes and perform action such as play, delete and forward messages through menus displayed on their phone. By default, on phones with a **MESSAGES** button, the navigation is via spoken prompts. This option allows that to be replaced by Visual Voice on phones that support Visual Voice menus. For further details see the button action.
Enable Outcalling	Default = Off *(Outcalling not allowed)*. This setting is used to enable or disable system support for outcalling on **Embedded Voicemail** and Voicemail Pro. When not selected, all outcalling and configuration of outcalling through mailboxes is disabled. For Voicemail Pro, outcalling can also be disabled at the individual user mailbox level using the Voicemail Pro client.

Voicemail Channel Reservations

These settings allow the channels used for calls into voicemail to be reserved for particular functions. Unreserved channels can be used for any function but reserved channels cannot be used for any function other than that indicated.

Field	Description
Unreserved Channels	Default = All channels This setting shows the number of voicemail channels, out of the total available, that have not been reserved.
Auto-Attendant	Default = 0 This setting sets the number of channels reserved for calls directed to one of the configured auto-attendants. .
Announcements	Default = 0 This setting sets the number of channels reserved for announcements. When no channels are available, calls continue without announcements.
Voice Recording	Default = 0 This setting sets the number of channels reserved for voice recording other than mandatory voice recording (see below). If no channels are available, recording does not occur though recording progress may be indicated.
Mailbox Access	Default = 0 This setting sets the number of channels reserved for users accessing mailboxes to collect messages.
Mandatory Voice Recording	Default = 0 This setting sets the number of channels reserved for mandatory voice recording. When no channels are available for a call set to mandatory recording, the call is barred and the caller hears busy tone.

Call Recording

These settings apply to call recording provided by Voicemail Pro.

Field	Description
Maximum Recording Retention (Days)	Default = 30 days. Range 1 to 365 days. Used for subscription systems using Centralized Media Manager to store call recordings. This field sets how long recordings should be kept in the recording library before it is automatically deleted.
Auto Restart Paused Recording (sec)	Default = 15 seconds The value used to set a delay after which recording is automatically resumed.
Hide Auto Recording	Default = Cleared In addition to the audible advice of call recording prompt, Avaya Workplace Client displays a message that states the meeting or call is being recorded.

Table continues…

Field	Description
Play Advice on Call Recording	Default = On Sets whether an advice warning is played to all callers when their call is being recorded. It is a legal requirement in some countries to inform the callers before recording their calls, therefore you must get confirmation before you turn this option off. This option is not shown in IP Office Manager. It can be set through either IP Office Web Manager or the Voicemail Pro client.

Speech AI

These settings as available on subscription mode systems. If enabled, the system can use text-to-speech (TTS) and automatic speech recognition (ASR) services with auto-attendants and system meet-me conferences.

Field	Description
Google Speech AI	Default = Off If enabled, the system can use text-to-speech (TTS) and automatic speech recognition (ASR) services with auto-attendants and system meet-me conferences.
Speech Language	Default = Match the system locale language if possible. Sets the default language used for TTS prompts. This can be overridden by the particular setting of the auto-attendant or system meet-me conference.
Speech Voice	Sets the voice to be used with the speech language. The number of voices available varies depending on the speech language selected.

DTMF Breakout

Allows system defaults to be set. These are then applied to all user mailboxes unless the user's own settings differ.

The Park & Page feature is supported when the system voicemail type is configured as **Embedded Voicemail** or **Voicemail Pro**. It allows a call to be parked while a page is made to a hunt group or extension. This feature can be configured for Breakout DTMF 0, Breakout DTMF 2, or Breakout DTMF 3.

Park & Page is also supported on systems where Avaya Aura Messaging, Modular Messaging over SIP, or CallPilot (for IP Office Aura Edition with CS 1000 deployments) is configured as the central voice mail system and the local Embedded Voicemail or Voicemail Pro provides auto attendant operation.

Field	Description
Reception/ Breakout (DTMF 0)	The number to which a caller is transferred if they press 0while listening to the mailbox greeting rather than leaving a message (***0** on Embedded Voicemail in IP Office Mode). For voicemail systems set to Intuity emulation mode, the mailbox owner can also access this option when collecting their messages by dialing ***0**. If the mailbox has been reached through a Voicemail Pro call flow containing a **Leave Mail** action, the option provided when **0** is pressed are: • For IP Office mode, the call follows the **Leave Mail** action's **Failure** or **Success** results connections depending on whether the caller pressed **0** before or after the record tone. • For Intuity mode, pressing **0** always follows the **Reception/Breakout (DTMF 0)** setting. • When Park & Page is selected for a DTFM breakout, the following drop-down boxes appear: - **Paging Number**: Displays a list of hunt groups and users (extensions). Select a hunt group or extension to configure this option. - **Retries**: The range is 0 to 5. The default setting is 0. - **Retry Timeout**: Provided in the format M:SS (minute:seconds). The range can be set in 15-second increments. The minimum setting is 15 seconds and the maximum setting is 5 minutes. The default setting is 15 seconds
Breakout (DTMF 2)	The number to which a caller is transferred if they press 2while listening to the mailbox greeting rather than leaving a message (***2** on Embedded Voicemail in IP Office Mode).
Breakout (DTMF 3)	The number to which a caller is transferred if they press 3while listening to the mailbox greeting rather than leaving a message (***3** on Embedded Voicemail in IP Office Mode).

Voicemail Code Complexity

Defines the requirements for the voicemail code.

For IP Office systems that have **Voicemail Type** set to **Centralized**, the **Voicemail Code Complexity** settings must be the same as the IP Office system that is connected to Voicemail Pro.

Field	Description
Enforcement	Default = On. When on, a user PIN is required. The enforcement is not forced during upgrade but after checking, it can not be cleared.
Minimum Length	Default = 6. Maximum 31 digits. Older configurations can continue to have 4 digits with a maximum of 20 digits.

Table continues…

Field	Description
Complexity	Default = On. When on, the following complexity rules are enforced. • The user extension number cannot be used. • A PIN consisting of repeated digits is not allowed (111111). • A PIN consisting of a sequence, forward or reverse, is not allowed (123456, 564321). The number of users having invalid Voicemail Code complexity is highlighted below this field in red colored text.

SIP Settings

For Embedded Voicemail and Voicemail Pro, for calls made or received on a SIP line where any of the line's SIP URI fields are set to **Use Internal Data**, that data is taken from these settings. These options are shown if the system has SIP trunks and is set to use **Embedded Voicemail**, **Voicemail Lite/Pro**, **Centralized Voicemail** or **Distributed Voicemail**.

Field	Description
SIP Name	Default = Blank on Voicemail tab/Extension number on other tabs. This value is used for fields, other the `Contact` header, where the SIP URI entry being used has its **Contact** field set to **Use Internal Data**. • On incoming calls, if the **Local URI** is set to **Use Internal Data**, the system can potentially match the received `R-URI` or `From` header value to a user and/or group **SIP Name**. This requires the SIP URIs **Incoming Group** to match a Incoming Call Route with the same **Line Group ID** and a **.** (period) destination.
SIP Display Name (Alias)	Default = Blank on Voicemail tab/Name on other tabs. The value from this field is used when the **Display** field of the SIP URI being used is set to **Use Internal Data**.
Contact	Default = Blank on Voicemail tab/Extension number on other tabs. The value is used for the `Contact` header when the **Contact** field of the SIP URI being used for a SIP call is set to **Use Internal Data**.
Anonymous	Default = On on Voicemail tab/Off on other tabs. If the `From` field in the SIP URI is set to **Use Internal Data**, selecting this option inserts `Anonymous` into that field rather than the **SIP Name** set above. See Anonymous SIP Calls on page 935.

Voicemail Language Prompts

When the system routes a call to the voicemail server it indicates the locale for which matching prompts should be provided if available. The locale sent to the voicemail server by the system is determined as show below. If the required set of prompts is not available, the voicemail will fallback to another appropriate language and finally to English (refer to the appropriate voicemail installation manual for details).

- **Short Code Locale**: The short code locale, if set, is used if the call is routed to voicemail using the short code.

- **Incoming Call Route Locale**: The incoming call route locale, if set, is used if caller is external.
- **User Locale**: The user locale, if set, is used if the caller is internal.
- **System Locale**: If no user or incoming call route locale is set, the system locale is used unless overridden by a short code locale.

Systems using Embedded Voicemail, if the required set of upgraded language prompts to match the locale is not present on the system SD card, Manager will display an error. The required prompt set can be uploaded from Manager using the **Add/Display VM Locales** option.

Related links

System on page 451

System Events

Navigation: **System Settings** > **System** > **System Events**

The system supports a number of methods by which events occurring on the system can be reported. These are in addition to the real-time and historical reports available through the System Status Application (SSA).

Related links

System on page 451
SNMP Settings on page 469
Add SNMP Trap on page 471

SNMP Settings

Navigation: **System Settings** > **System-SNMP** > **SNMP Settings**

This form is used for general configuration related to system alarms.

Note that the QoS Parameters are only available in Manager.

Configuration Settings

These settings can only be edited offline. Changes to these settings require a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
SNMP Agent Configuration	
SNMP Enabled	Default = Off. Enables support for SNMP. This option is not required if using SMTP or Syslog.
Community (Read-only)	Default = Blank. The SNMP community name to which the system belongs.

Table continues…

Field	Description
SNMP Port	Default = 161. Range = 161, or 1024 to 65535. The port on which the system listens for SNMP polling.
Device ID	This is a text field used to add additional information to alarms. If an SSL VPN is configured, Avaya recommends that the Device ID match an SSL VPN service Account Name. Each SSL VPN service account name has an associated SSL VPN tunnel IP address. Having the displayed Device ID match an SSL VPN service account name helps identify a particular SSL VPN tunnel IP address to use for remotely managing IP Office.
Contact	This is a text field used to add additional information to alarms.
Location	This is a text field used to add additional information to alarms.

QoS Parameters

These parameters are used if the setting **System Settings** > **System** > **System Events** > **Enable RTCP Monitor on Port 5005** is set to On. They are used as alarm thresholds for the QoS data collected by the system for calls made by Avaya H.323 phones and for phones using VCM channels. If a monitored call exceeds any of the threshold an alarm is sent to the System Status application. Quality of Service alarms can also be sent from the system using Alarms.

- The alarm occurs at the end of a call. If a call is held or parked and then retrieved, an alarm can occur for each segment of the call that exceeded a threshold.
- Where a call is between two extensions on the system, it is possible that both extensions will generate an alarm for the call.
- An alarm will not be triggered for the QoS parameters recorded during the first 5 seconds of a call.

Round Trip Delay (msec)	Default = 350. Less than 160ms is high quality. Less than 350ms is good quality. Any higher delay will be noticeable by those involved in the call. Note that, depending on the compression codec being used, some delay stems from the signal processing and cannot be removed: G.711 = 40ms, G.723a = 160ms, G.729 = 80ms.		
Jitter (msec)	Default =20. Jitter is a measure of the variance in the time for different voice packets in the same call to reach the destination. Excessive jitter will become audible as echo.		
Packet Loss (%)	Default = 3.0. Excessive packet loss will be audible as clipped words and may also cause call setup delays.		
		Good Quality	**High Quality**
	Round Trip Delay	< 350ms	< 160ms
	Jitter	< 20ms	< 20ms
	Packet Loss	< 3%	< 1%

Related links

System Events on page 469

Add SNMP Trap

Navigation: **System Settings** > **System-SNMP** > **Add/Edit SNMP Trap**

Offline Editing

These settings must be edited offline.

To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

This form is used to configure what can cause alarms to be sent using the different alarm methods.

- Up to 5 alarm traps can be configured for use with the SNMP settings on the **System | System Events | Configuration** tab.
- Up to 3 email alarms can be configured for sending using the systems **System | SMTP** settings. The email destination is set as part of the alarm configuration below.
- Up to 2 alarms can be configured for sending to a Syslog destination that is included in the alarm settings.

Configuration Settings

These settings can only be edited offline. Changes to these settings require a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
New Alarm	This area is used to show and edit the alarm.
Destination To use SNMP or Email the appropriate settings must be configured on the Configuration sub-tab. Note that the Destination type is grayed out if the maximum number of configurable alarms destinations of that type has been reached. Up to 5 alarm destinations can be configured for SNMP, 3 for SMTP email, and 2 for Syslog	
Trap	If selected, the details required in addition to the selected Events are: • **Server Address**: Default = Blank. The IP address or fully qualified domain name (FQDN) of the SNMP server to which trap information is sent. • **Port**: Default = 162. Range = 0 to 65535. The SNMP transmit port. • **Community**: Default = Blank The SNMP community for the transmitted traps. Must be matched by the receiving SNMP server. • **Format**: Default = IP Office. The options are: - **IP Office** SNMP event alarms format in accordance with IP Office. - **SMGR** SNMP event alarms format in accordance with SMGR.

Table continues…

Field	Description
Syslog	If selected, the details required in addition to the selected Events are: • **IP Address**: Default = Blank. The IP address of the Syslog server to which trap information is sent. • **Port**: Default = 514. Range = 0 to 65535. The Syslog destination port. • **Protocol**: Default = UDP. Select UDP or TCP. • **Format**: Default = Enterprise. The options are: - **Enterprise** Syslog event alarms format in accordance with Enterprise. - **IP Office** Syslog event alarms format in accordance with IP Office.
Email	If selected, the details required in addition to the selected Events are: **Email**: The destination email address.
Minimum Security Level	Default = Warnings. The options are: • **Warnings**: All events, from Warnings to Critical, are sent. • **Minor**: Minor, major, and critical events are sent. Warnings are not sent. • **Major**: Major and critical events are sent. Warnings and minor events will not be sent. • **Critical**: Only critical events are sent.
Events	Default = None Sets which types of system events should be collected and sent. The table below lists the alarms associated with each type of event. Text in italics in the messages is replaced with the appropriate data. Items in [] brackets are included in the message if appropriate. The subject line of SMTP email alarms takes the form "System name: IP address - System Alarm".

Type	Events	Event State	Message
Entity	**Application**	Voicemail operation	The Voicemail server is now operational.
		Voicemail Failure	The Voicemail server is down.
		Voicemail Event - storage OK	The Voicemail server storage is OK.
		Voicemail Event - storage nearly full	The Voicemail server storage is nearly full.
		Voicemail Event - storage full	storage full The Voicemail server storage is full.
	Service	Feature license missing	Attempt to use a feature for which no license is installed. License Type: <name>
		All licenses in use	The following licenses are all in use. License Type: <name>
		Clock source changed	8kHz clock source changed. Details will be provided.

Table continues…

Type	Events	Event State	Message
		Logon failed	Logon failure reason will be provided.
		No free channels available	No free channels were available. Outgoing group ID: <number>
		Hold music file failure	Failed to load Hold Music source file.
		All resources in use	The following system resources are all in use: <resource type> will be provided.
		OEM card slot error	System running secondary software or error description with OEM card will be provided.
		Network interconnect failure	Details of the network interconnection failure will be provided.
		SIP message too large	SIP message Rx error - too large - ignored.
	Contact Flash Card	Change	The PC card in *name* has changed.
	Expansion Module	Operational	Expansion module *name* link is up.
		Failure	Expansion module *name* link is down.
		Error	Expansion module *name* link has a link error.
		Change	Expansion module *name* link has changed.
	Trunk	Operational	Trunk number (name) [on expansion module number] is now operational.
		Failure	Trunk number (name) [on expansion module number] is down.
	Trunk	Trunk seize failure	Seize failure: Channel [number] or Port [number].
		Incoming call outgoing trunk failure	Incoming call outgoing trunk: Channel [number] or Port [number].
		CLI not delivered	CLI not delivered: Channel [number] or Port [number].
		DDI incomplete	DDI incomplete. Expected Number of digits: .
		LOS	LOS
		OOS	OOS
		Red Alarm	Red Alarm
		Blue Alarm	Blue Alarm
		Yellow Alarm	Yellow Alarm
		IP connection failure	IP connection failure. IP Trunk Line Number: <number> or Remote end IP address: <IP address>

Table continues…

Type	Events	Event State	Message
		Small Community Network invalid connection	Small Community Network invalid connection. IP trunk line number: <number> or remote end IP address: <IP address>
	Link	Device changed	Device changed. Home Extension Number: .
		LDAP server communication failure	LDAP server communication failure
		Resource down	Link/resource down. Module type, number and name will be provided.
		SMTP server communication failure	SMTP server communication failure
		Voicemail Pro connection failure	Voicemail Pro connection failure
		Dialer connection failure	The Dialer connection has been lost.
	VCM	Operational	VCM module *name* is now operational.
		Failure	VCM module *name* has failed.
Memory Card	**Invalid Card**		
	Free Capacity		
Generic	**Generic**	Non-primary location boot alarm	System running backup software.
		Invalid SD Card	Incompatible or Invalid (System or Optional) SD Card fitted.
		Network link failure	Network Interface *name* (ip address) has been disconnected.
		Network link operational	Network Interface *name* (ip address) has been connected.
		System warm start	System has been restarted (warm start).
		System cold start	System has restarted from power fail (cold start).
		SNMP Invalid community	Invalid community specified in SNMP request.
License	**License Server**	Server Operational	The license server is now operational.
		Server failure	The license server is no longer operational.
	License Key Failure	License Key Failure	
Loopback	**Loopback**	Near end line loopback	Trunk number (*name*) [on expansion module *number*] is in near end loopback.
		Near end payload loopback	Trunk number (*name*) [on expansion module *number*] is in near end loopback with payload.

Table continues…

Type	Events	Event State	Message
		Loopback off	Trunk number (*name*) [on expansion module *number*] has no loopback.
Phone Change	**Phone Change**	Phone has been unplugged	The phone with id *n* has been removed from extension *extension* (*unit*, port *number*).
		Phone has been plugged in	The phone with type *type* (*id number*) has been plugged in for extension *extension* (*unit*, port *number*).
Quality of Service	**QoS Monitoring**	If Enable RTCP Monitor on Port 5005 is selected, any monitored calls that exceeds the set QoS Parameters causes an alarm.	
Syslog	**Basic Audit**	Events as written to the system Audit Trail. Available on Syslog output only.	
	Extended Audit	Configuration change information. Each message contains one configuration or security settings object attribute change, and optionally the previous and new values.	
	System Monitor	If selected, System monitor traces are packed into Syslog traces.	
System	**Configuration**	Small Community Network dial plan conflict	Small Community Network dial plan conflict
		No incoming call route for call	The following line had no Incoming Call Route for a call. Line: <number> or Line Group ID: <number>.
		Installed hardware failure	Installed hardware failure details will be provided.
	System Shutdown		
	Running Backup		
	Emergency Calls	Emergency call successful	Successful Emergency Call | Emergency call! Location:*location* Dialled:*dialled number* Called:*number* sent on the line CallerID: *ID* Usr:*user* Extn:*extension*
		Emergency call failed	Failed Emergency Call | Emergency *call*! Location:*location* Dialled:*dialled number*FailCause:*cause* Usr:*user* Extn: *extension*

Alarm Types

Note the following.

- **Voicemail Pro Storage Alarms**: The alarm threshold is adjustable through the Voicemail Pro client.
- **Embedded Voicemail Storage Alarms**: A disk full alarm is generated when the Embedded Voicemail memory card reaches 90% full. In addition a critical space alarm is generated at 99% full and an OK alarm is generated when the disk space returns to below 90% full.
- **Loopback**: This type of alarm is only available for systems with a United States locale.

The list of IP Office alarms is available on the Admin CD in the folder `\snmp_mibs\IPOffice`.

Related links

System Events on page 469

SMTP

Navigation: **System Settings** > **System** > **SMTP**

Offline Editing

These settings must be edited offline.

To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Configuration Settings

SMTP can be used as the method of sending system alarms. The email destination is set as part of the email alarms configured in **System Settings** > **System** > **System Events**.

SMTP can be used with Embedded Voicemail for Voicemail Email. The voicemail destination is set by the user's Voicemail Email address.

Field	Description
Server Address	Default = Blank This field sets the IP address of the SMTP server being used to forward SNMP alarms sent by email.
Port	Default = 25. Range = 0 to 65534. This field set the destination port on the SMTP server.
Email From Address	Default = Blank This field set the sender email address. Depending of the requirements of the SMTP server this may need to be a valid email address hosted by that server. Otherwise the SMTP email server may need to be configured to support SMTP relay.
Use STARTTLS	Default = Off. (Release 9.0.3). Select this field to enable TLS/SSL encryption. Encryption allows voicemail-to-email integration with hosted email providers that use secure transport.
Server Requires Authentication	Default = Off Select if the SMTP server requires authentication. When selected, the following fields become available
User Name	Default = Blank Sets the user name for SMTP server authentication.

Table continues…

Field	Description
Password	Default = Blank Sets the password for SMTP server authentication.
Use Challenge Response Authentication (CRAM-MD5)	Default = Off. Selected if the SMTP server uses CRAM-MD5.

Related links

System on page 451

DNS

Navigation: **System Settings** > **System** > **DNS**

These settings configure the DNS servers to which the IP Office system should send DNS request when it needs to resolve name addresses into numeric IP addresses.

- DNS is a mechanism through which the URL's such as `www.avaya.com` are resolved into IP addresses. Typically the customer's internet service provider (ISP) specifies the address of the DNS server their customers should use. In more complex networks, the customer may host their own DNS server.
- WINS (Windows Internet Name Service) is a mechanism used within a Windows network to convert PC and server names to IP addresses using a WINS server.

If the IP Office system is acting as a DHCP server, in addition to providing clients with their IP address settings, it can also provide them with their DNS and WINS settings if requested by the client.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Configuration Settings

Field	Description
DNS Service IP Address	Default = 0.0.0.0 (Do not provide DNS/Use DNS forwarding) The IPv4 address of the DNS Server. • If left at the default, the IP Office system uses its own LAN address as the DNS server for DHCP clients and forward DNS requests to the service provider when **Request DNS** is selected in the service being used (**Service** > **IP**). • The IP Office does not support DNS priority. If the DNS response contains multiple addresses with priority, the IP Office only uses the first address.
Backup DNS Server IP Address	Default = 0.0.0.0 (No backup) The alternate IPv4 DNS server address used if the server address above does not respond.

Table continues…

Field	Description
DNS Domain	Default = Blank (No domain) This is the domain name for your IP address. Your Internet service provider or network administrator provides this. Typically this field is left blank.
WINS Server IP Address	Default = 0.0.0.0 (Do not provide WINS) This is the IP address of your local WINS server. This is used by Windows PCs to connect to the NT server that is the network WINS server. Setting a value will result in sending a mode of "hybrid". • WINS settings are not supported on Linux-based IP Office systems.
Backup WINS Server IP Address	Default = 0.0.0.0 (No backup) This is alternate WINS server address used if the server address above does not respond.
WINS Scope	Default = Blank (no scope) This is provided by your network administrator or left blank.

Related links

System on page 451

SMDR

Navigation: **System Settings** > **System** > **SMDR**

The system can be configured to output SMDR (Station Message Detail Reporting) records for each completed call.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Output	Default = No Output. Select the type of call record that the system should create. The options are: • **No Output** – Do not generate SMDR records. • **SMDR Only** – Generate SMDR records and send those records using the settings below. • **Hosted Only** - Used for subscriptions systems only. Stores the system's SMDR records on the cloud services supporting the system. Specific users can be configured to access those settings through the user portal.
SMDR: Station Message Detail Recorder Communications This fields are available when SMDR is selected as the output. For information on SMDR record details, see the SMDR appendix.	

Table continues…

Field	Description
IP Address	Default = 0.0.0.0 (Listen). The destination IP address for SMDR records. Each time a new record is generated, the system will attempt to send the record to the address specified. • The address 0.0.0.0 puts the system into listen mode. Using an application such as HyperTerminal or Putty, a TCP/IP connection to the system's IP address and specified TCP port will collect any new and or buffered records. • Any other address puts the system into send mode. Each time a new record is generated, the system attempts to send the record to the specified address and port using a TCP/IP connection. If the connection is not successful, the record is buffered (see below) until a successful connection occurs for a subsequent new record.
TCP Port	Default = 0. The IP port for sending or collecting SMDR records.
Records to Buffer	Default = 500. Range = 10 to 3000. The system buffers new records when there is not TCP/IP connection. It can buffer up to 3000 SMDR records. If the cache is full, the system discards the oldest record each time a new record is added.
Call Splitting for Diverts	Default = Off. When enabled, for calls forwarded off-switch using an external trunk, the SMDR produces separate initial call and forwarded call records: • The two sets of records have the same **Call ID**. • The **Call Start Time** fields of the forwarded call records are reset from the moment of forwarding on the external trunk. This applies for: • Calls forwarded by forward unconditional, forward on no answer, forward on busy, DND or mobile twinning. • Calls forwarded off-switch by an incoming call route.

Related links

System on page 451

LAN1

Navigation: **System Settings** > **System** > **LAN1**

Used to configure the behavior of the services provided by the system's first LAN interface.

Up to 2 LAN's (LAN1 and LAN2) can be configured. The control unit has 2 RJ45 Ethernet ports, marked as LAN and WAN. These form a full-duplex managed layer-3 switch. Within the system configuration, the physical LAN port is LAN1, the physical WAN port is LAN2.

Configuring both interfaces with the same IP address on the same subnet is not supported. However, no warning is issued when this configuration is implemented.

Related links

System on page 451
Settings on page 480
Settings (IPv6) on page 483
VoIP on page 487
Network Topology on page 495

Settings

Navigation: **System Settings** > **System** > **LAN1** > **Settings**

Configuration Settings

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
IP Address	Default = 192.168.42.1 Sets or shows the IP Office IPv4 address on the LAN. • If the IP Office is also acting as a DHCP server for the LAN, this address is also the starting address for the DHCP address range.
IP Mask	Default = 255.255.255.0 or DHCP client. This is the IP subnet mask used with the **IP Address**.
Primary Transfer Address	Default = 0.0.0.0 (Disabled) This setting is available on LAN1 of IP500 V2 systems. Any incoming IP packets without a matching service or session are translated to this address if set.

Table continues…

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>RIP Mode</td><td>Default = None

This setting is available on IP500 V2 systems. Routing Information Protocol (RIP) lets network routers exchange information about device locations and routes. Routes learnt using RIP are known as 'dynamic routes'. The IP Office system also supports 'static routes' though its IP Route settings.

The options are:

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>None</td><td>The LAN does not listen to or send RIP messages</td></tr>
<tr><td>Listen Only (Passive)</td><td>Listen to RIP-1 and RIP-2 messages to learn RIP routes on the network.</td></tr>
<tr><td>RIP1</td><td>Listen to RIP-1 and RIP-2 messages. Send RIP-1 responses as a sub-network broadcast.</td></tr>
<tr><td>RIP2 Broadcast (RIP1 Compatibility)</td><td>Listen to RIP-1 and RIP-2 messages. Send RIP-2 responses as a sub-network broadcast.</td></tr>
<tr><td>RIP2 Multicast</td><td>Listen to RIP-1 and RIP-2 messages. Send RIP-2 responses to the RIP-2 multicast address.</td></tr>
</table></td></tr>
<tr><td>Enable NAT</td><td>Default = Off

This setting is available on IP500 V2 systems. It controls whether the IP Office should apply NAT to IP traffic from LAN1 to LAN2.</td></tr>
<tr><td>Number of DHCP IP Addresses</td><td>Default = 200. Range = 1 to 999.

This defines the number of sequential IP addresses available for DHCP clients.</td></tr>
</table>

Table continues…

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>DHCP Mode</td><td>Default = DHCP Client.
Sets the IP Office IPv4 DHCP mode for the LAN. When doing DHCP:
• For local devices on the LAN:
- The IP Office allocates LAN devices addresses from the bottom of the available address range upwards.
• For Dial-in users:
- The IP Office allocates addresses from the top of the available range downwards.
- The IP Office will only allocate an address from the same subnet as its own LAN address.
- If the IP Office is acting as a DHCP server on both LAN1 and LAN2, it allocates available addresses from the LAN1 pool first.
The DHCP options are:
<table><tr><th>Option</th><th>Description</th></tr><tr><td>Server</td><td>The system functions as a DHCP Server for the LAN, allocating IPv4 addresses when requested to other devices on the network and to PPP Dial-in users.</td></tr><tr><td>Disabled</td><td>The IP Office system is not a DHCP client or server.</td></tr><tr><td>Dial In</td><td>The IP Office functions as a DHCP server for PPP Dial-in users only.</td></tr><tr><td>Client</td><td>The IP Office system requests an IPv4 address from a DHCP server on the LAN.</td></tr></table></td></tr>
<tr><td>Advanced</td><td>Default = Disabled.
When functioning as a DHCP server, you can configure the IP Office with multiple address pools from which it can issue IPv4 addresses.
• When enabled, IP Office Web Manager displays the DHCP Pools settings below.</td></tr>
</table>

DHCP Pools

You can use DHCP pools to configure multiple sets of IPv4 addresses that the IP Office can allocate when configured as a DHCP server.

- IP Office Web Manager displays these settings when you have enabled **Advanced** above.
- On an IP500 V2 system, you can configure up to 8 pools.
- On Linux-based IP Office systems, you can configure up to 64 pools.
- The IP Office uses the **IP Address**, **IP Mask** and **Number of DHCP IP Addresses** settings set on the **LAN Settings** tab for the first pool.

When these actions are performed:

- For E129 and B179 SIP phone models, the IP Office triggers a reboot of the phones to renew their IP address lease and apply the new address settings.
- For the remaining DHCP clients, you must manually reboot the devices to force an IP addresses lease renewal. Otherwise, the devices continue to use the allocated IP addresses until the IP addresses lease time out expires. IP address lease time out is set to three days.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Apply to Avaya IP Phones Only</td><td>Default = Off.

When enabled, the IP Office only responds to DHCP requests from Avaya IP phones. Other devices must use static addresses or obtain their address from another DHCP server.

• In addition, Avaya IP phones will complete DHCP only with a DHCP server configured to support the same Site Specific Option Number (SSON) as set on the phone. For IP Office, the SSON numbers it supports are set on the System > LAN1 > VoIP and System > LAN2 > VoIP sub-tabs.

• After changing this setting, you must reboot DHCP client devices to force IP addresses updates.</td></tr>
<tr><td>DHCP Pool</td><td>When adding or editing pools, the options are:

<table><tr><th>Setting</th><th>Description</th></tr><tr><td>Start Address</td><td>Default = Blank

Sets the first IP address in the pool.</td></tr><tr><td>Subnet Mask</td><td>Default = 255.255.255.0

Sets the subnet mask for addresses issued from the pool.</td></tr><tr><td>Default Router</td><td>Default = 0.0.0.0

The default router address to include in the DHCP response.

• For pools issuing IP addresses on the same subnet as the IP Office LAN, entering 0.0.0.0 instructs the IP Office to issue the default router as being the Destination of the IP Route entry that matches the IP address and subnet mask.

• For pools issuing addresses for a different subnet from the IP Office LAN, you must set the default router to the correct value for devices on that subnet.</td></tr><tr><td>Pool Size</td><td>Default = 0

Set the number of client IP addresses available in the pool.</td></tr></table>
The first pool matches the IP Address, IP Mask and Number of DHCP IP Addresses on the LAN Settings sub-tab.</td></tr>
</table>

Related links

LAN1 on page 479

Settings (IPv6)

Navigation: **System Settings** > **System** > **LAN1** > **Settings (IPv6)**

You can use these settings to configure IPv6 address support on the LAN.

- The IP Office licensing and configuration requirements for remote extensions are the same for IPv6 as for IPv4. The IP Office treats any extension using an IPv6 global unicast address not issued by IP Office DHCP as a remote extension.

Configuration Settings

You must edit these settings offline. Select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
IPv6	Default = Disabled IP Office supports IPv6 on Linux-based IP Office systems only. When enabled, the IP Office system supports IPv6 features on the LAN. • If using the IP Office self-signed certificates, you must regenerate the self-signed IP Office certificates after enabling IPv6 support. • You can also configure the IP Office system IPv6 address settings through the server **Platform View**/**Web Control** menus. • Avaya supports IPv6 on IP Office LAN1. Avaya also supports IPv6 on LAN2 but only when IPv6 is enabled on LAN1 also.
IP Address	Default = Blank Sets or shows the IP Office IPv6 address on the LAN. • You cannot change the address if the IP Office is a DHCPv6 client. • You cannot change the address if the IP Office is using **Stateless Address Auto-configuration (SLAAC)**. • If setting a static address, the IP Office supports /64 subnet prefixes only. - The IP Office supports IPv6 addresses in the following formats: • Full address: For example, `2001:0000:040F:0000:0000:0000:805B:001B`. • Replace one series of `:0000:` parts with `::`. For example, `2001:0000:040F::805B:001B`. • Replace any individual `:0000:` parts with `:0:`. For example, `2001:0:040F::805B:001B`. • Remove leading `0` zeros after any `:` colon. For example, `2001:0:40F::805B:1B`.
Gateway	Display = Blank Displays the default gateway settings for routing. If not using DHCP, you can edit the field to change the setting.
Stateless Address Auto-configuration (SLAAC)	Default = Disabled If enabled: • The IP Office uses SLAAC (RFC4862) to set an IPv6 unicast address for the LAN, and to obtain details of the network IPv6 routers. • IP Office Manager disables all other settings on the tab. • Avaya assumes that dynamically addressed devices on the LAN use SLAAC for their IPv6 addresses.

Table continues…

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Number of DHCP IP Addresses</td><td>Default = 24. Range = 1 to 500.
This defines the number of sequential IP addresses available for DHCP clients.</td></tr>
<tr><td>DHCP Mode</td><td>Default = DHCP Client.
Set the IP Office IPv6 DHCP mode for the LAN. The options are:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Server Stateful</td><td>In response a DHCPv6 request, the IP Office issues information such as domain name, DNS server address, and file server address. This includes issuing an IPv6 address.
• The IP Office maintains details of the IPv6 addresses it has issued.</td></tr>
<tr><td>Server Stateless</td><td>In response to a DHCPv6 request, the IP Office issues information such as domain name, DNS server address, and file server address. However:
• The IP Office does not issue an IPv6 IP address.
• The IP Office expects other dynamically-addressed devices on the LAN to obtain their IPv6 address using mechanisms such as SLAAC.</td></tr>
<tr><td>Client</td><td>The IP Office system request IPv6 address information from a DHCPv6 server on the LAN.</td></tr>
<tr><td>Disabled</td><td>The IP Office system is not a DHCPv6 client or server.</td></tr>
</table></td></tr>
<tr><td>Advanced</td><td>Default = Disabled.
When functioning as a DHCP server, you can configure the IP Office with multiple address pools from which it can issue IPv6 addresses.
• When enabled, IP Office Web Manager displays the DHCP Pools (IPv6) settings below.</td></tr>
</table>

DHCP Pools (IPv6)

You can use DHCP pools to configure multiple sets of IPv4 addresses that the IP Office can allocate when configured as a stateful DHCPv6 server.

- IP Office Web Manager displays these settings when you have enabled **Advanced** above.
- Supported on Linux-based IP Office R12.1 systems only. To enable IPv6 support, select **LAN1** > **LAN Setting (IPv6)** > **IPv6** and/or **LAN2** > **LAN Setting (IPv6)** > **IPv6**.
- You can configure up to 64 pools.
- The IP Office uses the **IP Address** and **Number of DHCP IP Addresses** settings set on the **LAN Setting (IPv6)** tab for the first pool.

Field	Description
Apply to Avaya IP Phones Only	Default = Off. When enabled, the IP Office only responds to DHCP requests from Avaya IP phones. Other devices must use static addresses or obtain their address from another DHCP server. • In addition, Avaya IP phones will complete DHCP only with a DHCP server configured to support the same Site Specific Option Number (SSON) as set on the phone. For IP Office, the SSON numbers it supports are set on the **System** > **LAN1** > **VoIP** and **System** > **LAN2** > **VoIP** sub-tabs. • After changing this setting, you must reboot DHCP client devices to force IP addresses updates.
DNS Server (IPv6)	Default = :: (Do not use) The IPv6 address of the DNS server. If the IP Office system is acting as a DHCP server, in addition to providing clients with their IP address settings, it can also provide them with DNS if requested by the client. • If left at the default, the IP Office system uses its own LAN address as the DNS server for DHCP clients. • The IP Office does not support DNS priority. If the DNS response contains multiple addresses with priority, the IP Office only uses the first address.
Backup DNS Server (IPv6)	Default = :: (Do not use) The alternate IPv6 DNS server address clients can use if the server address above does not respond.
DHCP Pool	The first pool matches the **IP Address** and **Number of DHCP IP Addresses** on the **LAN Setting (IPv6)** sub-tab. When adding or editing pools, the options are:

Setting	Description
Start Address	Default = Blank Sets the first IP address in the pool. • The IP Office supports IPv6 addresses in the following formats: - Full address: For example, `2001:0000:040F:0000:0000:0000:805B:001B`. - Replace one series of `:0000:` parts with `::`. For example, `2001:0000:040F::805B:001B`. - Replace any individual `:0000:` parts with `:0:`. For example, `2001:0:040F::805B:001B`. - Remove leading `0` zeros after any `:` colon. For example, `2001:0:40F::805B:1B`.
Pool Size	Default = 0, Range = 1 to 500 Set the number of client IP addresses available in the pool.

Related links

LAN1 on page 479

VoIP

Navigation: **System Settings** > **System** > **LAN1** > **VoIP**

Additional configuration information

For more information on remote H.323 extensions, see “Configuring Remote H.323 Extensions” in the chapter **Configure general system settings** in Administering Avaya IP Office™ Platform with Web Manager.

Configuration settings

Used to set the system defaults for VoIP operation on the LAN interface.

The following settings can be edited online.

- **Auto-create Extn**
- **Auto-create User**
- **H.323 Signaling over TLS**
- **Remote Call Signaling Port**
- **Auto-create Extn/User**
- **Enable RTCP Monitoring on Port 5005**
- **RTCP collector IP address for phones**
- **Scope**
- **Initial keepalives**
- **Periodic timeout**
- **VLAN**
- **1100 Voice VLAN Site Specific Option Number (SSON)**
- **1100 Voice VLAN IDs**

The remaining settings must be edited offline. Changes to these settings requires a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

H.323 Gatekeeper Enable

Field	Description
H.323 Gatekeeper Enable	Default = Off This settings enables gatekeeper operation.

Table continues…

Field	Description
H.323 Signaling over TLS	Default = Disabled. For hosted deployments, default = Preferred. When enabled, TLS is used to secure the registration and call signaling communication between IP Office and endpoints that support TLS. The H.323 phones that support TLS are 9608, 9611, 9621, and 9641 running firmware version 6.6 or higher. When enabled, certificate information is configured in the `46xxSettings.txt` file on IP Office and automatically downloaded to the phone. When IP Office receives a request from the phone for an identity certificate, IP Office searches its trusted certificate store and finds the root CA that issued its identity certificate. IP Office then provides the root CA as an auto-generated certificate file named `Root-CA-xxxxxxxx.pem`. For information on IP Office certificates, see **Security** > **Certificates**. The options are: • **Disabled**: TLS is not used. • **Preferred**: Use TLS when connecting to a phone that supports TLS. • **Enforced**: TLS must be used. If the phone does not support TLS, the connection is rejected. When set to **Enforced**, the **Remote Call Signaling Port** setting is disabled. If TLS security is enabled (**Enforced** or **Preferred**), it is recommended that you enable a matching level of media security on **System Settings** > **System** > **VoIP Security**.
H.323 Remote Extn Enable	Default = Off. The system can be configured to support remote H.323 extensions in the case where NAT is used in the connection path. This could be the case where the IP Office is located behind a corporate NAT/Firewall router and/or the H.323 phone is located behind residential NAT enable router. The use of this option and the interaction and configuration of external third party elements is beyond the scope this help file. In the case where the public IP address of the corporate router is unknown, the LAN's Network Topology settings should be used to configure a STUN Server. Enabling **H.323 Remote Extn Enable** allows configuration of the **RTP Port number Range (NAT)** settings.

Table continues…

Field	Description
Auto-create Extn	Default = Off The field to set up auto creation of extensions for H.323 phones registering themselves with the System as their gatekeeper. If selected, the system displays the **Auto Create Extension Password** window prompting you to type a Password and Confirm Password. This password is used for subsequent auto creation of extensions. A message `H.323 Auto-Create Extension option is active` is flashed next to the **Auto Create Extension** field till the option is cleared. SIP Extensions use a separate setting, see below. This setting is not supported on systems configured to use WebLM server licensing. If using resilience backup to support Avaya IP phones, **Auto-create Extn** and **Auto-create User** should not be left enabled after initial configuration or any subsequent addition of new extensions and users. Leaving auto-create options enabled on a system that is a failover target may cause duplicate extension/user records on the multi-site network under multiple failure scenarios. For security, any auto-create settings that are enabled are automatically disabled after 24 hours.

SIP Trunks Enable

Field	Description
SIP Trunks Enable	Default = On. This settings enables support of SIP trunks. It also requires entry of **SIP Trunk Channels** licenses. Enabling **SIP Trunks Enable** allows configuration of the **RTP Port number Range (NAT)** settings.

SIP Registrar Enable

Field	Description
SIP Registrar Enable	Default = Off. If enabled, the IP Office can act as a SIP Registrar to which SIP endpoints register. • Separate SIP registrars can be configured on LAN1 and LAN2. • Registration of a SIP endpoint requires an available **IP Endpoints** license. • SIP endpoints are also still subject to the extension capacity limits of the system.

Table continues…

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>SIP Remote Extn Enable</td><td>Default = Off.

The system can be configured to support remote SIP extensions in the case where NAT is used in the connection path. This could be the case where the IP Office is located behind a corporate NAT/Firewall router and/or the SIP phone is located behind residential NAT enable router.

• This option cannot be enabled on both LAN1 and LAN2.

• The use of this option and the interaction and configuration of external third party elements is beyond the scope this help file.

In the case where the public IP address of the corporate router is unknown, the LAN's Network Topology settings should be used to configure a STUN Server. Enabling SIP Remote Extn Enable allows configuration of:

• the Remote UDP Port, Remote TCP Port, Remote TLS Port settings

• the Port Number Range (NAT) settings</td></tr>
<tr><td>Allowed SIP User Agents</td><td>Default = Block Blacklist Only

Select which SIP devices can register with the IP Office system, using SIP User Agents specified on System > VoIP > Access Control Lists tab.

The options are:

<table><tr><th>Setting</th><th>Description</th></tr><tr><td>Allow All</td><td>Do not block any devices based on their UA string.</td></tr><tr><td>Block Blacklist Only</td><td>Block devices with a UA string listed in the SIP UA Blacklist.</td></tr><tr><td>Avaya Clients & Whitelisted</td><td>Allow devices with an Avaya UA string or with a UA string listed in the SIP UA Whitelist.</td></tr><tr><td>Avaya Clients Only</td><td>Allow devices with an Avaya UA string.</td></tr><tr><td>Whitelisted Only</td><td>Allow devices with a UA string listed in the SIP UA Whitelist.</td></tr></table></td></tr>
<tr><td>Auto-create Extn/User</td><td>Default = Off.

The field to set up auto creation of extensions for SIP phones registering themselves with the SIP registrar. If selected, the system prompts you to enter and confirm the password is used for subsequent auto creation of extensions.

• This setting is not supported on systems configured to use WebLM server licensing.

• For security, any auto-create settings set to On are automatically set to Off after 24 hours.</td></tr>
</table>

Table continues…

Field	Description
SIP Domain Name	Default = Blank This value is used by SIP endpoints for registration with the IP Office system. SIP endpoints register with IP Office using their SIP address that consists of their phone number and IP Office SIP domain. Since IP Office does not allow calls from unauthorized entities, the SIP domain does not need to be resolvable. However, the SIP domain should be associated with FQDN (Fully Qualified Domain Name) for security purposes. The entry should match the domain suffix part of the SIP Registrar FQDN below, for example, `example.com`. If the field is left blank, registration uses the LAN 1, LAN2, or public IP address. **Note:** For Avaya SIP telephones supported for resilience, the **SIP Domain Name** must be common to all systems providing resilience.
SIP Registrar FQDN	Default = Blank The fully-qualified domain name to which the SIP endpoint send their registration requests. For example, `sbc.example.com`. • This FQDN is also used for **Avaya Cloud Services** and **Avaya Push Notification Services** The customer DNS must resolve this FQDN to an IP address that routes to the IP Office. That is: • For local extensions, the IP address of the IP Office LAN. • For remote extensions, the external IPv4 address of the Avaya SBC or customer firewall that routes to the IP Office.
Challenge Expiry Time (secs)	Default = 10. The challenge expiry time is used during SIP extension registration. When a device registers, the IP Office SIP Registrar sends a challenges and waits for a response. If a response is not received within this timeout, the registration fails.
Layer 4 Protocol	Default = TCP 5060 + UDP 5060. Sets the ports on which the IP Office listens for SIP extension connections. Note that most SIP clients use TLS/TCP/UDP in order of priority unless configured otherwise, and will not fallback to a lower priority protocol even if it is enabled on the IP Office. • **UDP Port**: Default = 5060 Enabled. • **TCP Port**: Default = 5060 Enabled. • **TLS Port**: Default = 5061 Disabled.

Table continues…

Field	Description
	The following additional port settings are used if **SIP Remote Extn Enable** is selected. Otherwise, the ports above are used for all SIP extension connections. They set the ports the ports on which the IP Office listens for SIP extension connections from remote extensions: • **Remote UDP Port**: Default = 5060 Enabled. • **Remote TCP Port**: Default = 5060 Enabled. • **Remote TLS Port**: Default = 5061 Disabled.

RTP

Field	Description
Port Number Range	For each VoIP call, a receive port for incoming Real Time Protocol (RTP) traffic is selected from a defined range of possible ports, using the even numbers in that range. The Real Time Control Protocol (RTCP) traffic for the same call uses the RTP port number plus 1, that is the odd numbers. On some installations, it may be a requirement to change or restrict the port range used. It is recommended that only port numbers between 49152 and 65535 are used, that being the range defined by the Internet Assigned Numbers Authority (IANA) for dynamic usage. **Important:** The minimum and maximum settings of the port range should only be adjusted after careful consideration of the customer network configuration and existing port usage. The gap between the minimum and maximum port values must be at least 254.
Port Range (minimum)	Default: IP500 V2 = 46750/Linux = 40750. Range = 1024 to 65530. This sets the lower limit for the RTP port numbers used by the system.
Port Range (maximum)	Default = 50750. Range = 1024 to 65530. This sets the upper limit for the RTP port numbers used by the system.

Port Number Range (NAT)

These settings are available when either **H.323 Remote Extn Enable**, **SIP Trunks Enable**, or **SIP Remote Extn Enable** is set to On.

This option is not supported if **System Settings** > **System** > **LAN1** > **Network Topology** is set to **Symmetric Firewall** or **Open Internet**.

Field	Description
Port Range (minimum)	Default: IP500 V2 = 46750/Linux = 40750. Range = 1024 to 65530. This sets the lower limit for the RTP port numbers used by the system.
Port Range (maximum)	Default = 50750. Range = 1024 to 65530. This sets the upper limit for the RTP port numbers used by the system.

Table continues…

Field	Description
Enable RTCP Monitor On Port 5005	Default = On. For 1600, 4600, 5600, 9600 and J100 Series phones, the system can collect VoIP QoS (Quality of Service) data from the phones. For other phones, including non-IP phones, it can collect QoS data for calls that use a VCM channel. The QoS data collected by the system is displayed by the System Status Application. • This setting is mergeable. However, it is only applied to IP phones when they register with the system. Therefore, any change to this setting requires the IP phones that have already registered to be rebooted. IP phones can be remotely rebooted using the System Status Application. • The QoS data collected includes: RTP IP Address, Codec, Connection Type, Round Trip Delay, Receive Jitter, Receive Packet Loss. • This setting is not the same as the RTCPMON option within Avaya H.323 phone settings. The system does not support the RTCPMON option.
RTCP collector IP address for phones	Default = Blank. Sets the destination for the RTCP Monitor data described above. This enables you to send the data collected to a third party QoS monitoring application. The **Enable RTCP Monitor On Port 5005** must be turned Off to enable this field. Changes to this setting requires a reboot of the phones.

Keepalives

These settings are used to keep open external connections through devices such as firewalls and session-border controllers. You can use these settings when the IP Office has connections to SIP trunks and/or H323 and SIP remote workers.

Field	Description
Scope	Default = Disabled Select whether the sending of keepalive packets should be disabled or sent for RTP or for both RTP and RTCP.
Periodic timeout	Default = 0 (Off). Range = 0 to 180 seconds. Sets how long the system will wait before sending a keepalive if no other packets of the select **SCOPE** are seen.
Initial keepalives	Default = Disabled. If enabled, keepalives can also been sent during the initial connection setup.

DiffServ Settings

When transporting VoIP over low speed links, data packets (1500 byte packets) can block or delay voice packets (typically 67 or 31 bytes). This can cause poor speech quality. Therefore, all traffic routers in a network should support Quality of Service (QoS).

The IP Office system supports the DiffServ (RFC2474) QoS mechanism. This uses a Type of Service (ToS) field in the IP packet header.

The IP Office applies the LANs DiffServ settings to outgoing traffic on any SIP lines which have **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Transport** > **Use Network Topology Info** set to match the LAN interface.

- The hex and decimal entry fields for the following values are linked. The hex value is equal to the decimal multiplied by 4.
- Do not use the same values for call signaling and call media (audio and voice).
- For correct operation, the same value must be set at both ends.

Field	Description
DSCP (Hex)	Default = B8 (Hex)/46 (decimal). Range = 00 to FF (Hex)/0 to 63 (decimal) The DiffServ Code Point (DSCP) setting applied to the media on VoIP calls. By default, this value is applied to both audio and video unless a separate video value is set.
Video DSCP (Hex)	Default = B8 (Hex)/46 (decimal). Range = 00 to FF (Hex)/0 to 63 (decimal) The DSCP setting applied to video VoIP calls.
DSCP Mask (Hex)	Default = FC (Hex)/63 (decimal). Range = 00 to FF (Hex)/0 to 63 (decimal) The mask applied to packets for the DSCP value.
SIG DSCP (Hex)	Default = 88 (Hex)/34 (decimal). Range = 00 to FF (Hex)/0 to 63 (decimal) This DSCP setting applied to the call signaling on VoIP calls. This must not match the settings used for the media.

DHCP Settings

Field	Description
Primary Site Specific Option Number (4600/5600)	Default = 176. Range = 128 to 254. A site specific option number (SSON) is used as part of DHCP to request additional information. 176 is the default SSON used by 4600 Series and 5600 Series IP phones.
Secondary Site Specific Option Number (1600/9600)	Default = 242. Range = 128 to 254. Similar to the primary SSON. 242 is the default SSON used by 1600 and 9600 Series IP phones requesting installation settings via DHCP.
VLAN	Default = Not present. This option is applied to H.323 phones using the system for DHCP support. If set to **Disabled**, the L2Q value indicated to phones in the DHCP response is 2 (disabled). If set to **Not Present**, no L2Q value is included in the DHCP response.
1100 Voice VLAN Site Specific Option Number (SSON)	Default = 232. This is the SSON used for responses to 1100/1200 Series phones using the system for DHCP.
1100 Voice VLAN IDs	Default = Blank. For 1100/1200 phone being supported by DHCP, this field sets the VLAN ID that should be provided if necessary. Multiple IDs (up to 10) can be added, each separated by a + sign.

Related links

LAN1 on page 479

Network Topology

Navigation: **System Settings** > **System** > **LAN1** > **Network Topology**

These settings are used for support of external SIP trunks when not using an SBC. They are also used for supporting remote SIP/H323 extensions.

Network Address Translation (NAT) Overview

The network address translation (NAT) done by firewalls can affect VoIP calls. Two methods that can be used to overcome this are STUN or TURN.

NAT Method	Description
STUN	STUN (*"Session Traversal for NAT"*) is a mechanism to overcome the effect of some NAT firewalls. In summary: • The device configured for STUN sends test packets to the STUN server address. These go through the firewall NAT process. • The STUN server replies, including in the reply copies of the original packets it received. • By comparing the packets sent and received, the sender can try to determine the type of NAT applied. It can then modify future packets it sends to other destinations to overcome the effects of the firewall NAT.
TURN	TURN (*"Traversal Using Relays around NAT"*) is a NAT traversal mechanism that works by relaying all traffic via a TURN server. This is typically a TURN service provided by the customer's SBC.

STUN allows direct connection between the sender and receiver once setup, but is more restricted in the types of NAT with which it can work. TURN supports more types of NAT, but also needs to relay all traffic between the sender and receiver via the TURN server. STUN is easier to implement and maintain compared to TURN, however most SBC devices support TURN.

Configuration Settings

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

General

These settings are used by the IP Office for connection to a STUN server to support SIP trunks.

Field	Description
IP Office STUN Server	Default = Blank The IP address or fully qualified domain name (FQDN) of the STUN server the IP Office should use. The system will send basic SIP messages to this destination and from data inserted into the replies can try to determine the type NAT changes being applied by any firewall between it and the ITSP.

Table continues…

Field	Description
Port	Default = 3478. Sets the port to which the STUN requests are sent.
Run STUN	This button tests STUN operation between the system LAN using the settings above. The results are used to automatically fill the **NAT** fields with appropriate values discovered by the system. A information icon is then shown against the fields to indicate that the values were automatically discovered rather than manually entered. Before using **Run STUN**, the SIP trunk must be configured.
Run STUN on startup	Default = Off This option is used in conjunction with values automatically discovered using **Run STUN**. When selected, the system reruns STUN discovery whenever the system is rebooted or connection failure to the SIP server occurs.

WebRTC

These settings are used for remote User Portal users using WebRTC (**Softphone** mode) to make and receive calls using STUN and/or TURN. The values set are provided to the remote user portal sessions through their normal MTCTI connection.

Field	Description
WebRTC Client STUN Server	Default = Blank (use `stun.freeswitch.org:3478`) Set the IP address or FQDN of the STUN server that the clients should use.
Port	Default = 3748 The port the clients should use for STUN.
WebRTC Client Turn Server	Default = Blank This is used for solutions that use a TURN service configured on an SBC. It provides the IP address or FQDN of the TURN service. • You can add the required port by adding `:<port number>`. For example add `:3748` to the address or FQDN. • You can set the required transport method by adding `?transport=udp` or `?transport=tcp` to the address or FQDN. By default UDP is assumed. • The TURN server connection uses the name and password of an IP Office service user. - The service user must be a member of the security rights group **TURN Server** with **TURN Server Connection** enabled. - On new and defaulted systems, a service user called **TURNServer** exists and is a member of the **TURN Server** rights group. However the service user is disabled by default. • The details of the TURN server address, name and password are passed to IP Office User Portal sessions using their MTCTI connection to the IP Office.

NAT

The following fields can be completed either manually or the system can attempt to automatically discover the appropriate values using **Run STUN**.

To complete the fields automatically:

1. Check that the SIP trunk to the ITSP is configured.
2. Set the **IP Office STUN Server** address.
3. Test STUN by clicking **Run STUN**.
4. Close and reload the configuration. If STUN was successful, the remaining fields are updated using the results. A icon is shown against the fields to indicate that the values were automatically discovered rather than manually entered.

Field	Description
Firewall/NAT Type	Default = Unknown The settings here reflect different types of network firewalls. For descriptions of the various options, see the table below.
Binding Refresh Time (seconds)	Default = 0 (Never). Range = 0 to 3600 seconds. To keep the firewall port open for incoming calls, the system can send recurring `SIP OPTIONS` requests to the remote proxy terminating the trunk. This setting configures the frequency of those requests. If you do not set a binding refresh time, you may experience problems receiving inbound SIP calls after a short period of normal operation.
Public IP Address (IPv4)	Default = 0.0.0.0 If no address is set, the system's **LAN1** address is used.
SIP Registrar public ports	The public port values for **UDP**, **TCP**, and **TLS**. • **UDP** - Default = 5060 • **TCP** - Default = 5056 • **TLS** - Default = 5061

Firewall/NAT Type	Description
Blocking Firewall	–
Full Cone NAT	A full cone NAT is one where: • All requests from the same internal IP address and port are mapped to the same external IP address and port. • Any external host can send a packet to the internal host, by sending a packet to the mapped external address. • SIP packets need to be mapped to NAT address and Port. • Any host in the internet can call on the open port. The local info in the SDP will apply to multiple ITSP Hosts.

Table continues…

Firewall/NAT Type	Description
Open Internet	If this mode is selected, the IP Office ignores settings obtained by STUN lookups. The IP address used is that of the IP Office system's LAN interface.
One-To-One NAT	This setting supports deployments where the IP Office is behind a NAT that performs IP address translation but not port mappings. All required ports must be open on the NAT. When set to **One-To-One NAT**, the following configuration settings are applied and cannot be edited. • The **NAT** > **SIP Registrar public ports** values are set to 0. • The **LAN1** > **VoIP** > **SIP Registrar Enable** remote protocol port values are set to equal their corresponding local protocol port values. • The **LAN1** > **VoIP** > **RTP** > **Port Number Range (NAT) RTP | Port Number Range (NAT)** values are set to equal the corresponding **Port Number Range** values.
Port Restricted Cone NAT	Similar to a **Restricted Cone NAT**, but the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P. SIP packets needs to be mapped. Keep-alives must be sent to all ports that will be the source of a packet for each ITSP host IP address. If this type of NAT/Firewall is detected or manually selected, no warning will be displayed for this type of NAT. Some Port Restricted NAT's have been found to be more symmetric in behavior, creating a separate binding for each opened Port, if this is the case the manager will display a warning `'Communication is not possible unless the STUN server is supported on same IP address as the ITSP'` as part of the manager validation.
Restricted Cone NAT	A restricted cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Unlike a full cone NAT, an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X. SIP packets needs to be mapped. Responses from hosts are restricted to those that a packet has been sent to. So if multiple ITSP hosts are to be supported, a keep alive will need to be sent to each host. If this type of NAT/Firewall is detected or manually selected, no warning will be displayed for this type of NAT.
Static Port Block	Use the RTP Port Number Range specified on the VoIP tab without STUN translation. Those ports must be fixed as open on any NAT firewall involved
Symmetric Firewall	SIP packets are unchanged but ports need to be opened and kept open with keep-alives. • If this type of NAT is detected or manually selected, a warning `'Communication is not possible unless the STUN server is supported on same IP address as the ITSP'` is displayed as part of the manager validation.

Table continues…

Firewall/NAT Type	Description
Symmetric NAT	A symmetric NAT is one where all requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host. SIP Packets need to be mapped but STUN will not provide the correct information unless the IP address on the STUN server is the same as the ITSP Host. • If this type of NAT is detected or manually selected, a warning `'Communication is not possible unless the STUN server is supported on same IP address as the ITSP'` is displayed as part of the manager validation.
Unknown	The type of NAT is unknown or could not be determined.

SBC

These settings are used to provide values to remote extensions that connect to the IP Office through an ASBCE. The values set are passed to the phones using methods that vary depending on the phone type. For example, by altering the values in the auto-generated `46xxsettings.txt` file when requested by a remote phone.

These settings replace the **RW_SB...** *NoUser* source numbers used in pre-R11.1.2.4 systems, which should be removed once replaced with these values.

Field	Description
Public IP Address (IPv4)	Default = Blank The public IPv4 address that routes to the public/external side of the ASBCE. Depending on the customer network, this can be the public IP address of another device such as a firewall that forwards to the SBC.

Table continues…

Field	Description
Public IP Address (IPv6)	Default = Blank As above but using an IPv6 address. Use of an IPv6 address is supported for: • Avaya Workplace Client R3.35 (Android and iOS). • IP Office R11.1.3.1 or higher. • ASBCE 10.1.2 or higher. • The IP Office supports IPv6 addresses in the following formats: - Full address: For example, `2001:0000:040F:0000:0000:0000:805B:001B`. - Replace one series of `:0000:` parts with `::`. For example, `2001:0000:040F::805B:001B`. - Replace any individual `:0000:` parts with `:0:`. For example, `2001:0:040F::805B:001B`. - Remove leading `0` zeros after any `:` colon. For example, `2001:0:40F::805B:1B`. For further information, see the Deploying Remote IP Office SIP Phones with an ASBCE manual.
Private IP Address (IPv4)	Default = Blank The private IPv4 address of the ASBCE.
FQDN	Default = Blank The fully-qualified domain name of the ASBCE. You must set this value. • The IP Office uses this value in the auto-generated `46xxsettings.txt` file requested by remote Avaya Workplace Client extensions. For other remote SIP extensions, the IP Office uses the **SIP Registrar FQDN**. • The customer DNS must resolve this FQDN to an IP address that routes to the IP Office. That is: - For remote extensions, the external IPv4 address of the Avaya SBC or customer firewall that routes to the IP Office. - If supporting remote Avaya Workplace Client extensions using IPv6, the FQDN must resolve to both the external IPv4 and IPv6 addresses of the Avaya SBC or customer firewall that routes to the IP Office.
SBC Registrar public ports	The public ports on which the ASBCE is configured to listen for incoming SIP call. • **UDP** - Default = 5060 • **TCP** - Default = 5056 • **TLS** - Default = 5061

Related links

LAN1 on page 479

LAN2

Navigation: **System Settings** > **System** > **LAN2**

These settings used to configure the system's second LAN interface.

These settings can only be edited offline. Changes to these settings require a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

The fields available for LAN2 are the same as for LAN1 except for the following:

- Avaya supports IPv6 on IP Office LAN1. Avaya also supports IPv6 on LAN2 but only when IPv6 is enabled on LAN1 also.

Field	Description
Firewall	Default = <None> (No firewall) Allows the selection of a system firewall which the IP Office applies to traffic routed from LAN2 to LAN1.

Related links

System on page 451

VoIP

Navigation: **System Settings** > **System** > **VoIP**

These setting set overall controls for the system's support of VoIP connections.

Related links

System on page 451
VoIP on page 501
VoIP Security on page 503
Access Control Lists on page 506

VoIP

Navigation: **System Settings** > **System** > **VoIP** > **VoIP**

This tab is used to set the codecs available for use with all IP lines and extensions and the default order of codec preference.

- Avaya H.323 telephones do not support G.723 and ignore it if selected.
- For IP Office systems with H.323 lines and extensions, one of the G.711 codecs must be selected.
- G.723 and G.729b are not supported by Linux-based IP Office systems.
- The number of channels provided by an IP500 VCM 32 or IP500 VCM 64 card, up to a maximum of 32 or 64 respectively, depends on the actual codecs being used. This also

applies to IP500 VCM 32 V2 and IP500 VCM 64 V2 cards. The following table assumes that all calls using the VCM use the same codec.

Codec	IP500 VCM 32 IP500 VCM 32 V2	IP500 VCM 64 IP500 VCM 64 V2
G.711	32	64
G.729a	30	60
G.723	22	44
G.722	30	60

Paging from an IP device uses the preferred codec of that device. It is the system administrator's responsibility to ensure all the target phones in the paging group support that codec.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Ignore DTMF Mismatch for Phones	Default = Enabled. When enabled, the following settings are visible and configurable: • **Call Management** > **Extensions** > **Edit Extension** > **H323 VoIP** > **Requires DTMF** • **Call Management** > **Extensions** > **Edit Extension** > **SIP VoIP** > **Requires DTMF** When enabled, during media checks, the system ignores DTMF checks if the call is between two VoIP phones and the extension setting **Requires DTMF** is set to **Off**. The two phones can be located on different systems in a Server Edition or SCN deployment.
Allow Direct Media Within NAT Location	Default = Off. When enabled, the system allows direct media between devices that reside behind the same NAT. Devices are behind the same NAT if their public IP addresses are the same. • Direct media may still not be possible if other settings, such as codecs, NAT settings, or security settings do not match. The default behavior is to allow direct media between all types of devices (H323 and SIP remote workers and IP Office Lines behind a NAT). In the case of routers that have H323 or SIP ALG, it can be desirable to allow direct media only between certain categories of devices. This can be configured by adding the NoUser Source Number MEDIA_NAT_DM_INTERNAL. For information, see **Call Management** > **Users** > **Add/Edit Users** > **Source Numbers**.
Disable Direct Media For Simultaneous Clients	Default = Disabled If enabled, the **Allow Direct Media Within NAT Location** settings for virtual extension records is disabled.

Table continues…

Field	Description
RFC2833 Default Payload	Default = 101. Range = 96 - 127. This field specifies the default value for RFC2833 dynamic payload negotiation. Service providers that do not support dynamic payload negotiation may require a fixed value.
OPUS Default Payload	Default = 116. This field specifies the default value and the range to be used for Opus codec. This field is only used for Linux-based systems. **Note:** This field is not avialable on IP500v2, but the **Unknown Codec passthrough** and the **OPUS** settings are available to set individually.
Available Codecs	This list shows the codecs supported by the system and those selected as usable. Those codecs selected in this list are then available for use in other codec lists shown in the configuration settings. For example, the adjacent **Default Selection** list and the individual custom selection list on IP lines and extensions. **Warning:** Removing a codec from this list automatically removes it from the codec lists of any individual lines and extensions that are using it. The supported codecs (in default preference order) are: Opus, G.711 A-Law, G.711 U-Law, G.722, G.729, and G.723.1. The default order for G.711 codecs varies to match the default companding settings of the system. G.723.1 and G.729b are not supported on Linux- based systems.
Default Codec Selection	By default, all IP (H.323 and SIP) lines and extensions added to the system have their **Codec Selection** setting set to **System Default**. That setting matches the codec selections made in this list. The buttons between the two lists can be used to move codecs between the **Unused** and the **Selected** parts of the list and to change the order of the codecs in the selected codecs list.

Related links

VoIP on page 501

VoIP Security

Navigation: **System Settings** > **System** > **VoIP Security**

Use to set system level media security settings. These settings apply to all lines and extensions on which SRTP is supported and which have their **Media Security** settings configured to be **Same as System**. Individual lines and extensions have media security settings that can override system level settings.

Simultaneous SIP extensions that do not have physical extensions in the configuration use the system security settings.

SM lines and all centralized user extensions must have uniform media security settings.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Name	Description
Default Extension Password	Default = Extension password set during initial configuration. This default extension password is automatically assigned to each H.323 and SIP extension entry when they are added to the system configuration. Each extension's password can be changed through the extension's own settings if required. The extension password is used for registration of IP phones with the system. The password must be 9 to 13 digits. Use the 'eye' icon to see the existing default password.
Media Security	Default = Disabled. Secure RTP (SRTP) can be used between IP devices to add additional security. These settings control whether SRTP is used for this system and the settings used for the SRTP. The options are: • **Disabled**: Use RTP. • **Preferred**: Attempt to use SRTP. If SRTP call setup is unsuccessful, fall back to RTP. • **Enforced**: Use SRTP. If SRTP call setup is unsuccessful, the call fails. - For calls using **Dial Emergency**, the IP Office will switch to RTP if SRTP call setup fails. If media security is enabled (**Enforced** or **Preferred**), we recommend that you enable a matching level of security using **System Settings** > **System** > **LAN1** > **VoIP** > **H.323 Signalling over TLS**. The endpoints that support Secure RTP are: • IP Office , SIP and SM lines • Avaya H.323 extensions: 9608, 9611, 9621, 9641 • Avaya SIP extensions: 9608, 9611, 9621 and 9641 (in centralized branch deployments), 1100 Series, 1200 Series, B179, E129, H175, J100 Series, K100 Series (Vantage), Scopia XT series • 3rd Party SIP extensions that support SRTP
Media Security Options	Not displayed if **Media Security** is set to **Disabled**. The options are: • **Encryptions**: Default = RTP This setting allows selection of which parts of a media session should be protected using encryption. The default is to encrypt just the RTP stream (the speech). • **Authentication**: Default = RTP and RTCP This setting allows selection of which parts of the media session should be protected using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Not adjustable. • **Crypto Suites**: Default = `SRTP_AES_CM_128_SHA1_80`. There is also the option to select `SRTP_AES_CM_128_SHA1_32`.

Table continues…

Name	Description
Strict SIPS	Default = Off. This setting is available in Enterprise Branch deployments only. This option provides a system-wide configuration for call restrictions based on SIPS URI. When this option is off, calls are not rejected due to SIPS. A call is sent according to the configuration of the outgoing trunk or line that it is routed to, regardless of the way the call came in, even if the call came in as a SIP invite with SIPS URI and is being sent with a SIP URI onto a non-secure SIP trunk. When this option is on, an incoming SIP invite with SIPS URI if targeted to a SIP trunk (SM line or SIP line) is rejected if the target trunk is not configured with SIPS in the URI Type field. **Note:** • Strict SIPS is not supported with 9600 Series and J100 Series SIP Feature phones.

Calling Number Verification

These settings configure the SIP trunks use of STIR protocols for calling number verification.

For more details, see SIP Calling Number Verification (STIR/SHAKEN) on page 959.

Field	Description
Incoming Calls Handling	Default = **Allow Not Failed** Sets the defaults for which calls are accepted by the system based on the authentication level of the call. This default can be overridden in the individual line configuration. • **Allow All** - Allow all calls regardless of calling number verification. • **Allow Validated** - Only accept verified calls with full or partial attestation. • **Allow Not Failed** - Accept all calls expect those that specifically failed verification. Note this can include calls with no reported verification result.
Validation Presentation	Default = Off If enabled, the system will prefix the caller ID information displayed on phones with a character indicating the result of the call's validation result. This will be: • A tick mark for full verification. • A question mark for partial verification. • A cross for authentication failed. When enabled, the system will also inspect the display information on all received trunk calls to ensure they do not start with these characters in order to avoid spoofing.

Related links

VoIP on page 501

Access Control Lists

Navigation: **System Settings** > **System** > **VoIP**

Name	Description
SIP UA Blacklist	Default = Empty. You can use this list to set SIP User Agent (UA) strings the IP Office will block when the **System** > **LAN1** > **VoIP** > **Allowed SIP User Agents** setting is set to **Block Blacklist Only**. • Not supported on IP500 V2 systems.
SIP UA Whitelist	Default = Empty. You can use this list to set the SIP User Agent (UA) strings the IP Office will allow to register when the **System** > **LAN1** > **VoIP** > **Allowed SIP User Agents** setting is set to **Avaya Clients & Whitelisted** or **Whitelisted Only**. • Not supported on IP500 V2 systems.
Whitelisted Only	The IP Office system will automatically block traffic from an IP address making repeated failed registration attempts. You can use this list to specify IP addresses the IP Office system should not block. • This is useful when there are multiple devices registering from behind the same single public IP address. In such a scenario, there can a higher incidence of failed registrations. • Supported on IP500 V2 systems for IP Office R11.1 FP2 and higher. • Not supported for IPv6 addresses.

Related links

VoIP on page 501

Directory Services

Navigation: **System Settings** > **System** > **Directory Services**

Related links

System on page 451
LDAP on page 506
HTTP on page 510

LDAP

Navigation: **System Settings** > **System** > **Directory Services** > **LDAP**

Additional configuration information

For additional configuration information, see Centralized System Directory on page 734.

Configuration settings

LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network. It can also be used to import directory information.

The IP Office supports both LDAP V2 and LDAP V3:

- **LDAP v2:** This menu (**System Settings** > **System** > **Directory Services** > **LDAP**) supports LDAP v2 direct from the IP Office service.
- **LDAP v3:** The Collaboration service on IP Office R11.1.2 and higher Linux-based IP Office servers supports LDAP v3. For IP500 V2 servers, the Collaboration service is provided by an IP Office Application Server. Using IP Office Web Manager, see **Solution** > **Solution Settings** > **User Synchronization Using LDAP**.

Tip:

- IP Office systems also support the import of directory records from another IP Office using HTTP. That includes using HTTP to import records that the other IP Office has imported using LDAP.

LDAP records can contain several telephone numbers. Each will be treated as a separate directory record when imported into the system directory.

An LDAP directory is organized in a simple "tree" hierarchy consisting of the following levels:

- The "root" directory (the starting place or the source of the tree), which branches out to
- Countries, each of which branches out to
- Organizations, which branch out to
- Organizational units (divisions, departments, and so forth), which branches out to (includes an entry for)
- Individuals (which includes people, files, and shared resources such as printers)

An LDAP directory can be distributed among many servers. Each server can have a replicated version of the total directory that is synchronized periodically. An LDAP server is called a Directory System Agent (DSA). An LDAP server that receives a request from a user takes responsibility for the request, passing it to other DSA's as necessary, but ensuring a single coordinated response for the user.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
LDAP Enabled	Default = Off This option turns LDAP support on or off. If the server being queried is an LDAP V3 server, support for LDAP V2 may need to be enabled on that server. LDAP V3 servers typically support LDAP V2 but do not have it enabled by default.

Table continues…

Field	Description
User Name	Default = Blank Enter the user name to authenticate connection with the LDAP database. To determine the domain-name of a particular Windows user look on the "Account" tab of the user's properties under "Active Directory Users and Computers". Note that this means that the user name required is not necessarily the same as the name of the Active Directory record. There should be a built-in account in Active Directory for anonymous Internet access, with prefix "IUSR_" and suffix server_name. Thus, for example, the user name entered is this field might be: IUSR_CORPSERV@example.com
Password	Default = Blank Enter the password to be used to authenticate connection with the LDAP database. Enter the password that has been configured under Active Directory for the above user. Alternatively, an Active Directory object may be made available for anonymous read access. This is configured on the server as follows. 1. In **Active Directory Users and Computers**, enable **Advanced Features** under the **View** menu. 2. Open the properties of the object to be published and select the **Security** tab. 3. Click **Add** and select **ANONYMOUS LOGON** and click **Add** and then **OK** 4. Click **Advanced** and select **ANONYMOUS LOGON**. 5. Click **View/Edit** and change **Apply to** to **This object and all child objects**. 6. Click **OK** to exit the menus. 7. Once this has been done on the server, any record can be made in the **User Name** field in the **System** configuration form (however, this field cannot be left blank) and the **Password** field left blank. Other non-Active Directory LDAP servers may allow totally anonymous access, in which case neither **User Name** nor **Password** need be configured.
Server IP Address	Default = Blank Enter the IP address of the server storing the database.
Server Port	Default = 389 This setting is used to indicate the listening port on the LDAP server.
Authentication Method	Default = Simple Select the authentication method to be used. The options are: • **Simple**: clear text authentication • **Kerberos**: Not used.

Table continues…

Field	Description
Resync Interval (secs)	Default = 3600 seconds. Range = 60 to 99999 seconds. The frequency at which the system should resynchronize the directory with the server. This value also affects some aspects of the internal operation. The LDAP search inquiry contains a field specifying a time limit for the search operation and this is set to 1/16th of the resync interval. So by default a server should terminate a search request if it has not completed within 225 seconds (3600/16). The client end will terminate the LDAP operation if the TCP connection has been up for more than 1/8th of the resync interval (default 450 seconds). This time is also the interval at which a change in state of the "LDAP Enabled" configuration item is checked.
Search Base **Search Filter**	Default = Blank These fields are used together to refine the extraction of directory records. The **Search Base** specifies the point in the tree to start searching. • The **Search Base** is a distinguished name in string form as defined in RFC1779. The **Search Filter** specifies which objects under the base are of interest. • The **Search Filter** deals with the attributes of the objects found under the **Search Base**. It uses the format defined in RFC2254 except that extensible matching is not supported. • If left blank, the **Search Filter** defaults to `(objectClass=*)` which matches all objects under the **Search Base**. • You must ensure that the whole filter, and each object within the filter, are enclosed within `( )` brackets. The following are some examples applicable to an Active Directory database. • To all user phone numbers in a domain: - **Search Base** - `cn=users,dc=acme,dc=com` - **Search Filter** - `(telephonenumber=*)` • To restrict the search to a particular Organizational Unit (for example an office site) and get cell phone numbers also: - **Search Base** - `ou=holmdel,DC=example,DC=com` - **Search Filter** - `(|(telephonenumber=*)(mobile=*))` • To get the members of distribution list "group1": - **Search Base** - `cn=users,dc=example,dc=com` - **Search Filter** - `(&(memberof=cn=group1,cn=users,dc=example,dc=com)(telephonenumber=*))`

Table continues…

Field	Description
Number Attributes	Default = `telephoneNumber,otherTelephone,homePhone=H,otherHomePhone=H,mobile=M,otherMobile=M` Enter the number attributes the server should return for each record that matches the **Search Base/Search Filter**. • Other Active Directory records are `ipPhone`, `otherIpPhone`, `facsimileTelephoneNumber`, `otherfacsimileTelephone Number`, `pager` or `otherPager`. • The attribute names are not case sensitive. • Other LDAP servers may use different attributes. • The optional `"=string"` sub-fields define how that type of number is tagged in the directory. Thus, for example, a cell phone number would appear in the directory as: `John Birbeck M 7325551234`
Auto Populate MS Teams Data	Default = Enabled When **LDAP Enabled** setting is enabled, the **Auto Populate MS Teams Data** setting auto populates the Microsoft Teams URI obtained by IP Office in **User | Mobility** > **MS Teams URI** and makes the **MS Teams URI** setting read-only.

Related links

Directory Services on page 506

HTTP

Navigation: **System Settings** > **System** > **Directory Services** > **HTTP**

Additional configuration information

For additional configuration information, see Centralized System Directory on page 734.

Configuration settings

The system can use HTTP to import the directory records held by another system. Note that support for HTTP can be disabled. The setting **System Settings** > **System** > **System** > **Avaya HTTP Clients Only** can restrict a system from responding to HTTP requests. The system's **Unsecured Interfaces** security settings also included controls for HTTP access (**HTTP Directory Read** and **HTTP Directory Write**).

For Server Edition, on Secondary Server, Expansion System (L) and Expansion System (V2) systems, the HTTP settings are automatically defaulted to obtain the system directory from the Primary Server.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Directory Type	Default = None (No HTTP import)/IP Office SCN on Server Edition. Set whether HTTP import should be used and the method of importation. The options are: • **None**: Do not use HTTP import. • **IP Office**: Import from the system at the IP address set in the **Source** field. • **IP Office SCN**: Import from a system in a multi-site network. The **Source** field is used to select the **Outgoing Line** ID that matches the H.323 line to the remote system. • **Collaboration Services**: When selected, other non configurable options are hidden or their controls disabled with the enforced setting displayed.
Source	Default = Blank/9999 on Server Edition. The form of this field changes according to the **Directory Type** selection above. For **IP Office** this field requires the IP address of the other system. For **IP Office SCN**, the outgoing group ID of the **IP Office** line to the remote system is used.
List	Default = All. This field sets what types of directory record should be imported. The options are: • **All**: Import the full set of directory records from the remote system. • **Config Only**: Import just directory records that are part of the remote system's configuration. Note that these will be treated as imported records and will not be added to the local systems own configuration records. • **LDAP Only**: Import just directory records that the remote system has obtained as the result of its own LDAP import. This allows LDAP directory records to be relayed from one system to another. • **HTTP Only**: Import just directory records that the remote system has obtained as the result of its own HTTP import. This allows HTTP directory records to be relayed from one system to another.
URI	Default = /system/dir/complete_dir_list?sdial=true This field is for information only and cannot be adjusted. The path shown changes to match the **List** setting above.
Resync Interval (secs)	Default = 3600 seconds. Set how often the system should request an updated import. When a new import is received, all previously imported records are discarded and the newly imported records are processed.
HTTPS Enabled	Default = On. Turns HTTPS support on or off for directory record import.
Port Number	Default = 443. The port used for the Directory import. When **HTTPS Enabled** is set to On, the default value is 443. When **HTTPS Enabled** is set to Off, the default value is 80.

Related links

Directory Services on page 506

Telephony

Navigation: **System Settings** > **System** > **Telephony**

Used to set the default telephony operation of the system. Some settings shown here can be overridden for individual users through their User | Telephony tab. The settings are split into a number of sub-tabs.

Related links

System on page 451
Telephony on page 512
Park and Page on page 521
Tones and Music on page 522
Ring Tones on page 526
SM on page 526
MS Teams on page 527
Call Log on page 528
TUI on page 529

Telephony

Navigation: **System Settings** > **System** > **Telephony**

Additional configuration information

- The **Directory Overrides Barring** setting allows you to control barred numbers. For additional configuration information, see Call Barring on page 821.
- The **Inhibit Off-Switch Forward/Transfer** stops any user from transferring or forwarding calls externally. For additional information, see Off-Switch Transfer Restrictions on page 902.
- For additional information regarding the **Media Connection Preservation** setting, see Media Connection Preservation on page 743.

Configuration settings

Used to configure a wide range of general purpose telephony settings for the whole system.

These settings can be edited online with the exception of **Companding LAW** and **Media Connection Preservation**. These settings must be edited offline and requires a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Analog Extensions

These settings apply only to analog extension ports provided by the system. For Server Edition this field is only available on Expansion System (V2) systems

Field	Description
Default Outside Call Sequence	Default = Normal. See Ring Tones on page 775. This setting is only used with analog extensions. It sets the ringing pattern used for incoming external calls. For details of the ring types see **System Settings** > **System** > **Telephony** > **Ring Tones**. This setting can be overridden by a user's **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Settings** > **Outside Call Sequence** setting. Note that changing the pattern may cause fax and modem device extensions to not recognize and answer calls.
Default Inside Call Sequence	Default = Ring Type 1. See Ring Tones on page 775. This setting is only used with analog extensions. It sets the ringing pattern used for incoming internal calls. For details of the ring types see **System Settings** > **System** > **Telephony** > **Ring Tones**. This setting can be overridden by a user's **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Settings** > **Inside Call Sequence** setting.
Default Ring Back Sequence	Default = Ring Type 2. See Ring Tones on page 775. This setting is only used with analog extensions. It sets the ringing pattern used for ringback calls such as hold return, park return, voicemail ringback, and Ring Back when Free. For details of the ring types see **System Settings** > **System** > **Telephony** > **Ring Tones**. This setting can be overridden by a user's **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Settings** > **Ringback Call Sequence** setting.
Restrict Analog Extension Ringer Voltage	Default = Off. Supported on IP500 V2 systems only. If selected: • The ring voltage on analog extension ports on the system is limited to a maximum of 40V Peak-Peak. • The message waiting indication (MWI) settings for analog extension are limited to **Line Reversal A**, **Line Reversal B** or **None**. • Any analog extension already set to another MWI setting is forced to **Line Reversal A**.

Companding Law

Field	Description
Companding Law	These settings should not normally be changed from their defaults. They should only be used where 4400 Series phones (ULAW) are installed on systems which have A-Law digital trunks. **A-Law or U-Law>** PCM (Pulse Code Modulation) is a method for encoding voice as data. In telephony, two methods of PCM encoding are widely used, A-Law and U-Law (also called Mu-Law or μ-Law). Typically U-Law is used in North America and a few other locations while A-Law is used elsewhere. As well as setting the correct PCM encoding for the region, the A-Law or U-Law setting of a system when it is first started affects a wide range of regional defaults relating to line settings and other values. For IP500 V2 systems, the encoding default is set by the type of Feature Key installed when the system is first started. The cards are either specifically A-Law or U-Law.

Telephony

Field	Description
Dial Delay Time (secs)	Default = 4 (USA/Japan) or 1 (ROW). Range = 1 to 30 seconds. This setting sets the time the system waits following a dialed digit before it starts looking for a short code match. In situations where there are potential short codes matches but not exact match, it also sets the delay following the dialing of a digit before dialing complete is assumed.
Dial Delay Count	Default = 0 digits (USA/Japan) or 4 digits (ROW). Range = 0 to 30 digits. This setting sets the number of digits dialed after which the system starts looking for a short code match regardless of the **Dial Delay Time**.

Table continues…

Field	Description
Default No Answer Time (secs)	Default = 15 seconds. Range = 6 to 99999 seconds. This setting controls the amount of time before an alerting call is considered as unanswered. How the call is treated when this time expires depends on the call type. • **For calls to a user:** • - the call follows the user's **Forward on No Answer** settings if enabled. If not set, the call goes to voicemail if available or else continues to ring. - This timer is also used to control the duration of call forwarding if the forward destination does not answer. - It also controls the duration of ringback call alerting. - For a user, this setting is overridden by the user's **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Settings** > **No Answer Time** setting if different. • For calls to hunt groups: - This setting controls the time before the call is presented to the next available hunt group member. - This setting is overridden by the group's **Call Management** > **Group** > **Add/Edit Group** > **Group** > **Fallback** > **Group No Answer Time** setting if different. If the system includes users who are using Avaya Workplace Client on iOS devices, it is recommended to set the time to at least 20 seconds. You should do this for either the system default, or for the individual users and any hunt groups to which they belong.
Hold Timeout (secs)	Default = US: 120 seconds/ROW: 15 seconds. Range = 0 (Off) to 99999 seconds. This setting controls how long calls remain on hold before recalling to the user who held the call. The user's wrap-up time is also added. Note that the recall only occurs if the user has no other connected call. Recalled calls will continue ringing and do not follow forwards or go to voicemail.
Park Timeout (secs)	Default = 300 seconds. Range 0 (Off) to 99999 seconds. This setting controls how long calls remain parked before recalling to the user who parked the call. Note that the recall only occurs if the user has no other connected call. Recalled calls will continue ringing and do not follow forwards or go to voicemail.
Ring Delay	Default = 5 seconds. Range = 0 to 98 seconds. This setting is used when any of the user's programmed appearance buttons is set to Delayed ringing. Calls received on that button will initially only alert visually. Audible alerting will only occur after the ring delay has expired. This setting can be overridden by a ring delay set for an individual user (**Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Multi-line Options** > **Ring Delay**).

Table continues…

Field	Description
Call Priority Promotion Time (secs)	Default = Disabled. Range = Disabled, 10 to 999 seconds. When calls are queued for a hunt group, higher priority calls are placed ahead of lower priority calls, with calls of the same priority sort by time in queue. External calls are assigned a priority (**1-Low**, **2-Medium** or **3-High**) by the Incoming Call Route that routed the call. Internal calls are assigned a priority of **1-Low**. This option can be used to increase the priority of a call each time it has remained queued for longer than this value. The calls priority is increased by 1 each time until it reaches 3-High. In situations where calls are queued, high priority calls are placed before calls of a lower priority. This has a number of effects: • Mixing calls of different priority is not recommended for destinations where Voicemail Pro is being used to provided queue ETA and queue position messages to callers since those values will no longer be accurate when a higher priority call is placed into the queue. Note also that Voicemail Pro will not allow a value already announced to an existing caller to increase. • If the addition of a higher priority call causes the queue length to exceed the hunt group's Queue Length Limit, the limit is temporarily raised by 1. This means that calls already queued are not rerouted by the addition of a higher priority call into the queue.
Default Currency	Default = Locale specific. This setting is used with ISDN Advice of Charge (AOC) services. Note that changing the currency clears all call costs stored by the system except those already logged through SMDR. The currency is displayed in the system SMDR output.
Default Name Priority	Default = Favor Trunk. For SIP trunks, the caller name displayed on an extension can either be that supplied by the trunk or one obtained by checking for a number match in the extension user's personal directory and the system directory. This setting determines which method is used by default. For each SIP line, this setting can be overridden by the line's own **Name Priority** setting if required. Select one of the following options: • **Favor Trunk**: Display the name provided by the trunk. For example, the trunk may be configured to provide the calling number or the name of the caller. The system should display the caller information as it is provided by the trunk. If the trunk does not provide a name, the system uses the **Favor Directory** method. • **Favor Directory**: Search for a number match in the extension user's personal directory and then in the system directory. The first match is used and overrides the name provided by the SIP line. If no match is found, the name provided by the line, if any, is used.
Media Connection Preservation	Default = Enabled. When enabled, attempts to maintain established calls despite brief network failures. Call handling features are no longer available when a call is in a preserved state. When enabled, Media Connection Preservation applies to SCN links and Avaya H.323 phones that support connection preservation.

Table continues…

Field	Description
Phone Failback	Default = Automatic. Applies to H.323 phones that support resiliency. The options are: • **Automatic** • **Manual** Phones are permitted to failover to the secondary gatekeeper when the IP Office Line link to the primary gatekeeper is down. When set to **Automatic**, if a phone's primary gatekeeper has been up for more than 10 minutes, the system causes the phone to failback if the phone is not in use. If the phone is in use, the system will reattempt failback 10 seconds after the phone ceases to be in use. When set to **Manual**, phones remain in failover until manually restarted or re-registered, after which the phone attempts to fail back. **Note:** Manual failback is not supported on SIP phones.
DSS Status	Default = Off This setting affects Avaya display phones with programmable buttons. It controls whether pressing a DSS key set to another user who has a call ringing will display details of the caller. When off, no caller information is displayed.
Auto Hold	Default = On (Off for the United States locale). Used for users with multiple appearance buttons. When on, if a user presses another appearance button during a call, their current call is placed on hold. When off, if a users presses another appearance button during a call, their current call is disconnected.
Show Account Code	Default = On This setting controls the display and listing of system account codes. • **When on:** When entering account codes through a phone, the account code digits are shown while being dialed. • **When off**: When entering account codes through a phone, the account code digits are replaced by s characters on the display.
Inhibit Off-Switch Forward/Transfer	Default = On When enabled, this setting stops any user from transferring or forwarding calls externally.

Table continues…

Field	Description
Restrict Network Interconnect	Default = Off. When this option is enabled, each trunk is provided with a **Network Type** option that can be configured as either **Public** or **Private**. The system will not allow calls on a public trunk to be connected to a private trunk and vice versa, returning number unobtainable indication instead. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Include location specific information	Default = Off. When set to On, this setting is available in the trunk configuration settings when **Network Type** is set to **Private**. Set to **On** if the PBX on the other end of the trunk is toll compliant.
Drop External Only Impromptu Conference	Default = On. If selected, when the last remaining internal user in a conference exits the conference, the conference is ended, regardless of whether it contains any external callers. If not selected, the conference is automatically ended when the last internal party or trunk that supports reliable disconnect exits the conference. The Inhibit Off-Switch Forward/Transfer option above is no longer applied to conference calls.
Visually Differentiate External Call	Default = Off. This setting is applied to the lamp flashing rate used for bridged appearance and call coverage appearance buttons on 1400, 1600 and 9600 Series phones and on their button modules. When selected, external calls alerting on those buttons will use a slow flash (200ms on/50ms off). If not selected or if the call is internal, normal flashing (500ms on/500ms off) is used.

Table continues…

Field	Description
Unsupervised Analog Trunk Disconnect Handling	Default = Off. When using analog trunks, various methods are used for trunk supervision. That is to detect when the far end of the trunk has disconnected and so disconnect the local end of the call. Depending on the locale, the system uses Disconnect Clear signaling and or Busy Tone Detection. This setting should only be enabled if it is know that the analog trunks do not provide disconnect clear signaling or reliable busy tone. For Server Edition this field is only available on Expansion System (V2) systems. When enabled: • Disconnect Clear signaling detection is disabled. Busy tone detection remains on. • Unsupervised transfers and trunk-to-trunk transfers of analog trunk calls are not allowed. The **Allow Analog Trunk to Trunk Connect** setting on analog trunks (Line | Analog Options) is disabled. • If Voicemail Pro is being used for external call transfers, **Supervised Transfer** actions should be used in call flows rather than **Transfer** actions. • All systems in the network must have this setting set to match each other.
High Quality Conferencing	Default = On. Supports the use of the G.722 codec. IP lines and extensions using G.722 are provided with wide band audio. If **High Quality Conferencing** is enabled, when several wide band audio devices are in the same conference, the system will ensure that the audio between them remains wide band, even if the conference also contains other lines and devices using narrow band audio (analog devices, digital devices and IP devices using codecs other than G.722).
Digital/Analogue Auto Create User	Default = On. (IP500 V2 only. Default = Off for Server Edition/On for others) When enabled, an associated user is created for each digital/analogue extension created. Digital/analogue extension creation occurs on initial start up, reset of configuration, or addition of new digital/analogue expansion units or plug-in modules.
Directory Overrides Barring	Default = On. When enabled, barred numbers are not barred if the dialed number is in the External Directory.

Table continues…

Field	Description
Advertize Callee State To Internal Callers	Default = Off. When enabled, for internal calls, additional status information is communicated to the calling party. Not supported for SIP endpoints except for J100 Series phones (not including the J129). • When calling another internal phone and the called phone is set to Do Not Disturb or on another call, the calling phone displays “Do Not Disturb” or “On Another Call” rather than “Number Busy”. • On 9500 Series, 9600 Series and J100 Series, if a line appearance is programmed on a button on phone A and that line is in use on phone B, then phone A displays the name of the current user of the line along with the line number. • If a line appearance on a phone is in use elsewhere in the system and another extension unsuccessfully attempts to seize that line, the phone displays “In Use:<name>” where <name> is the name of the user currently using the line. This configuration parameter sets the system wide default. Individual users can be configured for this feature using the setting **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Settings** > **Advertize Callee State To Internal Callers**
Internal Ring on Transfer	Default = Off. When enabled, the transfer enquiry calls ring with internal ring tone even if the call that is being transferred is an external call. If the user transferring the call completes the call when the call is ringing, the ring tone played to the target changes to the ring tone appropriate for the call being transferred. This feature is supported on phone series: 1400, 9500, 1600, 9600, and analog phones. This feature is not supported on SIP and H.323 DECT phones.

Login Code Complexity

Defines the requirements for the login code.

Field	Description
Enforcement	Default = On. When on, a user PIN is required.
Minimum Length	Default = 6. Maximum 15 digits. The number of users with login codes less than six digits is displayed below the field in red colored text.

Table continues…

Field	Description
Complexity	Default = On. When on, the following complexity rules are enforced. • The user extension number cannot be used. • A PIN consisting of repeated digits is not allowed (111111). • A PIN consisting of forward or backward sequence are not allowed. Examples: 123456, 654321.

RTCP Collector Configuration

Field	Description
Send RTCP to an RTCP Collector	When the check box is selected, system RTCP reporting is enabled. For IP Office Release 10.0 and higher, in addition to having the individual phones send RTCP call quality reports, the system can also send RTCP reports for calls.
Server Address	This Sets the address of the third-party QoS monitoring application to which the system sends RTCP reports.
UDP Port Number	The destination port. The default for this filed is 5005.
RTCP reporting interval (secs)	This setting sets the time interval at which the system sends RTCP reports.

Related links

Telephony on page 512

Park and Page

Navigation: **System Settings** > **System** > **Telephony** > **Park and Page**

The Park and Page tab allows for simple configuration of the of the short code and the programmable button for the park and page function.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Central Park Range	Default = Blank. Range = nX to nnnnnnnXX The park slot ID range definition, where n is a digit sequence from 1 to 9999999 and X represents a park slot value from 0 to 99. The Central Park Range cannot exceed 9 characters total length. Examples: • 1X defines range 10-19 • 3XX defines range 300-399 • 9876543XX defines range 987654300-987654399

Table continues…

Field	Description
Page Target Group List	Default = Blank. The list of paging group targets that are presented on supported phones if the Page action is requested after the Call Park. On some phones, only the first three groups can be presented as Page options (via the Softkeys on the phone). On phones that support scrolling lists, a larger list of possible Page targets can be presented.

Related links

Telephony on page 512

Tones and Music

Navigation: **System Settings** > **System** > **Telephony** > **Tones and Music**

Additional configuration information

For additional information on configuring hold music, see Music On Hold on page 777.

Configuration settings

Used to configure the various tones and music on hold sources used by the system.

The settings can be edited online except for **Disconnect Tone** and **Busy Tone Detection**. These settings must be edited offline and requires a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Conferencing Tone	Default = Entry & Exit Tones. This settings controls how conference tones are used. The options are: • **Entry & Exit Tones** A single tone is heard when a new party joins a conference and double-tone is heard when a party leaves the conference. • **Repeating Tone** A conference tone is heard every 10 seconds by all conference parties.

Table continues…

Field	Description
Disconnect Tone	Default = Default (Use locale setting). For digital and IP phones, when the system detects that the far end of a call has disconnected, it can make the near end either go idle or play disconnect tone (analog phones always play disconnect tone). By default, the chosen behavior depends on the system locale. Note also that when using disconnect tone, the tone used depends on the system locale. • **Default** Use the system locale default for disconnected calls. See Avaya IP Office Locale Settings. • **On** Play disconnect tone when far end disconnection is detected. • **Off** Go idle when far end disconnection is detected.
Busy Tone Detection	Default = Off. Enables or disables the use of busy tone detection for call clearing. This is a system wide setting.
CLI Type	This field is used to set the CLI detection used for incoming analog trunks. Note that the CLI Type field is shown for locales other than **Customize**. For the **Customize** locale, it is set through the **System Settings** > **System** > **System** form. The options are **DTMF**, **FSK V23** or **FSK BELL202**.
Local Dial Tone	Default = On For all normal operation this setting should be left enabled as it allows the system to provide dial tone to users (essential for MSN working).
Local Busy Tone	Default = Off This setting should only be used when the local exchange gives a busy signal via Q.931 but does not provide busy tone.
Beep on Listen	Default = On This setting controls whether call parties hear a repeating tone when their call is monitored by another party using the Call Listen feature. **Warning:** • Listening to a call without the other parties being aware is subject to local regulations. You must ensure that you have complied with the local regulations. Failure to do so can result in penalties.

Table continues…

Field	Description
GSM Silence Suppression	Default = Off. This setting should only be selected if voice quality problems are experienced with calls to voicemail or while recording calls. When on, the system signals silence by generating silence data packets in periods when the voicemail system is not playing prompts. Note that use of this option may cause some timeout routing options in voicemail to no longer work.
Analog Trunk VAD	Default = Off. Select this option to enable Voice Activity Detection (VAD) for analog trunks terminating on the ATM4U-V2 card. VAD functionality provides a Call Answer signal triggered by voice activity. This signal can be used for: • Mobile Twinning • SMDR • Call Forwarding • Call Display • Mobile Call Control • Transfer Ringing Call • TAPI • Trunk to Trunk Call
Busy Tone Detection	Default = System Frequency (Defined by system locale. See Avaya IP Office Locale Settings.) Allows configuration of the system's busy tone detection settings on lines that do not provide reliable disconnect signaling. In that case, the system will use tone disconnect clearing to disconnect such lines after 6 seconds of continuous tone. • The settings should only be adjusted if advised by Avaya Technical Support. • Changes to this setting require a reboot when the new configuration is sent to the system. • For Server Edition, this field is only available on Expansion System (V2) systems.

Hold Music

This section is used to define the source for the system's music on hold source. You must ensure that any MOH source you use complies with copyright, performing rights and other local and national legal requirements.

Server Edition deployments support centralized music on hold, where the Primary Server streams music to the Secondary Server and all expansion servers.

The WAV file properties must be:

- PCM, 8kHz 16-bit Mono.
- Maximum length: 90 seconds on IP500 V2 systems, 600 seconds on Linux-based systems.

If the file downloaded is in the incorrect format, it will be discarded from memory after the download.

Caution:

Copying files in the incorrect format directly into the `opt/ipoffice/system/primary` directory can disable the music on hold function.

The WAV file used as the system source must be named `HoldMusic.wav`. For WAV files used as alternate sources WAV files:

- Up to 27 IA5 characters with no spaces.
- Any file extension.
- On Linux-base systems, the filename is case sensitive.

Field	Description
System Source	Default = WAV File. Selects the default hold music source. Note that changes to the **System Source** requires a reboot. The options are: **Setting** / **Description** **WAV** — Use the `HoldMusic.wav` file. The IP Office loads the file using TFTP, or you can directly add the file using the embedded file manager. **WAV (restart)** — Identical to WAV except that for each new listener, the file plays from the beginning. • Not supported on IP500 V2 systems. • Cannot be used as a centralized source. **External** — Applicable to IP500 V2 systems. Use the audio source connected to the **Audio** port on the control unit. **Tone** — Use a double beep tone: 425Hz, 02./0.2/0.2/3.4 seconds on/off. • This tone is also used if the system source is set to **WAV File** but the `HoldMusic.wav` file has not been successfully loaded.
Alternate Sources	You can assigned a configured alternate source as the **Hold Music Source** for an **Incoming Call Route** or **Group**, overriding the default use of the system source. For more details, see **Alternate Source** on page 779. Adding and changing a source can be merged, but deleting a source requires a reboot. • **Number**: Automatically assigned by the system. • **Name**: Up to 31 characters. Use this field to associate a name with the alternate source. That name is then used to select the source in the **Hold Music Source** field on **Incoming Call Routes** and **Group** settings. • **Source**: Up to 31 characters. Defines the source for the music on hold.

Related links

Telephony on page 512

Ring Tones

Navigation: **System Settings** > **System** > **Telephony** > **Ring Tones**

Additional configuration information

For additional ring tone configuration information, see Ring Tones. on page 775

Configuration settings

Used to configure distinct ring tones for groups and incoming call routes. Ring tone override features are only supported on 1400 Series, 9500 Series and J100 Series (except J129) phones.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Available Ring Tones	In this table, the **Number**, **Name**, and **Source** values are system supplied. The **Name** value is used to create a ring tone plan.
Ring Tone Plan	Use this table to specify available ring tones. Ring tones in this table can be applied to hunt groups and incoming call routes and by short codes. • **Number**: System supplied. The **Number** can be used in a short code by adding r(x) to the **Telephone Number** field, where x = 1 to 8 and specifies which ring tone plan to use. • **Name**: A descriptive name for where this ring tone is used. For example, the name of a hunt group. Each name in the table must be unique. Once configured in this table, ring tone names can be selected from the **Ring Tone Override** field at: - **Call Management** > **Group** > **Add/Edit Group** > **Group** - **System Settings** > **Incoming Call Route** > **Add/Edit Incoming Call Route** • **Ring Tone**: The list of ring tone names from the **Available Ring Tones** table.

Related links

Telephony on page 512

SM

Navigation: **System Settings** > **System** > **Telephony** > **SM**

Used to configure settings that apply to both SM lines.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Branch Prefix	Default = Blank. Maximum range = 15 digits. This number is used to identify the IP Office system within the Avaya Aura® network. On calls routed via an SM Line, the branch prefix is added as a prefix to the caller's extension number. • The branch prefix of each IP Office system must be unique and must not overlap. For example 85, 861 and 862 are okay, but 86 and 861 overlap. • You can leave the prefix blank. If you do not configure the branch prefix, the IP Office user extensions must be defined with the user's full enterprise extension number.
Local Number Length	Default = Blank (Off). Range = Blank or 3 to 9 in deployments with IP Office users and blank or 3 to 15 in deployments with only centralized users. This field sets the default length for extension numbers for extensions, users, and hunt groups added to the IP Office configuration. Entry of an extension number of a different length will cause an error warning. The number of digits entered in the **Branch Prefix** field plus the value entered in the **Local Number Length** field must not exceed 15 digits. You can leave the **Local Number Length** field blank.
Proactive Monitoring	Default = 60 seconds. Range = 60 seconds to 100000 seconds. The branch IP Office system sends regular `SIP OPTIONS` messages to the SM line in order to check the status of line. This setting controls the frequency of those messages when the SM line is currently in service.
Monitoring Retries	Default = 1. Range = 0 to 5. The number of times the branch IP Office system retries sending an `OPTIONS` request to Session Manager before the SM Line is marked out-of-service.
Reactive Monitoring	Default 60 seconds. Range = 10 to 3600 seconds. The branch IP Office system sends regular `SIP OPTIONS` messages to the SM line in order to check the status of line. This setting controls the frequency of those messages when the SM line is currently out-of-service.
User Shortcode Routing	Default = Rainy day. Set when user dialing should be checked against IP Office user short codes and processing of matches applied: • **Rainy day** - Only check when no SM line connection is available. • **Always** - Always check.

Related links

Telephony on page 512

MS Teams

Navigation: **System Settings** > **System** > **Telephony** > **SM** > **MS Teams**

These settings are applied to an IP Office system configured for MS-Teams direct routing. For installation details, refer to the Deploying MS Teams Direct Routing with IP Office manual.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Auto Populate MS Teams Data	Default = Enabled. When enabled, the user **MS Teams URI** settings cannot be edited. Instead, they are controlled via the system's configured Azure Active Directory connection.

Related links

Telephony on page 512

Call Log

Navigation: **System Settings** > **System** > **Telephony** > **Call Log**

The IP Office stores a centralized call log for each user:

- The user's centralized call log is stored by the IP Office system on which the user is configured. If the user is logged in on another system, new call log records are sent to the user's home IP Office system, but using the time and date on the IP Office system where the user is logged in.
- Each user's centralized call log can contain 30 (IP500 V2) or 60 (Server Edition) call records. Each new call record replaces the oldest previous record when it reaches the limit.
- By default, the centralized call log is displayed on Avaya phones with a fixed **Call Log** or **History** button (1400, 1600, 9500, 9600, J100 Series) and in the one-X Portal, Avaya Workplace Client, and IP Office User Portal applications.
- The centralized call log moves with the user as they log onto different phones and IP Office applications.
- The missed call count is updated per unique caller, not per call.

These settings control the IP Office systems default application of user centralized call logs. Additional user specific settings (**User** > **Telephony** > **Call Log**) can override and change the system settings.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Default Centralized Call Log On	Default = On. • If enabled, Avaya phones with a fixed **Call Log** or **History** button (1400, 1600, 9500, 9600, J100 Series) display the user's centralized call. The use of centralized call logging can be enabled/disabled on a per user basis using the setting **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Log** > **Centralized Call Log**.

Table continues…

Field	Description
Log Missed Calls Answered at Coverage	Default = Off. This setting controls whether the users' centralized call logs should include calls that alert the users but are then answered elsewhere. • Coverage applies for calls that alert the user and are then answered elsewhere. For example by call pickup, call coverage buttons, a coverage group member, bridged appearance button, user button, voicemail, and so on. • Coverage does not apply for calls that do not alert the user and are answered elsewhere. For example, forward unconditional. • If covered by another user, that user will have an answered call in their centralized call log.
Log Missed Hunt Group Calls	Default = Off. This setting controls whether the user centralized call log can include missed hunt group calls. • If disabled, users' centralized call logs only include hunt group calls answered by the user. • If enabled, the IP Office also stores call logs of hunt group calls not answered by anyone, including hunt group calls that go to voicemail. - The IP Office system stores up to 10 call records for each hunt group. When this limit is reached, new call records replace the oldest record. - For each user, within the user call log settings (**Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Log**), you must select which hunt group's missed calls are displayed as part of the user's centralized call log.

Related links

Telephony on page 512

TUI

Navigation: **System Settings** > **System** > **Telephony** > **TUI**

Used to configure system wide telephony user interface (TUI) options for 1400, 1600, 9500, 9600 and J100 Series phones (except the J129).

Use these settings to define the default phone display when feature menus are disabled. Note that for new users, the default phone display options are set to the system default values.

Feature menus can be disabled in one of two ways.

- Set **System Settings** > **System** > **Telephony** > **TUI** > **Features Menu** to **Off**. Set **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **TUI** > **User Setting** to **Same as System**.
- On **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **TUI**, set **User Setting** to **Custom** and set **Features Menu** to **Off**.

Configuration settings

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Phone Type	Variable	Description
1400 1600	Display Name Preference	Defines the default value of the User's Features > Phone User > Phone Screen Settings > Display Name setting. Default = Off When enabled, displays the user name.
9500 9608 9611	Column View Preference	Defines the default value of the User's Features > Phone User > Phone Screen Settings > Display Mode setting. Default = Dual Column view can be Single or Dual.
9621 9641	Quick Touch Panel Lines	Defines the default value of the User's Features > Phone User > Phone Screen Settings > Quick Touch Lines setting. Default = Optimize Sets the Quick Touch Panel number. The options are 1, 2, and Optimize. When set to Optimize: • 9621 = 1 • 9641 = 2

Field	Description
Time Format	Default = Locale Defined. Set the system time format display. The default time format is defined by the **Locale** setting. You can override the default and set the time format to a 12- hour or 24-hour clock.
Features Menu Controls	

Table continues…

Field	Description
Features Menu	Default = On When set to on, you can select to turn individual menus and features on users phone's on or off. The system level settings can be overridden at the individual user settings level if required for particular users. The following feature menus are listed: • **Basic Call Functions:** If selected, users can access menu options for call pickup, park, unpark and transfer to mobile functions. • **Advanced Call Functions:** If selected, users can access the menu options for do not disturb, account code, withhold number and internal auto-answer functions. Note, the **Account Code** menu is only shown if the system has been configured with accounts codes. • **Forwarding**: If selected, users can access the phone's menus for forwarding and follow me functions. • **Hot Desk Functions:** If selected, users can access the menu options for logging in and out. • **Passcode Change:** If selected, users can change their login code (security credentials) through the phone menus.. • **Phone Lock:** If selected, users can access the menu options for locking the phone and for setting it to automatically lock. • **Self Administration:** If selected, users can access the phone's **Self-Administration** menu options. • **Voicemail Controls**: If set, users can access the **Visual Voice** option through the phone's **Features** menu.
SIP Phone Options	
Application for Vantage	Default = Equinox on Vantage Select the application to be used on Avaya Vantage™. The system supports Avaya Vantage™ phones running either Avaya Vantage™ Connect or Avaya Workplace Client applications as the dialer application. This field sets which application is indicated in the auto-generated `K1xxSupgrade.txt` file the system provides to Avaya Vantage™ phones. If a mix of dialer applications is required, a static `K1xxSupgrade.txt` file needs to be used. The options on the interface are: • **Equinox on Vantage**: Select the option to use the Avaya Workplace Client client on Avaya Vantage™ device. • **Vantage Basic/Connect**: Select the option to use the Avaya Vantage™ Connect or Avaya Vantage™ Basic applications on Avaya Vantage™ device. **Note:** This setting is not available for Avaya Vantage™ 3.0 version and above.

Related links

[Telephony](#) on page 512

Contact Center

Navigation: **System Settings** > **System** > **Contact Center**

The Contact Center tab contains the user information required by IP Office to synchronize account information with an Avaya Contact Center Select (ACCS) system. The information is synchronized using the Contact Center Management Application (CCMA). These settings are only used for the deployment of an ACCS system.

This tab is visible on the Server Edition Primary Server and Standard Mode IP500 V2 systems.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Contact Center Application	Default = None. The options are: • Avaya Contact Center Select • Avaya IP Office Contact Center • Integrated Contact Reporter (not supported in IP Office Release 11.0)
Synchronize to this System	Default = Off. When set to On, the CCMA fields below are enabled.
CCMA Address	Default = Blank Address of the Contact Center Management Application system.
CCMA Username	Default = Blank User name on the Contact Center Management Application system.
CCMA Password	Default = Blank Password on the Contact Center Management Application system.

Related links

System on page 451

Avaya Cloud Services

Navigation: **System Settings** > **System** > **Avaya Cloud Services**

The **Avaya Cloud Services** tab contains configuration settings for features that use Avaya Cloud Services. For details, see the IP Office Avaya Workplace Client Installation Notes manual.

- Features that use Avaya Cloud Services are not supported for Avaya Workplace Client when using IPv6.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Profile Name	Default = None This name is used to identify the IP Office in the profile settings written into Avaya Cloud Services if **Enable Settings File URL Sync** is enabled. • Within a multi-site network, the name must be unique.
Enable Avaya Cloud Account	Default = Disabled Enable interoperation between the IP Office and Avaya Cloud Services. • You must also add the **Avaya Spaces API Key** and **Avaya Spaces Key Secret** for the customer domain to the IP Office security settings.

AVAYA CLOUD ACCOUNT CONFIGURATION

Field	Description
Account URL	Ensure that the URL matches the appropriate value below: • IP500 V2 = `accounts-ipo.avayacloud.com` • Linux-based Server = `accounts.avayacloud.com`
Company Domain	Default = Blank The company domain registered and verified with Avaya Cloud Services.

USER SYNCHRONIZATION

Field	Description
Enable user sync	Default = Disabled If enabled, the IP Office system automatically synchronizes user information with Avaya Cloud Services.
Manual user sync	Default = Disabled This option is only available in IP Office Web Manager. • You can use the **Refresh** button to request an manual synchronization. • The **Synchronization Status** field shows the result of the last synchronization.

SETTINGS FILE URL SYNCHRONIZATION

Field	Description
Enable Settings File URL Sync	Default = Disabled Controls whether the IP Office sends its SIP FQDN and **Profile Name** to Avaya Cloud Services. • Avaya Cloud Services uses the information to write a profile for the IP Office containing its profile name and `46xxsettings.txt` file address. The allows Avaya Workplace Client users to connect to the IP Office using their **Unique Identity** email address. • Avaya Cloud Services needs address details for each IP Office that is acting as a SIP registrar. The possible settings are: • **Enable for IP Office current Node** Send settings file information for just the current IP Office system. • **Enable for all IP Office Nodes** Send settings file information for all IP Office systems in the network. • **Disabled** Do not send settings file information from the IP Office.

AVAYA CLOUD AUTHORIZATION

Cloud authorization enables users to login to Avaya Workplace Client using a single-sign on (SSO) account such as their Google, Office 365, or Salesforce account. It also allows initial Avaya Workplace Client registration using the user' email address.

- When using IP Office Web Manager to manage a multi-site network (not SCN), you can use the **Solution** > **Actions** > **Synchronize Single Sign-On configuration** command to synchronize these settings on other servers with those on the primary server.

Field	Description
Enable Avaya Cloud Account Authorization	Default = Disabled Control whether cloud authorization is enabled. • Avaya Cloud Account Authorization requires TLS between the IP Office and the Avaya Workplace Client.
Token Cache Time	Default = 15 minutes. Range = 15 to 60 minutes. The time in minutes that the IP Office caches authorization tokens from Avaya Cloud Services.

Related links

System on page 451

Avaya Push Notification Services

Navigation: **System Settings** > **System** > **Avaya Push Notification Services**

Push notification is used to send Avaya Workplace Client users on Apple iOS devices notification of new calls and voicemail messages. Push notifications also requires Avaya Cloud Services on page 532 to be enabled.

For full details, refer to the IP Office Avaya Workplace Client Installation Notes manual.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Field	Description
Enable Apple Push Notification	Default = Off If enabled, the IP Office system will use push notifications for iOS Avaya Workplace Client users. • Avaya Cloud Account Authorization requires TLS between the IP Office and the Avaya Workplace Client. • When using IP Office Web Manager to manage a multi-site network (not SCN), you can use the following commands to synchronize settings on other servers with the primary server: - **Solution** > **Actions** > **Synchronize APNS configuration** synchronizes the **Enable Apple Push Notification** setting. - **Solution** > **Actions** > **Synchronize APNP System-ID** synchronizes the **System-ID**, **Avaya Spaces API Key** and **Avaya Spaces Key Secret** settings. • The **System-ID** is a hidden value generated by an IP Office when the **Enable Apple Push Notification** setting is enabled.
Avaya Push Notification Provider Address	Default = `pnp.avaya.com` This setting is for information only, not editable. This is the address of the Avaya service to which the IP Office sends push notifications. The service forwards those notifications to the Apple Push Notification service which forwards notifications the iOS devices.
Payload Encryption	Default = On This setting is for information only, not editable.
Push Notification Application Type	Default = `com.avaya.AvayaCommunicator` This setting is for information only, not editable. This is the application string for which push notifications are sent. Avaya Workplace Client still uses the older `com.avaya.AvayaCommunicator` string.

Related links

System on page 451

Remote Operations

Navigation: **System Settings** > **System** > **Remote Operations**

In addition to monitoring the status and alarms of a subscription mode IP Office system, Customer Operations Management (COM) can support a number of additional services for the IP Office system. For details, refer to Using Customer Operations Manager for IP Office Subscription Systems.

Settings	Description
Remote Access	This option supports HTTPS, SFTP, SSH and RDP connections to IP Office servers managed by Customer Operations Management.
Co-located Servers	This option allows **Remote Access** support to extend to other servers on the same network as the IP Office system. That includes connection to UCM modules and standalone IP Office Application servers. This option requires configuration of a TCP tunnel for each connection through the **System** > **Services** > **Remote Support Services** menu.
Remote Upgrade/ Backup	This option supports backup and restoration from IP Office to COM. Enabling the **Remote Upgrade/Backup** setting allows automatic daily backups.
Centralized Management	This option supports remote connections to IP Office servers using IP Office admin tools (System Status Application, SysMonitor and IP Office Web Manager).
Centralized Diagnostics Log	This option supports the uploading and storage of system log files to COM.

Related links

System on page 451

Chapter 35: Time Profiles

System Settings > **Time Profiles**

Time profiles contains time, date and weekly schedule settings. Using those each time profile is currently either ‘true’ or ‘false’. That value is used to change the behavior of other types of record that can be linked to the time profile such as incoming call routes.

For additional configuration information, see:

- Configuring Time Profiles on page 787
- the button action Time Profile on page 1185

Main content pane

The **Time Profiles** main content pane lists provisioned time profiles. The contents of the list depends upon the filter options selected. Click the icons beside a profile to edit or delete.

Bulk delete: You can delete multiple records. Select the check box to the right of each record you want to delete and click **Delete**. You receive a prompt to confirm the deletion.

Click **Add/Edit Time Profile** to add a time profile. When you click **Add/Edit Time Profile**, you are prompted to add to time profile as a common object or on a specific server.

Related links

Add Time Profile on page 537

Add Time Profile

Navigation: **System Settings** > **Time Profiles** > **Add/Edit Time Profile**

Additional configuration information

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 806.

Configuration settings

When configuring a time profile, you must enter the **Name** on the **Time Profile** page and then click **Add/Edit Time Profile Entry** to open the Recurrence pattern window.

For a time profile with multiple records, for example a week pattern and some calendar records, the profile is valid when any entry is valid. For Server Edition, this type of configuration record can be saved as a template and new records created from a template.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

- For systems using record consolidation, you can only add and edit this type of record at the solution level. The record is then automatically copied to each IP Office system in the network.

Field	Description
Name	Range = Up to 15 characters This name is used to select the time profile from within other tabs.
Manual Override	Default = Off. You can manually override a time profile. The override settings allow you to mix timed and manual settings. The options are: • **Active Until Next Timed Inactive**: Use for time profiles with multiple intervals. Select to make the current timed interval active until the next inactive interval. • **Inactive Until Next Timed Active**: Use for time profiles with multiple intervals. Select to make the current active timed interval inactive until the next active interval. • **Latch Active**: Set the time profile to active. Timed inactive periods are overridden and remain active. The setting is retained over a reboot. • **Latch Inactive**: Set the time profile to inactive. Timed active periods are overridden and remain active. The setting is retained over a reboot.
Time Entry List This list shows the current periods during which the time profile is active. Clicking on an existing entry will display the existing settings and allows them to be edited if required. To remove an entry, selecting it and then click on **Remove** or right-click and select **Delete**.	
Recurrence Pattern (Weekly Time Pattern)	When a new time entry is required, click **Add Recurring** and then enter the settings for the entry using the fields displayed. Alternately right-click and select **Add Recurring Time Entry**. This type of entry specific a time period and the days on which it occurs, for example 9:00 - 12:00, Monday to Friday. A time entry cannot span over two days. For example you cannot have a time profile starting at 18:00 and ending 8:00. If this time period is required two Time Entries should be created - one starting at 18:00 and ending 11:59, the other starting at 00:00 and ending 8:00. • **Start Time** The time at which the time period starts. • **End Time** The time at which the time period ends. Note that the endtime is at the end of the minute, for example 11:00 is interpreted as 11:00:59, not 11:00:00. • **Days of Week** The days of the week to which the time period applies.

Table continues…

Field	Description
Recurrence Pattern (Calendar Date)	When a new calendar date entry is required, click **Add Date** and then enter the settings required. Alternately right-click and select **Add Calendar Time Entry**. Calendar records can be set for up to the end of the next calendar year. • **Start Time** The time at which the time period starts. • **End Time** The time at which the time period ends. • **Year** Select either the current year or the next calendar year. • **Date** To select or de-select a particular day, double-click on the date. Selected days are shown with a dark gray background. Click and drag the cursor to select or de-select a range of days.

Related links

Time Profiles on page 537

Chapter 36: Tunnel

Tunneling allows additional security to be applied to IP data traffic. This is useful when sites across an unsecure network such as the public internet. The IP500 V2 system supports two methods of tunneling, L2TP and IPSec. Once a tunnel is created, it can be used as the destination for selected IP traffic in the IP Route table.

- The use of tunnels is only supported on non-Subscription IP Office IP500 V2 systems.

Type	Description
L2TP	Layer 2 Tunneling Protocol PPP (Point to Point Protocol) authentication normally takes place between directly connected routing devices. For example when connecting to the internet, authentication is between the customer router and the internet service provider's equipment. L2TP allows additional authentication to be performed between the routers at each end of the connection regardless of any intermediate network routers. The use of L2TP does not require a license.
IPSec	IPSec allows data between two locations to be secured using various methods of sender authentication and or data encryption. The use of IPSec requires entry of an IPSec Tunneling license into the system at each end.

Related links

L2TP Tunnel on page 540
IP Security Tunnel on page 543

L2TP Tunnel

Layer 2 Tunneling Protocol PPP (Point to Point Protocol) authentication normally takes place between directly connected routing devices. For example when connecting to the internet, authentication is between the customer router and the internet service provider's equipment. L2TP allows additional authentication to be performed between the routers at each end of the connection regardless of any intermediate network routers. The use of L2TP does not require a license.

Related links

Tunnel on page 540
L2PT Tunnel on page 541
L2TP on page 542
L2TP PPP on page 542

L2PT Tunnel

Navigation: **Tunnel | Tunnel (L2TP)**

Configuration settings

These settings are not mergeable. Changes to these settings will require a reboot of the system.

Field	Description
Name	Default = Blank. A unique name for the tunnel. Once the tunnel is created, the name can be selected as a destination in the IP Route table.
Local Configuration The account name and password is used to set the PPP authentication parameters.	
Local Account Name	The local user name used in outgoing authentication.
Local Account Password/ Confirm Password	The local user password. Used during authentication.
Local IP Address	The source IP address to use when originating an L2TP tunnel. By default (un-configured), the system uses the IP address of the interface on which the tunnel is to be established as the source address of tunnel.
Remote Configuration The account name and password is used to set the PPP authentication parameters.	
Remote Account Name	The remote user name that is expected for the authentication of the peer.
Remote Account Password/ Confirm Password	The password for the remote user. Used during authentication.
Remote IP Address	The IP address of the remote L2TP peer or the local VPN line IP address or the WAN IP address.
Minimum Call Time (Mins)	Default = 60 minutes. Range = 1 to 999. The minimum time that the tunnel will remain active.
Forward Multicast Messages	Default = On Allow the tunnel to carry multicast messages when enabled.
Encrypted Password	Default = Off When enabled, the CHAP protocol is used to authenticate the incoming peer.

Related links

L2TP Tunnel on page 540

L2TP

Navigation: **Tunnel | L2TP**

These settings are not mergeable. Changes to these settings will require a reboot of the system.

Field	Description
Shared Secret/ Confirm Password	User setting used for authentication. Must be matched at both ends of the tunnel. This password is separate from the PPP authentication parameters defined on the L2TP|Tunnel tab.
Total Control Retransmission Interval	Default = 0. Range = 0 to 65535. Time delay before retransmission.
Receive Window Size	Default = 4. Range = 0 to 65535. The number of unacknowledged packets allowed.
Sequence numbers on Data Channel	Default = On When on, adds sequence numbers to L2TP packets.
Add checksum on UDP packets	Default = On. When on, uses checksums to verify L2TP packets.
Use Hiding	Default = Off When on, encrypts the tunnel's control channel.

Related links

L2TP Tunnel on page 540

L2TP PPP

Navigation: **Tunnel | PPP (L2TP)**

These settings are not mergeable. Changes to these settings will require a reboot of the system.

Field	Description
CHAP Challenge Interval (secs)	Default = 0 (Disabled). Range = 0 to 99999 seconds. Sets the period between CHAP challenges. Blank or 0 disables repeated challenges.
Header Compression	Default = None Select header compression. Options are: IPHC and/or VJ.
PPP Compression Mode	Default = MPPC Select the compression mode for the tunnel connection. Options are: Disable, StacLZS or MPPC.
Multilink/QoS	Default = Off Enable the use of Multilink protocol (MPPC) on the link.

Table continues…

Field	Description
Incoming traffic does not keep link up	Default = On When enabled, the link is not kept up when the only traffic is incoming traffic.
LCP Echo Timeout (msecs)	Default = 6. Range = 0 to 99999 milliseconds. When a PPP link is established, it is normal for each end to send echo packets to verify that the link is still connected. This field defines the time between LCP echo packets. Four missed responses in a row will cause the link to terminate.

Related links

L2TP Tunnel on page 540

IP Security Tunnel

IPSec allows data between two locations to be secured using various methods of sender authentication and or data encryption. The use of IPSec requires entry of an IPSec Tunneling license into the system at each end.

Related links

Tunnel on page 540
IPSec Main on page 543
Tunnel | IKE Policies (IPSec) on page 544
IPSec Policies on page 545

IPSec Main

Navigation: **Tunnel | Main (IPSec)**

These settings are not mergeable. Changes to these settings will require a reboot of the system.

Field	Description
Name	Default = Blank. A unique name for the tunnel. Once the tunnel is created, the name can be selected as a destination for traffic in the IP Route table.
Local Configuration The IP Address and IP Mask are used in conjunction with each other to configure and set the conditions for this Security Association (SA) with regard to inbound and outbound IP packets.	
IP Address	The IP address or sub-net for the start of the tunnel.
IP Mask	The IP mask for the above address.

Table continues…

Field	Description
Tunnel Endpoint IP Address	The local IP address to be used to establish the SA to the remote peer. If left un-configured, the system will use the IP address of the local interface on which the tunnel is to be configured.
Remote Configuration The IP Address and IP Mask are used in conjunction with each other to configure and set the conditions for this Security Association (SA) with regard to inbound and outbound IP packets.	
IP Address	The IP address or sub-net for the end of the tunnel.
IP Mask	The IP mask for the above address.
Tunnel Endpoint IP Address	The IP address of the peer to which a SA must be established before the specified local and remote addresses can be forwarded.

Related links

IP Security Tunnel on page 543

Tunnel | IKE Policies (IPSec)

Navigation: **Tunnel | IKE Policies (IPSec)**

These settings are not mergeable. Changes to these settings will require a reboot of the system.

Field	Description
Shared Secret/ Confirm Password	The password used for authentication. This must be matched at both ends of the tunnel.
Exchange Type	Default = ID Prot Aggressive provides faster security setup but does not hide the ID's of the communicating devices. **ID Prot** is slower but hides the ID's of the communicating devices.
Encryption	Default = 3DES CBC Select the encryption method used by the tunnel. The option is: • **3DES CBC**
Authentication	Default = SHA The method of password authentication. The option is: • **SHA**
DH Group	Default = Group 1
Life Type	Default = KBytes Sets whether **Life** (below) is measured in seconds or kilobytes.
Life	Range = 0 to 99999999. Determines the period of time or the number of bytes after which the SA key is refreshed or re-calculated.

Related links

IP Security Tunnel on page 543

IPSec Policies

Navigation: **Tunnel | IKE Policies (IPSec)**

These settings are not mergeable. Changes to these settings will require a reboot of the system.

Field	Description
Protocol	Default = ESP The options are: • **ESP** (Encapsulated Security Payload) • **AH** (Authentication Header, no encryption)
Encryption	Default = DES3 Select the encryption method used by the tunnel. The option is: • **DES3**
Authentication	Default = HMAC SHA The method of password authentication. The option is: • **HMAC SHA**
Life Type	Default = KBytes Sets whether Life (below) is measured in seconds or kilobytes.
Life	Determines the period of time or the number of bytes after which the SA key is refreshed or re-calculated.

Related links

IP Security Tunnel on page 543

Chapter 37: User Rights

System Settings > **User Rights**

User rights can be used to override some of the individual settings of some users. Changes to the user rights are then automatically applied to all those users rather than having to individually edit each user.

For additional configuration information, see Configuring User Rights on page 858.

Main content pane

The **User Rights** main content pane lists provisioned user rights. The contents of the list depends on the filter options selected. Click the icons beside a record to edit or delete.

Bulk delete: You can delete multiple records. Select the check box to the right of each record you want to delete and click **Delete**. You receive a prompt to confirm the deletion.

Click **Add/Edit User Right** to open the Add User Rights window where you can provision a user right. When you click **Add/Edit User Right**, you are prompted to specify if the user right will be a common object or specific to a server.

Related links

Add User Right on page 546
User on page 547
Short Codes on page 547
Button Programming on page 548
Telephony on page 548
User Rights Membership on page 552
Voicemail on page 553
Forwarding on page 554

Add User Right

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right**

Related links

User Rights on page 546

User

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **User**

Used to set and lock various user settings.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Description
Name	The name for the user rights . This must be set in order to allow the user rights to be selected within the User Rights drop down list on the User | User tab of individual users.
Application Servers Group	Default = Off. Set to On if the IP Office system is deployed in an IP Office Contact Center solution or an Avaya Contact Center Select solution. Only one user rights record can be configured to be the Application Servers Group. If it is set on any one group then the control is disabled on all other groups.
Locale	Default = Blank Sets and locks the language used for voicemail prompts to the user, assuming the language is available on the voicemail server. On a digital extension it also controls the display language used for messages from the system to the phone. See Avaya IP Office Locale Settings.
Priority	Default = 5, Range 1 (Lowest) to 5 (Highest) Sets and locks the user's priority setting for least cost routing.
Do Not Disturb	Default = Off Sets and locks the user's DND status setting.

Related links

User Rights on page 546

Short Codes

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Short Codes**

Used to set and lock the user's short code set. The tab operates in the same way as the **User | Short Codes** tab. User and User Rights short codes are only applied to numbers dialed by that user. For example they are not applied to calls forwarded via the user.

Warning:

User dialing of emergency numbers must not be blocked. If short codes are edited, the users ability to dial emergency numbers must be tested and maintained.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Short codes can be added and edited using the **Add**, **Remove** and **Edit** buttons. Alternatively you can right-click on the list of existing short code to add and edit short codes.

Related links

User Rights on page 546

Button Programming

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Button Programming**

This tab is used to set and lock the user's programmable button set. When locked, the user cannot use **Admin** or **Admin1** buttons on their phone to override any button set by their user rights.

Buttons not set through the user rights can be set through the user's own settings. When **Apply user rights value** is selected, the tab operates in the same manner as the **User | Button Programming** tab.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Adding Blank Buttons

There are scenarios where users are able to program their own buttons but you may want to force certain buttons to be blank. This can be done through the user's associated **User Rights** as follows:

1. Assign the action **Emulation | Inspect** to the button. This action has no specific function. Enter some spaces as the button label.
2. When pressed by the user, this button will not perform any action. However it cannot be overridden by the user.

Related links

User Rights on page 546

Telephony

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Telephony**

Allows various user telephony settings to be set and locked. These match settings found on the **Call Management** > **Users** > **Add/Edit Users** > **Telephony** tab.

Related links

User Rights on page 546
Call Settings on page 549
Supervisor Settings on page 550
Multi-line Options on page 551
Call Log on page 551

Call Settings

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Telephony** > **Call Settings**

Additional configuration information

For additional information on ring tones, see Ring Tones on page 775.

Configuration settings

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

Field	Description
No Answer Time	Default = Blank (Use system setting). Range = 6 to 99999 seconds. Sets how long a call rings the user before following forwarded on no answer if set or going to voicemail. Leave blank to use the system default setting.
Transfer return Time (secs)	Default = Blank (Off), Range 1 to 99999 seconds. Sets the delay after which any call transferred by the user, which remains unanswered, should return to the user if possible.
Wrap up Time (secs)	Default = 2 seconds, Range 0 to 99999 seconds. Specifies the amount of time after ending one call before another call can ring. You may wish to increase this in a "call center" environment where users may need time to log call details before taking the next call. It is recommended that this option is not set to less than the default of 2 seconds. 0 is used for immediate ringing.
Call waiting on/Enable call waiting	Default = Off For users on phones without appearance buttons, if the user is on a call and a second call arrives for them, an audio tone can be given in the speech path to indicate a waiting call (the call waiting tone varies according to locale). The waiting caller hears ringing rather than receiving busy. There can only be one waiting call, any further calls receive normal busy treatment. If the call waiting is not answered within the no answer time, it follows forward on no answer or goes to voicemail as appropriate. User call waiting is not used for users on phones with multiple call appearance buttons.

Table continues…

Field	Description
Busy on held/ Enable busy on Held	Default = Off If on, when the user has a call on hold, new calls receive busy tone (ringing for incoming analog call) or are diverted to voicemail if enabled, rather than ringing the user. Note this overrides call waiting when the user has a call on hold. Not supported (should be set to off) for users with call appearance buttons.

Related links

Telephony on page 548

Supervisor Settings

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Telephony** > **Supervisor Settings**

These settings relate to user features normally only adjusted by the user's supervisor.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Description
Can Intrude	Default = Off If enabled, the user can perform is allowed to perform a range of action on other user's calls. For example: **Call Intrude**, **Call Listen**, **Call Steal** and **Dial Inclusion**. See Call Intrusion on page 834.
Cannot be Intruded	Default = On If checked, this user's calls cannot be interrupted or acquired by users who have **Can Intrude** enabled. This setting also affects whether other users can use their appearance buttons to bridge into a call to which this user has been the longest present user.
Deny Auto Intercom Calls	Default = Off. When enabled, any automatic intercom calls to the user's extension are automatically turned into normal calls.
Force Login	Default = Off If checked, the user must log in using their **Login Code** to use an extension. For example, if Force Login is ticked for User A and user B has logged into A's phone, after B logs off A must log back. If **Force Login** was not ticked, A would be automatically logged back in.
Force Account Code	Default = Off If checked, the user must enter a valid account code to make an external call.

Table continues…

Field	Description
Inhibit Off-Switch Forward/Transfer	: Default = Off When enabled, this setting stops the user from transferring or forwarding calls externally. Note that all user can be barred from forwarding or transferring calls externally by the **System | Telephony | Telephony | Inhibit Off-Switch Forward/Transfers** setting.
Outgoing Call Bar	Default = Off When set, bars the user from making external calls.
Coverage Group	Default = <None> If a group is selected, the system will not use voicemail to answer the users unanswered calls. Instead the call will continue ringing until either answered or the caller disconnects. For external calls, after the users no answer time, the call is also presented to the users who are members of the selected Coverage Group. For further details refer to Coverage Groups.

Related links

Telephony on page 548

Multi-line Options

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Telephony** > **Multi-line Options**

Additional configuration information

For additional configuration information, see Appearance Button Operation on page 1198.

Configuration settings

Multi-line options are applied to a user's phone when the user is using an Avaya phones which supports appearance buttons (call appearance, line appearance, bridged and call coverage).

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

Field	Description
Individual Coverage Time (secs)	Default = 10 seconds, Range 1 to 99999 seconds. This function sets how long the phone will ring at your extension before also alerting at any call coverage users. This time setting should not be equal to or greater than the No Answer Time.

Related links

Telephony on page 548

Call Log

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Telephony** > **Call Log**

The IP Office stores a centralized call log for each user:

- The user's centralized call log is stored by the IP Office system on which the user is configured. If the user is logged in on another system, new call log records are sent to the user's home IP Office system, but using the time and date on the IP Office system where the user is logged in.
- Each user's centralized call log can contain 30 (IP500 V2) or 60 (Server Edition) call records. Each new call record replaces the oldest previous record when it reaches the limit.
- By default, the centralized call log is displayed on Avaya phones with a fixed **Call Log** or **History** button (1400, 1600, 9500, 9600, J100 Series) and in the one-X Portal, Avaya Workplace Client, and IP Office User Portal applications.
- The centralized call log moves with the user as they log onto different phones and IP Office applications.
- The missed call count is updated per unique caller, not per call.

Field	Description
Centralized Call Log	Default = System Default (On) This setting allows the use of centralized call logging to be enabled or disabled on a per user basis. The default is to match the system setting **System Settings** > **User Rights** > **Add/Edit User Right** > **Telephony** > **Call Log** > **Default Centralized Call Log On**. The other options are **On** or **Off** for the individual user. If off is selected, the call log shown on the users phone is the local call log stored by the phone.
Delete records after (hours:minutes)	Default = 00:00 (Never). If a time period is set, records in the user's call log are automatically deleted after this period.
Groups	Default = System Default (On). This section contains a list of hunt groups on the system. If the system setting **System Settings** > **User Rights** > **Add/Edit User Right** > **Telephony** > **Call Log** > **Log Missed Hunt Group Calls** has been enabled, then missed calls for those groups selected are shown as part of the users call log. The missed calls are any missed calls for the hunt group, not just group calls presented to the user and not answered by them.

Related links

Telephony on page 548

User Rights Membership

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **User Rights Membership**

The tabs display the users associated with the user rights and allows these to be changed.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Description
Members of this User Rights	This tab indicates those users associated with the user rights. If the user has an associated Working hours time profile, their association to the user rights applies only during the periods defined by the time profile. If the user does not have an associated Working hours time profile, they are associated with the user rights at all times.
Members when out of service	This tab indicates those users associated with the user rights outside the time periods defined by their Working hours time profile. The Members when out of service tab is not populated unless there are time profiles available within the configuration.

Related links

User Rights on page 546

Voicemail

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Voicemail**

Display the users associated with the user rights and allows these to be changed.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Description
Voicemail On	Default = On When on, the mailbox is used by the system to answer the user's unanswered calls or calls when the user's extension returns busy. Note that selecting off does not disable use of the user's mailbox. Messages can still be forward to their mailbox and recordings can be placed in it. The mailbox can also still be accessed to collect messages.
Voicemail Ringback	Default = Off When enabled and a new message has been received, the voicemail server calls the user's extension to attempt to deliver the message each time the telephone is put down. Voicemail will not ring the extension more than once every 30 seconds.

Table continues…

Field	Description
DTMF Breakout When a caller is directed to voicemail to leave a message, they can be given the option to be transferred to a different extension. The greeting message needs to be recorded telling the caller the options available. The extension numbers that they can be transferred to are entered in the fields below. These system default values can be set for these numbers and are used unless a different number is set within these user settings. The Park & Page feature is supported when the system voicemail type is configured as **Embedded Voicemail** or **Voicemail Pro**. Park & Page is also supported on systems where Avaya Aura Messaging, Modular Messaging over SIP, or CallPilot (for Enterprise Branch with CS 1000 deployments) is configured as the central voice mail system and the local Embedded Voicemail or Voicemail Pro provides auto attendant operation. The Park & Page feature allows a call to be parked while a page is made to a hunt group or extension. This feature can be configured for Breakout DTMF 0, Breakout DTMF 2, or Breakout DTMF 3.	
Reception/ Breakout (DTMF 0)	The number to which a caller is transferred if they press `0`while listening to the mailbox greeting rather than leaving a message (***0** on Embedded Voicemail in IP Office mode). For voicemail systems set to Intuity emulation mode, the mailbox owner can also access this option when collecting their messages by dialing ***0**. If the mailbox has been reached through a Voicemail Pro call flow containing a **Leave Mail** action, the option provided when **0** is pressed are: • For IP Office mode, the call follows the **Leave Mail** action's **Failure** or **Success** results connections depending on whether the caller pressed **0** before or after the record tone. • For Intuity mode, pressing **0** always follows the **Reception/Breakout (DTMF 0)** setting. When Park & Page is selected for a DTFM breakout, the following drop-down boxes appear: • **Paging Number –** displays a list of hunt groups and users (extensions). Select a hunt group or extension to configure this option. • **Retries –** the range is 0 to 5. The default setting is 0. • **Retry Timeout –** provided in the format M:SS (minute:seconds). The range can be set in 15-second increments. The minimum setting is 15 seconds and the maximum setting is 5 minutes. The default setting is 15 seconds
Breakout (DTMF 2)	The number to which a caller is transferred if they press `2`while listening to the mailbox greeting rather than leaving a message (***2** on Embedded Voicemail in IP Office mode)
Breakout (DTMF 3)	The number to which a caller is transferred if they press `3`while listening to the mailbox greeting rather than leaving a message (***3** on Embedded Voicemail in IP Office mode).

Related links

User Rights on page 546

Forwarding

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Forwarding**

Additional configuration information

For additional configuration information, see the section “DND, Follow Me, and Forwarding” in the chapter **Configure user settings** in Administering Avaya IP Office™ Platform with Web Manager.

For additional configuration information, see DND, Follow Me, and Forwarding on page 862.

Configuration settings

Display the users associated with the user rights and allows these to be changed.

These settings are mergeable.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Description
Block Forwarding	
Enable Block Forwarding	Default = Off. When enabled, call forwarding is blocked. The following actions are blocked: • Follow me • Forward unconditional • Forward on busy • Forward on no answer • Call Coverage • Hot Desking The following actions are not blocked: • Do not disturb • Voicemail • Twinning

Related links

User Rights on page 546

Chapter 38: WAN Port

System Settings > **WAN Port**

Use these menus to configure physical and virtual WAN ports.

Click **Add/Edit WAN Port** to open the Add WAN Port page where you can provision a firewall. When you click **Add/Edit WAN Port**, you are prompted to specify the server where the WAN port will be configured.

- This type of configuration record is not available on subscription mode systems.

Related links

Add WAN Port — Sync PPP on page 556
Add WAN Port — Sync Frame Relay on page 557

Add WAN Port — Sync PPP

Navigation: **System Settings** > **WAN Port** > **Add/Edit WAN Port** > **Sync PPP**

Use these settings to configure a WAN port.

On IP500 V2 systems, these settings configure the leased line connected to the WAN port on the Control Unit. Normally this connection is automatically detected by the control unit. If a WAN Port is not displayed, connect the WAN cable, reboot the Control Unit and receive the configuration. The WAN Port configuration form is now be added.

These settings are not mergeable. Changes to these settings will require a reboot of the system.

Field	Description
Name	The physical ID of the Extension port,. This parameter is not configurable; it is allocated by the system.
Speed	The operational speed of this port. For example for a 128K connection, enter 128000. This should be set to the actual speed of the leased line as this value is used in the calculation of bandwidth utilization. If set incorrectly, additional calls may be made to increase Bandwidth erroneously.

Table continues…

Field	Description
Mode	Default = SyncPPP Select the protocol required. The options are: • **SyncPPP** For a data link. • **SyncFrameRelay** For a link supporting Frame Relay.
RAS Name	If the **Mode** is **SyncPPP**, selects the RAS service to associate with the port. If the **Mode** is **SyncFrameRelay**, the RAS Name is set through the DLCIs tab.

Related links

WAN Port on page 556

Add WAN Port — Sync Frame Relay

Navigation: **System Settings** > **WAN Port** > **Add/Edit WAN Port** > **Sync Frame Relay**

These settings are for Frame Relay configuration.

These settings are not mergeable. Changes to these settings will require a reboot of the system.

Field	Description
Frame Management Type	This must match the management type expected by the network provider. Selecting **AutoLearn** allows the system to automatically determine the management type based on the first few management frames received. If a fixed option is required the following options are supported: • **Q933 AnnexA 0393** • **Ansi AnnexD** • **FRFLMI** • **None**
Frame Learn Mode	This parameter allows the DLCIs that exist on the given WAN port to be provisioned in a number of different ways. • **None** No automatic learning of DLCIs. DLCIs must be entered and configured manually. • **Mgmt** Use LMI to learn what DLCIs are available on this WAN. • **Network** Listen for DLCIs arriving at the network. This presumes that a network provider will only send DLCIs that are configured for this particular WAN port. • **NetworkMgmt** Do both management and network listening to perform DLCI learning and creation.
Max Frame Length	Maximum frame size that is allowed to traverse the frame relay network.

Table continues…

Field	Description
Fragmentation Method	The options are: • **RFC1490** • **RFC1490+FRF12**

DLCIs

DLCIs are created for Frame Relay connections. These settings are not mergeable. Changes to these settings will require a reboot of the system.

Field	Description
Frame Link Type	Default = PPP Data transfer encapsulation method. Set to the same value at both ends of the PVC (Permanent Virtual Channel). The options are: • **None** • **PPP** Using PPP offers features such as out of sequence traffic reception, compression and link level connection management. • **RFC 1490** RFC 1490 encapsulation offers performance and ease of configuration and more inter-working with third party CPE. • **RFC1490 + FRF12** Alternate encapsulation to PPP for VoIP over Frame Relay. When selected all parameters on the Service | PPP tab being used are overridden.
DLCI	Default = 100 This is the Data Link Connection Identifier, a unique number assigned to a PVC end point that has local significance only. Identifies a particular PVC endpoint within a user's physical access channel in a frame relay.
RAS Name	Select the RAS Service you wish to use.
Tc	Default = 10 This is the Time Constant in milliseconds. This is used for measurement of data traffic rates. The Tc used by the system can be shorter than that used by the network provider.
CIR	(Committed Information Rate) Default = 64000 bps This is the Committed Information Rate setting. It is the maximum data rate that the WAN network provider has agreed to transfer. The committed burst size (Bc) can be calculated from the set Tc and CIR as Bc = CIR x Tc. For links carrying VoIP traffic, the Bc should be sufficient to carry a full VoIP packet including all its required headers. See the example below.
EIR	(Excess Information Rate) Default = 0 bps This is the maximum amount of data in excess of the CIR that a frame relay network may attempt to transfer during the given time interval. This traffic is normally marked as De (discard eligible). Delivery of De packets depends on the network provider and is not guaranteed and therefore they are not suitable for UDP and VoIP traffic. The excess burst size (Be) can be calculated as Be = EIR x Tc.

Advanced

These settings are used for Frame Relay connections.

These settings are not mergeable. Changes to these settings will require a reboot of the system.

Field	Description
Address Length	The address length used by the frame relay network. The network provider will indicate if lengths other than two bytes are to be used.
N391	Full Status Polling Counter Polling cycles count used by the CPE and the network provider equipment when bidirectional procedures are in operation. This is a count of the number of link integrity verification polls (T391) that are performed (that is Status Inquiry messages) prior to a Full Status Inquiry message being issued.
N392	Error Threshold Counter Error counter used by both the CPE and network provider equipment. This value is incremented for every LMI error that occurs on the given WAN interface. The DLCIs attached to the given WAN interface are disabled if the number of LMI errors exceeds this value when N393 events have occurred. If the given WAN interface is in an error condition then that error condition is cleared when N392 consecutive clear events occur.
N393	Monitored Events Counter Events counter measure used by both the CPE and network provider equipment. This counter is used to count the total number of management events that have occurred in order to measure error thresholds and clearing thresholds.
T391	Link Integrity Verification Polling Timer The link integrity verification polling timer normally applies to the user equipment and to the network equipment when bidirectional procedures are in operation. It is the time between transmissions of Status Inquiry messages.
T392	Polling Verification Timer The polling verification timer only applies to the user equipment when bidirectional procedures are in operation. It is the timeout value within which to receive a Status Inquiry message from the network in response to transmitting a Status message. If the timeout lapses an error is recorded (N392 incremented).

Related links

WAN Port on page 556

Part 5: The Security Menu

Chapter 39: Security Administration

The security settings for access to an IP Office system are separate from the configuration settings. You can only view and edit the security settings directly from the IP Office. You cannot save the security settings as a file on your PC.

This section provides an overview of the main security settings. For more information, see the Avaya IP Office™ Platform Security Guidelines manual.

You can setup security using the following elements:

- Access control to prevent unauthorized use.
- Encryption to guarantee data remains private.
- Message authentication to ensure that the data has not been tampering with.
- Identity assurance to verify the data source.

Related links

Service Users, Roles, and Rights Groups on page 561
Default Service Users and Rights Groups on page 563
Default Rights Groups on page 564
Access Control on page 566
Encryption on page 567
Message Authentication on page 568
Certificates on page 569
Implementing Security on page 569
SRTP on page 571

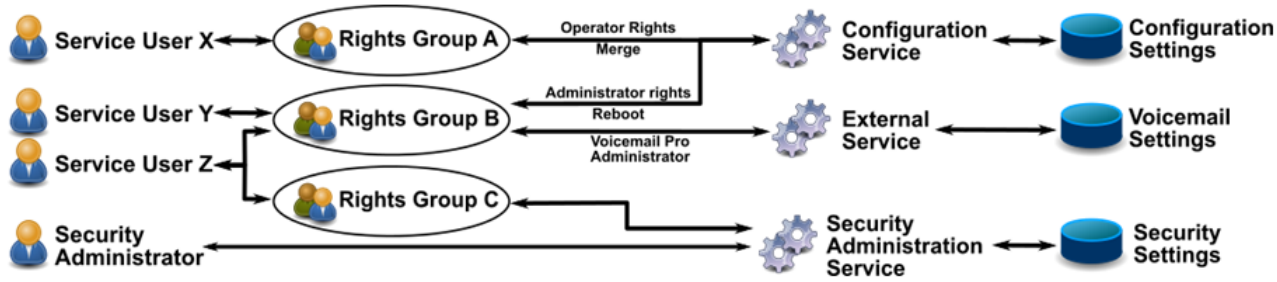
Service Users, Roles, and Rights Groups

The IP Office controls access to its settings and services using **Service Users** and **Rights Groups** stored in its security settings.

- Connecting to the IP Office requires entering a **Service Users** username and password.
- The **Rights Groups** to which the **Service Users** belongs define the permissions that the service user has.

Feature	Description
Security Administrator	The security administrator is a special user that differs from the service users. You can use their username and password to access and edit the security settings. However, the security administrator cannot access any other IP Office services. You cannot remove or disable this account.
Service Users	Each service user has a username, a password, and is a member of one or more **Rights Groups**. The IP Office supports up to 64 service users.
Rights Groups	The **Rights Groups** to which a service user belongs sets their permissions. For example: • Set whether the service user can view and/or edit the configuration settings. • Set which parts of the configuration settings the service user can access. • Set whether the service user can view and/or edit the security settings. • Set whether the service user can change their password. When a service user is a member of more than one rights group, they combine the permissions of each rights group. The IP Office supports up to 32 rights groups.

Example Rights Assignment



In the example above:

- Service user X can read and write the configuration settings. However, they can only edit operator settings, and can only make changes that are mergeable.
- Service user Y can read and write the configuration settings. They can edit all the configuration settings, including making changes that require an IP Office reboot. They can also access the settings of the Voicemail Pro service.
- Service user Z has the same configuration access as service user Y. However, they can also view and edit the security settings.
- The security administrator can only view and edit the security settings.

Changing Administrative Users and Rights Groups

You can use IP Office Manager and IP Office Web Manager to edit service users and rights groups. Before making any changes, you must consider the following:

- IP Office in a multi-site network must have consistent service users and rights groups. IP Office Manager and IP Office Web Manager have synchronization tools to assist in achieving this.

- All changes must follow security best practices. For example, following a password policy and only allowing minimal access rights.

Related links

Security Administration on page 561

Default Service Users and Rights Groups

The following information is applicable for IP Office R11.1FP2.

Security Administrator Account

This is the default security administration account and has all rights to all security settings. You cannot remove or disable this account.

Default Service User Accounts

The following service user accounts are present on the first start-up, and after a security settings reset:

Name	Account Status	Description/Default Rights	Default Rights Group Membership
Administrator	**Enabled**	This service user is the default account for IP Office configuration. Do not remove, disable, or rename this service user.	**Administrator Group** **System Status Group** **Business Partner**
AdjunctServer	**Disabled**	Subscription mode IP Office systems use this service user to enable COM support for an IP Office application server.	**Adjunct Server**
BranchAdmin	**Disabled**	The IP Office uses this service user for IP Office branch systems managed by SMGR.	**SMGR Admin**
BuisnessPartner	**Disabled**	The IP Office uses this service user for configuration access by business partners.	**Business Partner**
COMAdmin	**Enabled**	Subscription mode IP Office systems using this service user for connection to COM.	**COM Admin**
DirectoryService	**Enabled**	The IP Office uses this service user for HTTP directory access.	**Directory Group**
EnhTcpaService	**Enabled**	The IP Office uses this service user for connection with the Avaya one-X® Portal service.	**TCPA Group**
IPDectService	**Disabled**	The IP Office uses this service user for Avaya Wireless DECT system provisioning.	**IPDECT Group**
Maintainer	**Disabled**	The IP Office uses this service user for back up, restore and upgrade connections.	**Maintainer**

Table continues…

Name	Account Status	Description/Default Rights	Default Rights Group Membership
MCMAdmin	**Disabled**	The IP Office uses this service user for connection to Customer Operations Manager.	**MCM Admin**
TURNServer	**Disabled**	The IP Office uses this service user fto support User Portal WebRTC users using TURN.	**TURN Server**

Related links

[Security Administration](#) on page 561

Default Rights Groups

The following information is applicable for IP Office R11.1FP2 SP4 and higher. The following rights groups are present on first start-up and after a security settings reset.

Rights Group Settings

Rights Group	Rights Set		Rights Enabled
Administrator Group	**Configuration**	**IP Office Service Rights**	All
		Manager Operator Rights	**Administrator**
	External	**IP Office Service Rights**	**Media Manager Administrator**, **Reporter Administrator**
System Status Group	**System Status**	**IP Office Service Rights**	All
TCPA Group	**Telephony APIs**	**IP Office Service Rights**	**Enhanced TSPI Access**, **DevLink3**
	HTTP		**Directory Read**, **Directory Write**
IPDECT Group	**HTTP**	**IP Office Service Rights**	**DECT R4 Provisioning**, **Directory Read**
SMGR Admin	**Web Services**	**IP Office Service Rights**	All except **Service Monitor Read**
		Web Manager Rights	All except **Service Change**
Business Partner	**Configuration**	**IP Office Service Rights**	All
	Security Administrator		All
	System Status		All
	Web Services		All except **Service Monitor Read**
			All except **Service Change**

Table continues…

Rights Group	Rights Set		Rights Enabled
	External	**Web Manager Rights**	**Voicemail Pro Administrator**, **one-X Portal Administrator**, **Web Control Administrator**, **WebRTC Gateway Administrator**, **Authentication Module Server Administrator**
Maintainer	**Configuration**	**IP Office Service Rights**	**Read All Configuration**
	System Status		All
	Web Services		**Configuration Read All**, **Backup**, **Restore**, **Upgrade**
	External		**Voicemail Pro Basic**, **one-X Portal Super User**, **Web Control Administrator**, **Web Control Security**
Directory Group	**HTTP**	**IP Office Service Rights**	**Directory Read**, **Directory Write**
COM Admin	**Web Services**	**IP Office Service Rights**	**Security Write Own Password**, **Backup**, **Restore**, **Upgrade**
MCM Admin	**Security Administrator**	**IP Office Service Rights**	**Write Own Service User Password**
	Web Services		**Backup**, **Restore**, **Upgrade**
Adjunct Server	**External**	**IP Office Service Rights**	**Adjunct Server**
TURN Server	**External**	**IP Office Service Rights**	**TURN Server Connection**

Additional Rights Groups for Non-Subscription Systems

The IP Office creates these additional default rights groups on non-subscription mode systems. They have no associated default service users.

Rights Group	Rights Set		Rights Enabled
Manager Group	**Configuration**	**IP Office Service Rights**	All
		Manager Operator Rights	**Manager**
Operator Group	**Configuration**	**IP Office Service Rights**	All
		Manager Operator Rights	**Operator**
Security Admin	**Security Administrator**	**IP Office Service Rights**	All
Backup Admin	**Web Services**	**IP Office Service Rights**	**Backup**, **Restore**

Table continues…

Rights Group	Rights Set		Rights Enabled
	External	**IP Office Service Rights**	**one-X Portal Super User**
Upgrade Admin	**Web Services**	**IP Office Service Rights**	**Upgrade**
System Admin	**Configuration**	**IP Office Service Rights**	**Read All Configuration**, **Write All Configuration**, **Merge Configuration**
	Web Services	**IP Office Service Rights**	**Security Write Own Password**, **Configuration Read All**, **Configuration Write All**
		Web Manager Rights	All except **Service Change**
	External	**IP Office Service Rights**	**Voicemail Pro Standard**, **one-X Portal Administrator**, **WebRTC Gateway Administrator**
Maint Admin	**Web Services**	**IP Office Service Rights**	**Backup**, **Restore**, **Upgrade**
Customer Admin	**Web Services**	**IP Office Service Rights**	**Security Write Own Password**, **Configuration Read All**, **Configuration Write All**, **Backup**, **Restore**, **Upgrade**
		Web Manager Rights	All except **Service Change**
	External	**IP Office Service Rights**	**Voicemail Pro Standard**, **one-X Portal Super User**
Management API Group	**Web Services**	**IP Office Service Rights**	**Management API Read**, **Management API Write**
TURN Server	**External**	**IP Office Service Rights**	**TURN Server Connection**

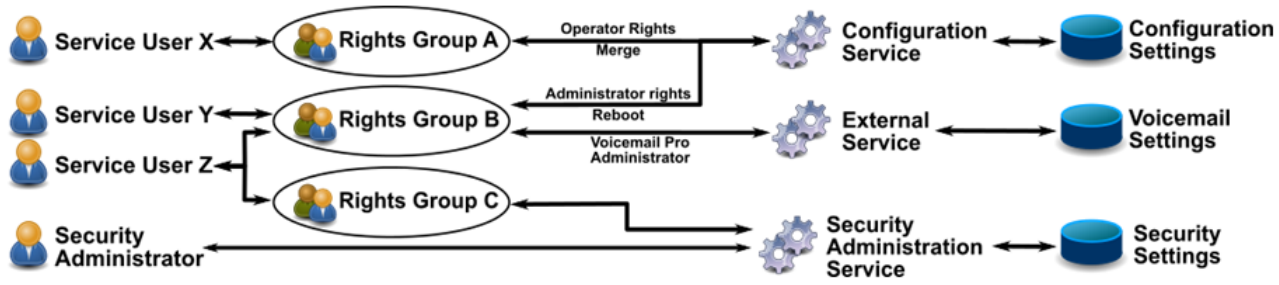
Related links

Security Administration on page 561

Access Control

The IP Office uses service user and rights group settings to control access to the IP Office settings. All connections to an IP Office service require a service user name and password. That service user must be a member of a rights group with permission to access the require service and perform the required actions.

Example Rights Assignment



In the example above:

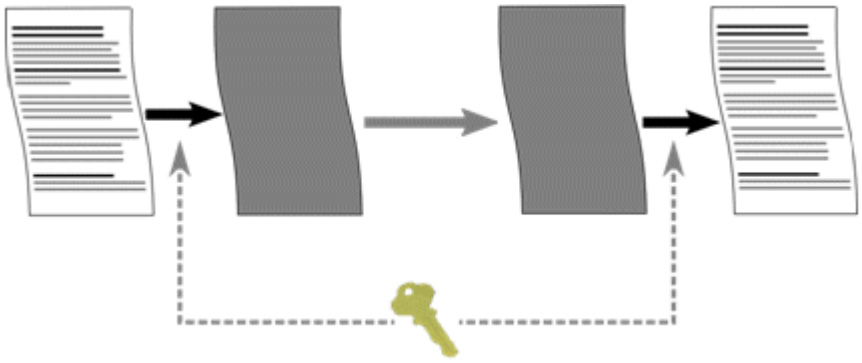
- Service user X can read and write the configuration settings. However, they can only edit operator settings, and can only make changes that are mergeable.
- Service user Y can read and write the configuration settings. They can edit all the configuration settings, including making changes that require an IP Office reboot. They can also access the settings of the Voicemail Pro service.
- Service user Z has the same configuration access as service user Y. However, they can also view and edit the security settings.
- The security administrator can only view and edit the security settings.

Related links

Security Administration on page 561

Encryption

Encryption ensures no one else can read the data sent to and from the IP Office. Encryption is the application of a complex mathematical process at the originating end, and a reverse process at the receiving end. The process at each end uses the same ‘key’ to encrypt and decrypt the data:



The IP Office can encrypt any data sent using a number the following algorithms:

Algorithm	Key size (bits)	Use
DES-40	40	Not supported.
DES-56	56	Not supported.
3DES	112	Low security.
RC4-128	128	Medium security.
AES-128	128	High security.
AES-256	256	High security.

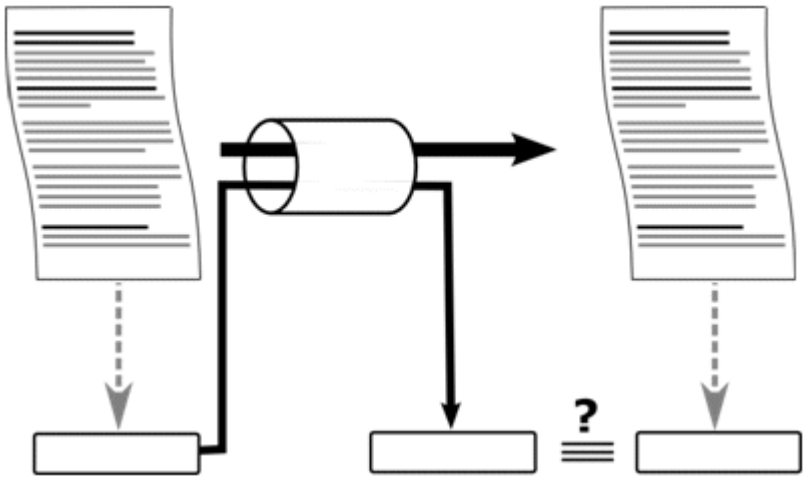
In general, the larger the key size, the more secure the encryption. However, smaller key sizes require less processing. The system supports encryption using the Transport Layer Security (TLS) protocol.

Related links

[Security Administration](#) on page 561

Message Authentication

Message authentication enables detection of any alteration to data to and from IP Office. To support authentication, the originator of the data also sends a signature (called a hash) of the data sent. The receiver can then check that the data and the signature received match.



The IP Office can authenticate data using the following algorithms:

Algorithm	Hash size (bits)	Use
MD5	128	Not recommended.
SHA-1	160	‘Acceptable’ security.
SHA-2	256, 384, 512	‘Strong’ security

In general, the larger the hash size, the more secure the signature. However smaller hash sizes require less processing.

IP Office supports message authentication using the Transport Layer Security (TLS) 1.0, 1.1, and 1.2 protocol.

Related links

Security Administration on page 561

Certificates

Public key cryptography is one of the ways to maintain a trustworthy networking environment. A public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

For more information, see Certificate Management on page 758.

Related links

Security Administration on page 561

Implementing Security

The IP Office has a range of security features. However, for ease of initial IP Office installation the security features are not enabled by default. Therefore, during installation it is necessary to implement the configuration options listed here.

Minimum Security

A minimum-security scenario is one where any individual with the correct service user name and password can access the configuration from any PC using IP Office Manager. Passwords can be simple and never age.

- Change the default passwords of all service users and the security administrator
- Set the system **Security Administration** service security level to **Secure, Low**.
- Leave the system service user **Password Reject Action** set to **Log to Audit Trail**.
- Leave the system **Client Certificate Checks** level set to **None**.
- Leave the system **Minimum Password Complexity** set to **Low**.
- Leave the system **Previous Password Limit** set to 0.
- Leave the system **Password Change Period** set to 0.

- Leave the system **Account Idle Time** set to 0.
- Leave the **Certificate Check Level** to **Low** in the IP Office Manager preferences.

Medium Security

A medium-security scenario uses password complexity restrictions. Passwords cannot be simple and will age.

- Change the default passwords of all service users and the security administrator
- Set the system **Security Administration** service security level to **Secure, Medium**.
- Set the system **Configuration** service security level to **Secure, Medium**.
- Leave the system service user **Password Reject Action** set to **Log to Audit Trail**.
- Leave the system **Client Certificate Checks** level set to **None**.
- Set the system **Minimum Password Complexity** to **Medium**.
- Set the system **Previous Password Limit** to a non-zero value.
- Set the system **Password Change Period** to non-zero value.
- Set the system **Account Idle Time** to a non-zero value.
- Disable all the system **Unsecured Interfaces**.
- Leave the **Certificate Check Level** to **Low** in the IP Office Manager preferences.

Maximum Security

A maximum-security scenario is one where both configuration and security settings are constrained. Certified individuals with the correct service user name and password can access the configuration from specific PC installations of IP Office Manager. Passwords cannot be simple and will age. IP Office Manager can manage specific systems.

- Change the default passwords of all service users and the security administrator
- Set the system **Security Administration** service security level to **Secure, High**.
- Set the system **Configuration** service security level to **Secure, High**.
- Set the system service user **Password Reject Action** to **Log and Disable Account**.
- Set the system **Client Certificate Checks** level to **High**.
- Set the system **Minimum Password Complexity** to **High**.
- Set the system **Minimum Password Length** to greater than 8.
- Set the system **Previous Password Limit** to greater than 5.
- Set the system **Password Change Period** to a non-zero value.
- Set the system **Account Idle Time** to a non-zero value.
- Install 1024-bit+ third-party certificates in all IP Office server certificates, derived from a trusted certificate authority.
- Install the corresponding trusted CA certificate in each of the IP Office Manager PC's Windows certificate stores.
- Install 1024-bit+ third-party certificates in all IP Office Manager Certificate Stores.

- Install the corresponding certificates in all the system Certificate Stores of all permissible Manager entities, and the trusted CA certificate.
- Disable all the system **Unsecured Interfaces**.
- Set the **Manager Certificate Checks** level to **High** in the IP Office Manager preferences.
- Set the certificate offered to the system in the IP Office Manager preferences.

The above essentially locks the IP Office and corresponding IP Office Manager together. Only recognized (by strong certificate) entities can communicate successfully on the service interfaces. All services use strong encryption and message authentication.

The use of intermediate CA certificates can overcome the limit of 6 certificates in each system IP Office certificate store.

Related links

Security Administration on page 561

SRTP

Secure Real-Time Transport Protocol (SRTP) refers to the application of additional encryption and or authentication to VoIP calls (SIP and H.323). The IP Office can apply SRTP to calls between phones, between ends of an IP trunk or in various other combinations.

IP Office supports:

- Individual configuration for RTP and RTCP authentication and encryption.
- HMAC SHA1 as the authentication algorithm.
- AES-CM as the encryption algorithm.
- 80-bit or 32-bit authentication tag.
- Key length of 128-bits.
- Salt length of 112-bits.

You can configure the use of SRTP at the system level. The options are **Best Effort** or **Enforced**. The recommended setting is **Best Effort**. In that scenario, the IP Office uses SRTP if supported by the other end. When using **Enforced**, the IP Office does not allow the call if the other end does not support SRTP.

You can set different SRTP settings for individual trunks and extensions if necessary. The IP Office supports SRTP on SIP Lines, SM Lines, and IP Office Lines.

Encrypted RTCP

The IP Office supports unencrypted RTCP by default. You can configure encrypted RTCP when required.

For SRTP calls where one end is using encrypted RTCP and the other is unencrypted, the call cannot use direct media. Instead, the IP Office provides SRTP relay for the call.

Authentication

The IP Office supports applying authentication to the voice (RTP) and or control signal (RTCP) parts of a call. The IP Office applies authentication after applying encryption. That allows authentication at the remote end before needing to decrypt.

- For the initial exchange of authentication keys during call setup, the IP Office uses SDESC for SIP calls and H235.8 for H.323 calls.
- The IP Office only supports SRTP when using an addition method such as TLS or a VPN tunnel to establish a secure data path before call setup.
- A replay attack is when someone intercepts packets and then attempts to use them to for a denial-of-service or to gain unauthorized access. Replay protection records the sequence of packets received. All RTP and RTCP packets in the call stream have a sequential index number. However, the packets can arrive in non- sequential order.

  The IP Office protects against replay attacks by using a moving replay window containing the index numbers of the last 64-authenticated packets received or expected. Using this

  - The IP Office only accepts packets that have an index ahead of or inside the replay window.

    The IP Office rejects previously received packets.
- Rekeying is the sending of new authentication keys at intervals during a secure call. The IP Office does not support rekeying, it sends authentication keys at the start of the call.

Emergency Calls

The IP Office allows emergency calls from an extension regardless of the SRTP requirements and support.

SRTP Indication

SRTP call indication depends on the model of phone. The System Status Application and SysMonitor applications can display details of SRTP calls.

Related links

Security Administration on page 561

Chapter 40: Security Settings

Navigation: Security > Security Settings

This section covers the system security settings available to service users which administrator access to view and manage those settings.

Related links

[General](#) on page 573
[System](#) on page 577
[Services](#) on page 581
[Rights Groups](#) on page 583
[Service Users](#) on page 589
[Certificates](#) on page 590

General

Security > Security Settings > General

Security Administrator

The security administrator is a special account that cannot be deleted or disabled. It can be used to access the system's security settings but cannot access the system's configuration settings.

Field	Description
Unique Security Administrator	Default = Off This setting is no longer used. It is greyed out and set to off, meaning that permission to access ad change security settings can also be assigned to other service user accounts through their rights groups memberships.
Name	Default = 'security'. Range = 6 to 31 characters. The name for the security administrator.
Change Password	Range = 9 to 31 characters. The password for the security administrator. In order to change the security administrator password, the current password must be known. The user's original password is set during the initial configuration of the system.

Table continues…

Field	Description
Minimum Password Complexity	Default = Medium. The password complexity requirements. The options are: • **Low** - Any password characters may be used without constraint. Password must not contain your user name. • **Medium** - The password must include characters from at least 2 of the character sets listed below. For example a mix of lower case and upper case. In addition, 3 or more consecutive identical characters of any type is not allowed. - Lower case alphabetic characters. - Upper case alphabetical character. - Numeric characters. - Non-alphanumeric characters, for example # or *. • **High** - As per medium but requiring characters from at least of the 3 character sets above.
Previous Password Limit (Entries)	Default = 24. Range = 0 (Off) to 24 records. The number of previous password to check for duplicates against when changing the password. When set to **0**, no checking of previous passwords takes place. This setting is active for attempted password changes on both Security Manager and the system.

Phone Registration

Field	Description
Block Default IP Phone Passcodes	Default = On If selected, existing IP phone registrations with default passcodes are not allowed in the system. Administrators must type in passwords for registering the existing phones. If not checked, existing IP phone registrations with default passcodes are allowed for registration with the system. Allowing existing phones to register with default passcodes pose a security risk as outsiders can access the system using those passcodes.

Service User Details

These settings control service user names and password/account policies. This setting is active for attempted password changes on all administration interfaces.

Field	Description
Minimum Name Length	Default = 6, Range 1 to 31 characters. This field sets the minimum name length for service user names.
Minimum Password Length	Default = 9, Range 1 to 31 characters. This field sets the minimum password length for service user passwords.
Password Reject Limits (Attempts)	Default = 3, Range 0 (Off) to 255. Sets how many times an invalid name or password is allowed within a 10 minute period before the **Password Reject Action** is performed.

Table continues…

Field	Description
Password Reject Action	Default = Log and Temporary Disable. The action performed when a user reaches the **Password Reject Limit**. The options are: • **No Action** • **Log to Audit Trail** - Creates a record in the system's audit trail indicating the service user account name and time of last failure. • **Log and Disable** - Create an audit trail record and disables the service user account. The account can only be re-enabled through the service user settings. • **Log and Temporary Disable** - Create an audit trail record and temporarily disables the service user account for 60 seconds.
Minimum Password Complexity	Default = Medium. The password complexity requirements. The options are: • **Low** - Any password characters may be used without constraint. Password must not contain your user name. • **Medium** - The password must include characters from at least 2 of the character sets listed below. For example a mix of lower case and upper case. In addition, 3 or more consecutive identical characters of any type is not allowed. - Lower case alphabetic characters. - Upper case alphabetical character. - Numeric characters. - Non-alphanumeric characters, for example # or *. • **High** - As per medium but requiring characters from at least of the 3 character sets above.
Previous Password Limit (Entries)	Default = 24. Range = 0 (Off) to 24 records. The number of previous password to check for duplicates against when changing the password.
Account Password Change Period (days)	Default = 0 (Off). Range 0 to 999 days. Sets how many days a password is valid following a password change. Note that the user must be a member of a rights group that has the option **Write own service user password** enabled. • Whenever this setting is changed, the system recalculates all existing service user password timers. • If this timer expires, the service user account is disabled. The account can only be re-enabled through the service user settings. • To prompt the user a number of days before the account is locked, set a **Expiry Reminder Time (days)** (see below).

Table continues…

Field	Description
Account Idle Time (days)	Default = 0 (Off). Range 0 to 999 days. Sets how many days a service user account can be inactive before it becomes disabled. The idle timer is reset whenever a service user successfully logs in. • If this timer expires, the service user account is disabled. The account can only be re-enabled through the service user settings. • Whenever this setting is changed and the OK button is clicked, the system recalculates all existing service user idle timers.
Expiry Reminder Time (days)	Default = 10. Range 0 (Off) to 999 days. Sets the period before password or account expiry during which a reminder indication is shown when the service user logs in. Reminders are sent, for password expiry due to the **Account Password Change Period (days)** (above) or due to the individual service user's **Account Expiry** date – whichever is the sooner. Currently Manager displays reminders but System Status does not.

IP Office User Details

These settings control IP Office user password/account policies.

Field	Description
Password Enforcement	Default = On. When enabled, password settings are enforced. When disabled, password requirements are not enforced and the remaining settings are not editable
Minimum Password Length	Default = 9, Range 1 to 31 characters. This field sets the minimum password length for user passwords
Minimum Password Complexity	Default = Medium. The password complexity requirements. The options are: • **Low** - Any password characters may be used without constraint. Password must not contain your user name. • **Medium** - The password must include characters from at least 2 of the character sets listed below. For example a mix of lower case and upper case. In addition, 3 or more consecutive identical characters of any type is not allowed. - Lower case alphabetic characters. - Upper case alphabetical character. - Numeric characters. - Non-alphanumeric characters, for example # or *. • **High** - As per medium but requiring characters from at least of the 3 character sets above.

Table continues…

Field	Description
Password Reject Limits (Attempts)	Default = 5, Range 0 (Off) to 255 failures. Sets how many times an invalid name or password is allowed within a 10 minute period before the Password Reject Action is performed.
Password Reject Action	Default = Log and Temporary Disable. The action performed when a user reaches the **Password Reject Limits (Attempts)**. The options are: • **No Action** • **Log to Audit Trail** - Creates a record indicating the user account name and time of last failure. • **Log and Disable** - Creates an audit trail record and additionally permanently disables the user account. The account can be enabled using the **Account Status** field on the **User** > **User** page. • **Log and Temporary Disable** - Creates an audit trail record and additionally temporarily disables the user account for 60 seconds.

Related links

Security Settings on page 573

System

Navigation: Security > **Security Settings** > **System**

Related links

Security Settings on page 573
System Details on page 577
Unsecured Interfaces on page 579

System Details

Navigation: Security > **Security Settings** > **System** > **System Details**

Base Configuration

Field	Description
Services Base TCP Port	Default = 50804. Range = 49152 to 65526. This is the base TCP port for services provided by the IP Office. It sets the ports on which the IP Office listens for requests to access those services, using its LAN1 IP address. Each service uses a port offset from the base port value. • If this value is changed from its default, the IP Office Manager application must be set value through its **File** > **Preferences** > **Preferences** > **Services Base TCP Port** setting. • For information on IP Office port used, see the Using IP Office System Monitor manual.
Maximum Service Users	Default = 64. This is a fixed value for information only. The maximum number of service users that you can configure in the IP Office system's security settings
Maximum Rights Groups	Default = 32. This is a fixed value for information only. The maximum number of rights groups that you can configure in the IP Office system's security settings.

System Discovery

System discovery is the processes used by applications to locate and list available systems. If required, you can disable the IP Office from responding to this process. If you do that, access to the IP Office requires its specific IP address.

Field	Description
TCP Discovery Active	Default = On. If enabled, the IP Office responds to TCP discovery requests.
UDP Discovery Active	Default = On. If enabled, the IP Office responds to UDP discovery those requests.

Security

These settings cover the per-system security aspects, primarily TLS settings.

Field	Description
Security Session ID Cache	Default = 10 hours, Range 0 to 100 hours. This sets how long the IP Office system retains TLS session IDs. If retained, the session ID may be used to quickly restart TLS communications between the system and a re-connecting application. When set to **0**, no caching takes place and each TLS connection is renegotiated.
HTTP Challenge Timeout (sec)	Default = 10. For HTTP/HTTPS connection attempts, this field sets the timeout for connection validation responses.

Table continues…

Field	Description
RFC2617 Session Cache (mins)	Default = 10. For HTTP/HTTPS sessions, this field sets the duration for successful logins as per RFC2617.
Minimum Protocol Version	Default = TLS 1.2 This sets the minimum TLS protocol version for TLS connections.

HTTP Ports

These settings set the ports for web-based configuration access to the system.

Field	Description
HTTP Port	Default = 80.
HTTPS Port	Default = 443.
Web Services Port	Default =8443.

Web Socket Proxy

These settings are applicable to WebSocket communication over IP Office lines.

Field	Description
Enabled	Default = On. • When enabled, IP Office Web Manager uses the proxy server to communicate between the Server Edition Primary server and other IP Office nodes. • When disabled, the WebSocket proxy is disabled. All IP Office line WebSocket communication is closed with `404 NotFound`.
Enforce Secure	Default = On. • When enabled, all proxy communication over IP Office line Websocket uses HTTPS. • When disabled, all HTTPS IP Office line Websocket communication is closed with `403 Forbidden`.

Avaya Spaces Configuration Details

Field	Description
Avaya Spaces API Key	The API key and key secret used for connection between the IP Office and Avaya Cloud Services. For further details, see the IP Office Avaya Workplace Client Installation Notes
Avaya Spaces Key Secret	

Related links

System on page 577

Unsecured Interfaces

Navigation: Security > Security Settings > System > Unsecured Interfaces

These features relate to applications that access the system configuration settings using older security methods.

Field	Description
System Password	Range = 0 to 31 characters. The system password is for the following: • IP Office Manager access to upgrade IP Office IP500 V2 systems. • UDP/TCP access by SysMonitor if the **Monitor Password** password is blank.
Voicemail Password	Default = Blank. Range = exactly 31 characters. For IP Office 11.1 FP1 and higher versions, the password for voicemail connection is enforced to 31 characters. • This password is also set through the Voicemail Pro client and Web Manager application. • When no password is set, an auto generated password is automatically set on both Voicemail Pro client and Web Manager systems.
Monitor Password	Default = Blank. Range = 0 to 31 characters. This password is used by SysMonitor for UDP and TCP access. If blank, then SysMonitor uses the **System Password**. If changing this password with no previous password set, enter the system password as the old password.
Use Service User Credentials	Default = Off. If enabled, SysMonitor access using UDP or TCP, uses service user names and passwords rather than the **Monitor Password**. The service user must also be a member of a rights group with **System Status** > **System Monitor - Access** enabled.

Application Controls

These check boxes control which actions the system will support for legacy applications. Different combinations are used by the different applications. A summary of the applications affected by changes is listed in the **Application Support** list.

- For Linux-based IP Office servers, some ports, such as port 69 and 80, are also controlled by the **Solution** > ☰ > **Platform View** > **Settings** > **System** > **Firewall Settings**.

Field	Description
TFTP Server	Default = On.
TFTP Directory Read	Default = Off. Used by Avaya Wireless DECT for IP Office contacts if using an AIWS.
TFTP Voicemail	Default = Off.
Program Code	Default = On. Controls use of the upgrade wizard from within IP Office Manager.

Table continues…

Field	Description
DevLink	Default = On. Control for DevLink applications, including UDP, TCP and HTTP access by SysMonitor.
TAPI/DevLink3	Default = Off. Controls support for connections from TAPI and DevLink3 applications.
HTTP Directory Read	Default = On. Allows system directory accessed using HTTP rather than HTTPS.
HTTP Directory Write	Default = On. Allow HTTP rather than HTTPS to import temporary directory records into the system directory.

Application Support

This panel is shown for information only. It indicates the effect on various applications of the Application Controls selections.

Related links

System on page 577

Services

Navigation: Security > Security Settings > System Services

This tab shows details of the services that the system runs to which service users can communicate.

Field	Description
Name	The name of the service. This is a fixed value for information only.
Host System	The IP Office system name.
Service Port	This is the port on which the IP Office system listens for attempts to access the service. The routing of traffic to this port must be enabled on firewalls and network devices between the service users and the IP Office system. The base port (TCP or HTTP) for each service is offset by a fixed amount from the ports set in System Settings. For information on port usage, see the *IP Office Port Matrix* document on the Avaya support site.

Table continues…

Field	Description
Service Security Level	Sets the minimum security level the service supports. • If the IP Office system does not already have an `X509` security certificate, selecting a setting other than **Unsecure Only** will cause the IP Office system to stop responding for up to a minute whilst it generates a self-signed security certificate. The options are: • **Unsecure Only** - This option allows only unsecured access to the service. The service's secure TCP port, if any, is disabled. This or disabled are the only options supported for the System Status Interface and Enhanced TSPI services. • **Unsecure + Secure** This option allows both unsecured and secure (Low) access. In addition, TLS connections are accepted without encryption, just authentication. • **Secure Low** - This option allows secure access to the service using TLS and weak (for example `DES_40+MD5`) encryption and authentication or higher. • **Secure Medium** - This option allows secure access to the service using TLS and moderate (for example `SHA-256`) encryption and authentication or higher. • **Secure High** - This option allows secure access to the service using TLS and strong encryption (for example `SHA-256`) and authentication, or higher. - Only supported by Linux-based IP Office systems. - A certificate is required from the client. For IP Office Manager, the **Certificates** > **Received certificate checks (Management interfaces)** setting sets the certificate checks it uses. • **Disabled** - This option is only available for the System Status Interface and Enhanced TSPI services. If selected, access to the service is disabled. For details of the ciphers supported by **Secure Medium** and **Secure High**, see the Avaya IP Office™ Platform Security Guidelines manual.
Service Access Source	Used for the **Configuration** service. Sets the supported modes for IP Office Manager access to the IP Officesystem: • **Server Edition Manager** - If selected, the IP Office system can only be configured using IP Office Manager in its Server Edition mode. This is the default for Server Edition systems. - Opening the configuration of a Server Edition system in IP Office Manager running in any mode other than Server Edition mode should be avoided unless absolutely necessary for system recovery. Even in that case, IP Office Manager will not allow renumbering, changes to the voicemail type, and changes to H.323 lines. • **Avaya Aura System Manager** - If selected, the IP Office system can only be configured using SMGR in Branch Mode. This is the default for centrally managed systems. • **Unrestricted** - The IP Office system can be configured using IP Office Manager in its normal simplified and advanced view modes.

Default Settings

Name	Service Port	Service Security Level	Service Access Source
Configuration	50805	**Secure Medium**	**Unrestricted**
Security Admin	50813	**Secure Medium**	–
System Status Interface	50809	**Secure Medium**	–
Enhanced TSPI Access	50814	**Secure Medium**	–
HTTP	80, 443	**Secure Medium**	–
Web Services	8443	**Secure Medium**	–
External	50821	**Disabled**	–

Related links

Security Settings on page 573

Rights Groups

Navigation: Security > Security Settings > Rights Groups

A rights group is a set of permissions to access various features and services. The rights groups to which a service user belongs sets what that service user can do. If the service user is a member of several rights groups, they gain the combined permissions of both rights groups.

Related links

Security Settings on page 573
Group Details on page 583
Configuration on page 584
Security Administrator on page 585
System Status on page 586
Telephony APIs on page 586
Web Services on page 586
External on page 588
HTTP on page 589

Group Details

This tab sets the name of the Rights Group.

Field	Description
Name	Range = Up to 31 characters The name for the Rights Group should be unique. The maximum number of rights groups is 32.

Related links

Rights Groups on page 583

Configuration

This tab sets the configuration settings access for service user's who are members of this Rights Group.

IP Office Service Rights

Field	
Read All Configuration	If selected, rights group members can read the system configuration.
Write All Configuration	If selected, rights group members can make changes to the system configuration.
Merge Configuration	If selected, rights group members can save configuration changes using a merge.
Default Configuration	If selected, rights group members can default the system configuration.
Reboot/Shutdown Immediately	If selected rights group members can reboot and shutdown the system.
Reboot When Free	If selected, rights group members can select reboot when free when rebooting the system.
Reboot At Time Of Day	If selected, rights group members can select reboot at a specific time when rebooting the system.

Manager Operator Rights

This setting controls what types of configuration records Manager will allow members of the Rights Group to viewed and what actions they can perform with those types of records. The **Administrator** and **Manager** rights group members are also able to access embedded file management.

Role	Actions	Configuration Record Types
Administrator	All	View, edit create and delete all configuration records.
Manager	View	View all except WAN Port.
	Edit	Extension, User, Hunt Group, Short Code, Service, RAS, Incoming Call Route, Directory, Time Profile, Firewall Profile, IP Route, Least Cost Route, Account Code, ARS.
	New	
	Delete	As edit except Short Code.
Operator	View	View all except WAN Port.
	Edit	Extension, User, Hunt Group, Short Code, Service, RAS, Incoming Call Route, Time Profile, Firewall Profile, IP Route, Least Cost Route, Account Code, License, ARS.
	New	None.

Table continues…

Role	Actions	Configuration Record Types
	Delete	Delete Incoming Call Route and Directory.
User & Group Edit	View	User and Hunt Group records only.
	Edit	
	New	None
	Delete	
User & Group Administrator	All	User and Hunt Group records only.
Directory & Account Administrator	All	Directory and Account Code records only.
Time & Attendant Administrator	All	Time Profile and Auto Attendant records only.
ICR & User Rights Administrator	All	Incoming Call Route and User Rights records only.
Read All Configuration	View	View all configuration records.
	Edit	None.
	New	
	Delete	

Related links

Rights Groups on page 583

Security Administrator

This tab sets the security settings access for Service user's who are members of this Rights Group. These settings are ignored and greyed out if a Unique Security Administrator has been enabled in General Settings.

Field	Description
Read All Security Settings	Members of the Rights Group can view the system's security settings.
Write All Security Settings	Members of the Rights Group can edit and return changes to the system's security settings.
Reset All Security Settings	If selected, members of the Rights Group can reset the security settings to default values.
Write Own Service User Password	If selected, members of the Rights Group can change their own password when requested to do so by the system. That request may be the result of the **Force new password** or **Account Password Change Period (days)** settings. The new password change is requested automatically at login time.

Related links

Rights Groups on page 583

System Status

This tab sets whether members of the group can access the system using the System Status Application (SSA).

Field	Description
System Status - Access	If selected, members of the Rights Group can view the system's current status and resources using the System Status Application (SSA).
Read All Configuration	The System Status application includes tools to take a snapshot of the system for use by Avaya for diagnostics. That snapshot can include a full copy of the system's configuration settings. This setting must be enabled for the SSA user to include a copy of the configuration in the snapshot.
System Control	If enabled, the SSA user is able to use SSA to initiate system shutdowns and memory card shutdown/restarts.
System Monitor - Access	If enabled, members of the Rights Group can use the System Monitor application to perform detailed diagnosis of system problems.

Related links

Rights Groups on page 583

Telephony APIs

Field	Description
Enhanced TSPI Access	If selected, applications in this rights group are able to use the system's Enhanced TSPI interface. This interface is currently used by the one-X Portal application server for its connection to the system.
DevLink3	If selected, applications in this rights group are able to use the system's DevLink3 interface. This is a TCP based interface that streams real time call events (Delta3 records) and is the recommended replacement to the existing DevLink Windows based DLL. A new Rights Group with a user name and password is required for external applications to connect via the DevLink3 interface.
Location API	If selected, applications in this rights group are able to use the system's Location API interface.

Related links

Rights Groups on page 583

Web Services

These settings are used by users in rights groups using web services to configure and manage the system. These are currently not used on Standard Mode systems

IP Office Service Rights

Field	Description
Security Read All	If selected, the rights group members can view system security settings.
Security Write All	If selected, the rights group members can change system security settings.
Security Write Own Password	If selected, members of the Rights Group can change their own password when requested to do so by the system. That request may be the result of the **Force new password** or **Account Password Change Period (days)** settings. The new password change is requested automatically at login time.
Configuration Read All	If selected, the rights group members can view system configuration settings
Configuration Write All	If selected, the rights group members can change system configuration settings.
Backup	If selected, the rights group members can initiate the system backup process.
Restore	If selected, the rights group members can initiate the system restore process.
Upgrade	If selected, the rights group members can initiate the system upgrade process.

Web Manager Rights

Field	Description
File Manager	If selected, the rights group members are assigned Read only access to embedded file management configuration settings in Web Manager by default.
Service Commands	If selected, the rights group members are assigned Read only access to Service Commands configuration settings in Web Manager by default.
Users, Extensions	If selected, the rights group members are assigned Read only access to Users and Extension configuration settings in Web Manager by default.
Groups, Auto Attendant	If selected, the rights group members are assigned Read only access to Groups, Auto Attendant configuration settings in Web Manager by default.
Incoming Call Routes, Alternate Route Selection, Short Codes	If selected, the rights group members are assigned Read only access to Incoming Call Routes, Alternate Route Selection, and Short Codes configuration settings in Web Manage by default.
System, Locations, Time Profiles and Licensing	If selected, the rights group members are assigned Read only access to on System, Locations, Time Profiles, and Licensing configuration settings in Web Manager by default.
Lines	If selected, the rights group members are assigned Read only access to Lines configuration settings in Web Manager by default.
Directory, Authorization Codes, Account Codes	If selected, the rights group members are assigned read only access to Directory, Authorization Codes, and Account Codes configuration settings in Web Manager by default.

Table continues…

Field	Description
IP Routes, WAN Ports, Firewall Profiles, RAS, Services, Tunnel	If selected, the rights group members are assigned read only access to IP Routes, WAN Ports, Firewall Profiles, RAS Services Users and Extension configuration settings in Web Manager by default.
User Rights	If selected, the rights group members can access to user rights configuration settings in Web Manager.

Related links

Rights Groups on page 583

External

IP Office Service Rights

These settings are used by users in rights groups for external components using web services to configure and manage the system.

Field	Description
Voicemail Pro Basic	If selected, the rights group members can read the configuration and perform backup, restore, and upgrade.
Voicemail Pro Standard	If selected, the rights group members can update the configuration and perform backup, restore, and upgrade.
Voicemail Pro Administrator	If selected, the rights group members can update the configuration and security settings.
one-X Portal Administrator	If selected, the rights group members can update the configuration and security settings. Does not include backup and restore.
one-X Portal Super User	If selected, the rights group members can perform backup and restore.
Web Control Administrator	If selected, the rights group members can update the configuration settings.
Web Control Security	If selected, the rights group members can update the security settings.
WebRTC Gateway Administrator	If selected, the rights group members can update the configuration settings.
Management API Read	If selected, support the use of the management API to access system configuration settings.
Management API Write	If selected, support the use of the management API to change system configuration settings.
Media Manager Administrator	If selected, the rights group members can update Media Manager configurations and settings. The rights group members can also access all archived recordings.
Media Manager Standard	If selected, the rights group members can have read-only access to Media Manager configurations and access to the recordings.

Table continues…

Field	Description
Reporter Administrator	If selected, the rights group members can have configuration access to Integrated Contact Reporter.
one-X CTI API	If selected, support use of one-X CTI API commands.
Adjunct Server Connection	Used to support a websocket connection between an IP Office system and an IP Office application server supporting that system.
TURN Server Connection	Allow the name and password details of the rights group's associated service user to be sent to IP Office User Portal sessions. They then use those details to connect to the TURN server specified in **System | LAN | Network Topology**.

Related links

Rights Groups on page 583

HTTP

This tab sets the HTTP services supported for members of the group.

Field	Description
DECT R4 Provisioning	This service allows the IP Office system to provision the Avaya Wireless DECT master base station with information from the IP Office configuration. It can then also respond to handsets subscribing to the Avaya Wireless DECT system. It requires both the IP Office system and Avaya Wireless DECT master base station to be configured to enable provisioning. See the Deploying Avaya Wireless DECT with IP Office manual.
Directory Read	If selected, members of the Rights groups have HTTP service read access to directory records.
Directory Write	If selected, members of the Rights groups have HTTP service read and write access to directory records.

Related links

Rights Groups on page 583

Service Users

Navigation: Security > **Security Settings** > **Service Users**

Click **Add/Edit Service User** to open the Add Service User window.

Note that the requirements for these setting (length and complexity) are set through the **Service User Details** on the **General** security settings tab.

Field	Description
Name	Range = Up to 31 characters. Sets the service user's name. • If changing the user name and/or password of the current service user used to load the security settings, after saving the changes close the configuration.
Password	Range = 9 to 31 characters. Sets the service user's password. Note that when changing a password, a error is indicated if the password does not meet the service user password rules.
Clear Cache	Clears the cache of previous passwords stored when **Previous Password Limit (Entries)** is enabled. Allows a previous password to be used again.
Account Status	Default = See Default Service Users and Rights Groups on page 563. Sets whether the account is **Enabled**, **Disabled** or **Force new password**. • The **Password Reject Action** on the **General** security settings tab can automatically disable an account after too many failed password attempts. • If an **Account Expiration** date is set, the account is automatically disabled after that date. • A service user set to **Force new password** if required to set a new password when logging in. After they enter a new password entered, the account status changes to **Enabled**.
Account Expiration	Default = <None> (No Expiry). You can use this option to set a calendar date after which the account is disabled. • To prompt the user for a new password before the expiry date, set an **Expiry Reminder Time (days)** on the **General** security settings tab.
Rights Groups	Default = See Default Service Users and Rights Groups on page 563. The check boxes are used to set the rights groups to which the service user account belongs. The service user's rights will be a combination of all the rights of those groups.

Related links

Security Settings on page 573

Certificates

Navigation: Security > Security Settings > Certificates

Services between the system and applications can, depending on the settings of the service being used for the connection, require the exchange of security certificates. The system can either generate self-signed certificate or use certificates from a trusted source can be loaded.

Identity Certificate

These settings relate to the X.509v3 certificate that the system users to identify itself when connecting another device using TLS. For example, a PC running IP Office Manager set to **Secure Communications**.

The system's certificate is advertised (used) by services which have their **Service Security Level** set to a value other than **Unsecure Only**.

By default, each IP Office server provides a self-generated certificate, generated when the system is first installed. However, the certificate can also come from other sources:

- An alternate identity certificate for the system from added using the **Set** button.
  - For secondary, expansion and application servers, this can be an identity certificate generated for that server from the web control menus of the primary server.
- For subscription mode systems, **Automatic Certificate Management** can be selected. COM then automatically provides the system with an appropriate identity certificate and certificate updates.

Field	Description
Offer Certificate	Default = On. This is a fixed value for indication purposes only. This sets whether the system will offer a certificate in the TLS exchange.
Offer ID Certificate Chain	Default = On When enabled, the IP Office advertises a chain of certificates during TLS session establishment. • The chain of certificates starts with the system's identity certificate • It then adds any certificates it finds in its trusted certificate store with the same `Common Name` in their "Issued By" `Subject Distinguished Name` field. • If the Root CA certificate is found in the trusted certificate store, that is also included in the certificate chain. • A maximum of six certificates are supported in the certificate chain.
Issued To	Default = IP Office identity certificate. For information only. The common name of certificate issuer.
Certificate Expiry Warning Days	Default = 60, Range = 30 to 180 IP Office Manager can display a warning when a system's security certificate is due to expire. This setting is used to set the trigger for certificate warnings.

The following settings are only shown for subscription mode systems. They allow COM to provide the system with its identity certificate and to automatically update the certificate when required.

Field	Description
Automatic Certificate Management	Default = Disabled Supported for subscription mode systems only. When enabled, the system uses an identity certificate supplied by COM along with a copy of the COM root certificate. The maintenance and renewal of the identity certificate and its trust chain are performed automatically.
SAN Details Origin	If the identity certificate issued to the system by COM needs to include any location specific subject alternate name values, this field can be used to define those values. • **Migrate from existing ID certificate** - When generating a new certificate for the system, use the SAN details from its existing identity certificate. • **Generate form current LAN configuration** - When generating a new certificate, create the SAN details from the system's existing LAN and SIP settings.
Automatic Phone Provisioning	Default = Enabled This additional option is supported when using **Automatic Certificate Management**. When enabled, phone certificates on phones that support certificate download, are automatically updated when the system identity certificate is updated. • New and default phones obtain the certificate using the normal trust on first use process. • When an update occurs, the `46xxsettings.txt` file is updated to includes details of both certificates. Following a restart, the phones fetch the new certificate using the old certificate details.

The following settings can be used to manage the current identity certificate.

Field	Description
Set	Using **Set** allows you to load an identity certificate and its associated private key. • This control is not shown for subscription mode systems using **Automatic Certificate Management**. The IP Office supports: • 1024, 2048 and 4096 bit RSA keys. Use of 4096 RSA keys may impact system performance. • SHA-1, SHA-256, SHA-384, and SHA-512 signature algorithms. Using signature size larger than SHA-256 may impact system performance. The source may be: • Current User Certificate Store. • Local Machine Certificate Store. • File in the PKCS#12 format. - Pasted from clipboard in PEM format, including header and footer text. This method must be used for PEM (`.cer`) and password protected PEM (`.cer`) files. The identity certificate requires both the certificate and private key. The CER format does not contain the private key. For these file types, select **Paste from clipboard** and then copy the certificate text and private key text into the Certificate Text Capture window. **Using a file as the certificate source:** In Manager, when using the file option, the imported file (`.p12`, `.pfx` or `.cer`) can only contain the private key and identity certificate data. It cannot contain additional Intermediate CA certificates or the Root CA certificate. The Intermediate CA certificates or the Root CA certificate must be imported separately into the IP Office Trusted Certificate Store. This does not apply to Web Manager. **Note:** Web Manager does not accept the file of type CER with extension `.cer`. That file type can only be used in Manager.
View	Displays details of the current identity certificate. The certificate view menu can also be used to install the certificate (but not its private key) into the viewing PCs local certificate store. This can the be used by the PC for secure connection to the system or to export the certificate from the PC.

Table continues…

Field	Description
Regenerate	This command generates a new identity certificate: • For system's using the system's own self-generated self-signed identity certificate, this command generates a replacement for the current identity certificate. • For subscription mode system's, this command requests a replacement identity certificate from COM. Alternatively, it can be used to request an identity certificate for another server. **Important:** • Regeneration takes up to a minute, during which time system performance is impacted. Therefore, only perform this action during a maintenance window. The regeneration takes places after saving the security settings. When clicked, the **Regenerate Certificate** window prompts you to enter the values in the following table.

Setting	Description
Signature	Default = SHA256/RSA2048. Select the signature algorithm and the RSA key length to use for the new self-signed identity certificate. The options are SHA256/RSA2048 or SHA1/RSA1024.
Subject Name	Default = None Specifies the common name for the subject of this certificate. The subject is the end-entity or system that owns the certificate (public key). Example: `ipoffice-0123456789AB.avaya.com`. If left blank, a system generated subject name is used.
Subject Alternative Name(s)	Default = None Specify any Subject Alternative Name (SAN) values to include in the certificate. • Each entry consists of a prefix, followed by the colon and then the value. Supported prefixes are `DNS`, `URI`, `IP`, `SRV` and `email`. • Multiple entries can be added, each separated by the comma. The input field has a maximum size limit of 511 characters. • Example: `DNS:192.168.0.180,IP:192.168.0.18,URI:SIP:example.com`
For Different Machine	Default = Off This option is only shown for subscription mode systems using **Automatic Certificate Management**. When selected, the address details of the other server and the duration of the certificate (maximum 825 days) are requested. After generating the certificate, the browser automatically downloads the certificate file.

Trusted Certificate Store

This section displays a list of the certificates held in the system's trusted certificate store and allows management those certificates. Up to 25 X.509v3 certificates can be placed into the store.

When adding a certificate, the source can be:

- Current User Certificate Store.
- Local Machine Certificate Store.
- A file in one of the following formats:
  - PEM (`.cer`)
  - password protected PEM (`.cer`)
  - DER (`.cer`)
  - password protected DER (`.cer`)
- Pasted from clipboard in PEM format, including header and footer text.

  This method must be used for PKCS#12 (`.pfx`) files. Select **Paste from clipboard** and then copy the certificate text into the **Certificate Text Capture** window.

Certificate Checks

Field	Description
Certificate Expiry Warning Days	Default = 60. Range = 30 to 180 days. Set the number of days before the expiry of any stored certificate, at which IP Office Manager, IP Office Web Manager, and System Status Application will display warnings
Use different certificate for SIP telephony	Default = None The possible settings are **None**, **SIP Trunks** or **SIP & SM Trunks, SIP Phones**. • When set to **None**, all secure telephony communications use the system's default identity certificate and settings. • When set to any other option, an extra set of options similar to those shown for **Identity Certificate** section are displayed. These can be used to define the certificate used for secure telephony communications. The certificate to use is uploaded to the system's certificate store using the **Set** button.

Table continues…

Field	Description
Received certificate checks (Management interfaces)	Default = None. This setting is used for HTTPS/TLS administration connections to the system by applications such as IP Office Manager when the **Service Security Level** of the service being used is set to **High**. The received certificate is tested as follows: • **None** - The certificate must be in date. No extra checks are made. • **Low** - As above but also: - Check the certificate's public key is 1024 bits or greater.. • **Medium** - As above, but also: - Check there is a trust chain from the Trusted Certificate Store (TCS) to the root Certificate Authority (CA). - For IP Office R11.1.3 and higher: • Check that the certificate has a key usage defined. • If the certificate has extended key usage settings, check they match the purpose for which the certificate is being used. • Check that the certificate does not include any unknown extensions marked as critical. • Note: For systems upgraded to R11.1.3, these additional checks are only used after the existing setting is changed. For example, changed from **Medium** to **High** and then back to **Medium**. Avaya recommend to backup the configuration before making any changes. • **High** - This settings enables implementation of a strict trust domain where only known certificates are accepted. This is a form of 'certificate pinning' and overcomes the limitation of the standard tree structure PKI where any certificates issued by the root CA are always trusted. **High** uses the same checks as **Medium** plus: - Check the certificate's public key is 2048 bits or greater - Check the certificate is not a self-signed certificate. - Not reflected. - Check there is a copy of the certificate in the IP Office system's Trusted Certificate Store. • **Medium + Remote Checks** - Use the same checks as **Medium** plus the following: - Perform hostname validation by verifying one of the SAN entries matches the connection's FQDN. If necessary, the SAN entry used can be an IP address. - For SIP, verify that the certificate source is authoritative for the SIP domain as per RFC5922. • **High + Remote Checks** - Use the same checks as **High** plus the same additional checks as **Medium + Remote Checks**.

Table continues…

Field	Description
Received certificate checks (Telephony endpoints)	Default = None. This setting sets how the IP Office validates the identity certificate it receives for TLS telephony connections. • An identity certificate is not installed in all SIP phones. Therefore, for SIP, the IP Office does not require a client certificate from SIP phones, only from SIP and SM trunks. The received certificate is tested as follows: • **None** - The certificate must be in date. No extra checks are made. • **Low** - As above but also: - Check the certificate's public key is 1024 bits or greater.. • **Medium** - As above, but also: - Check there is a trust chain from the Trusted Certificate Store (TCS) to the root Certificate Authority (CA). - For IP Office R11.1.3 and higher: • Check that the certificate has a key usage defined. • If the certificate has extended key usage settings, check they match the purpose for which the certificate is being used. • Check that the certificate does not include any unknown extensions marked as critical. • Note: For systems upgraded to R11.1.3, these additional checks are only used after the existing setting is changed. For example, changed from **Medium** to **High** and then back to **Medium**. Avaya recommend to backup the configuration before making any changes. • **High** - This settings enables implementation of a strict trust domain where only known certificates are accepted. This is a form of 'certificate pinning' and overcomes the limitation of the standard tree structure PKI where any certificates issued by the root CA are always trusted. **High** uses the same checks as **Medium** plus: - Check the certificate's public key is 2048 bits or greater - Check the certificate is not a self-signed certificate. - Not reflected. - Check there is a copy of the certificate in the IP Office system's Trusted Certificate Store. • **Medium + Remote Checks** - Use the same checks as **Medium** plus the following: - Perform hostname validation by verifying one of the SAN entries matches the connection's FQDN. If necessary, the SAN entry used can be an IP address. - For SIP, verify that the certificate source is authoritative for the SIP domain as per RFC5922.

Table continues…

Field	Description
	• **High + Remote Checks** - Use the same checks as **High** plus the same additional checks as **Medium + Remote Checks**.
H.323 Security Level	Default = **High** (**Medium** for IP500 systems and systems upgrade to R11.1.3 or higher). Sets the minimum cipher strength the IP Office accepts on TLS connections for H.323 phones and trunks. Not used for clients where ciphers are enabled and chosen based on those offered by the TLS server. • This setting replaces the **CIPHER_LEVELS_H232** NUSN used by R11.1.2.x systems. • For further details, see the Avaya IP Office™ Platform Security Guidelines manual. • **Low** (0) - Accept low, medium, and high-strength ciphers. Low and medium on IP500 V2 systems. • **Medium** (1) - Accept medium and high-strength ciphers. Medium on IP500 V2 systems. • **High** (2) - Accept high-strength ciphers. Not supported for IP500 V2 systems. - For a list of ciphers, see https://documentation.avaya.com/bundle/IPOfficeSecurity/page/Supported_Ciphers.html. - High-strength ciphers are GCM ciphers. These are not supported by any model of IP500 V2 system.
SIP Security Level	Default = **High** (**Medium** for IP500 V2 systems and systems upgraded to R11.1.3 or higher). Sets the minimum cipher strength the IP Office accepts on TLS connections for SIP phones and trunks. Not used for clients where ciphers are enabled and chosen based on those offered by the TLS server. • This setting replaces the **CIPHER_LEVELS_SIP** NUSN used by R11.1.2.x systems. • For further details, see the Avaya IP Office™ Platform Security Guidelines manual. • **Low** (0) - Accept low, medium, and high-strength ciphers. Low and medium on IP500 V2 systems. • **Medium** (1) - Accept medium and high-strength ciphers. Medium on IP500 V2 systems. • **High** (2) - Accept high-strength ciphers. Not supported for IP500 V2 systems. - For a list of ciphers, see https://documentation.avaya.com/bundle/IPOfficeSecurity/page/Supported_Ciphers.html. - High-strength ciphers are GCM ciphers. These are not supported by any model of IP500 V2 system.

SCEP Settings

These settings are used for branch system's which are under centralized management through SMGR.

Simple Certificate Enrollment Protocol (SCEP) is a protocol intended to ease the issuing of certificates in a network where numerous devices are using certificates. Rather than having to

individually administer the certificate being used by each device, the devices can be configured to request a certificate using SCEP.

These settings are normally set during the systems initial configuration.

Field	Description
Active	Default = Off.
Request Interval (sec)	Default = 120 seconds. Range = 5 to 3600 seconds.
SCEP Server IP Address/Name	Default = Blank.
SCEP Server Port	Default = 80 for HTTP and 443 for HTTPS.
SCEP URI	Default = /ejbca/publicweb/apply/scep/pkiclient.exe
SCEP Password	Default = Blank.

Related links

Security Settings on page 573

Part 6: The Applications Menu

Applications menu options

Solution > **Applications**

This menu is used to access various other applications or the settings for those applications.

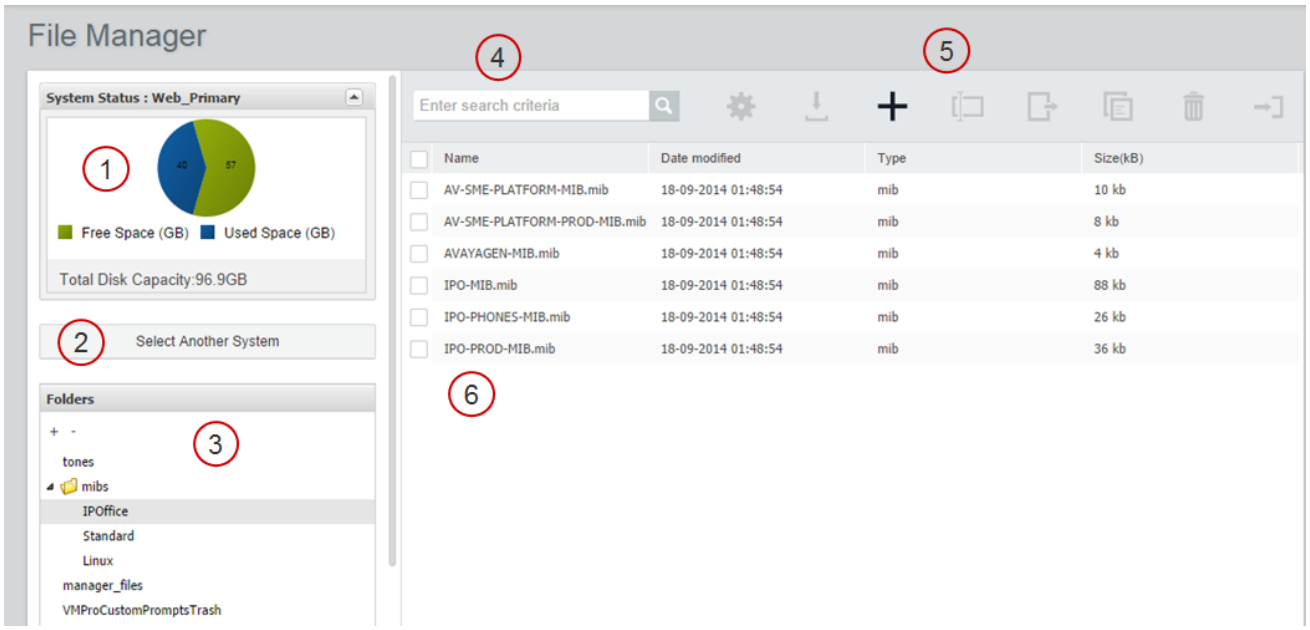
Application	Server Edition	IP500 V2	Application Server	UCM
File Manager	Yes	Yes	Yes	Yes
IP Office Manager	Yes	–	Yes	Yes
one-X Portal	Yes	–	Yes	Yes
Voicemail Pro - System Preferences	Yes	–	Yes	Yes
Voicemail Pro - Call Flow Management	Yes	–	Yes	Yes
WebRTC Configuration	Yes	–	Yes	
Media Manager	Yes	–	Yes	–
Centralized Media Manager Audit Trail	Yes	Yes	Yes	–

Chapter 41: File Manager

Solution > **Applications** > **File Manager**

This menu allows access to some of the folders on the server. It is intended for:

- Upload and download of files to and from the /system/primary folder used by the telephony service.
- Management of the custom prompts folder used by the voicemail service.



1	Graphic representation of disk capacity for the currently selected system.
2	Click to load a server into the File Manager.
3	The system folder directory. Select a folder to display the contents in the file list.
4	File search tool.
5	File management tool bar. Select a file in the file list to enable the tools.
6	File list.

Chapter 42: IP Office Manager

Solution > **Applications** > **IP Office Manager**

This command launches a locally installed instance of the IP Office Manager application and then automatically loads the IP Office service configuration file from the server. For details of using IP Office Manager, refer to Administering Avaya IP Office™ Platform with Manager.

Note:

- In order to open a client application (for example IP Office Manager), you must log into IP Office Web Manager using the IP Office LAN 1 IP address.

Note:

- This option is not supported by current browsers. The option is not available in later versions of IP Office Web Manager.

This action requires the IP Office service user account using IP Office Web Manager to have sufficient rights and to be shared on all the IP Office servers.

Manager software version

When used, the command checks whether IP Office Manager is already installed, and if so, the version of the application.

Scenario	Description
Manager version is current	If the Manager version is current, Manager launches without a login prompt and loads the configuration file for the server.
Manager version is not current	If the Manager version is not current, you are prompted to download and install the latest version and a link is provided. You can continue to use the currently installed version or download the current version. Upgrading to the current version requires a browser restart.
Manager is not installed:	If Manager is not installed, you are prompted to download and install the latest version and a link is provided. Once Manager is installed, a browser restart is required before launching Manager. • Note that the version of IP Office Manager installed is not the full version. It runs in English only and does not include the files needed for actions such as IP500 V2 system upgrades, phone firmware support, SD card recreation, etc. The full administration suite installer can be downloaded from support.avaya.com.

Synchronizing Server Edition passwords

In order to open IP Office Manager for a Server Edition solution, all IP Office systems in the solution must have a service user with common credentials. See Synchronize Service User and System Password on page 107.

Chapter 43: one-X Portal

Navigation: Solution > **Applications** > **one-X Portal**

Select **one-X Portal** to launch a administration menus of the one-X Portal service if that service is running on the server. For details of using the portal administrator menus, refer to Administering Avaya one-X Portal for IP Office.

Note:

- In order to open a client application (for example IP Office Manager), you must log into IP Office Web Manager using the IP Office LAN 1 IP address.

Chapter 44: Voicemail Pro - System Preferences

Navigation: Solution > Applications > Voicemail Pro - System Preferences

This menu provides access to the system preferences of the voicemail service running on the server.

Related links

General on page 605
Email on page 607
Gmail Integration on page 610
Housekeeping on page 611
SNMP Alarm on page 612
Outcalling on page 613
Voicemail Recording on page 614
Syslog on page 615
Alarms on page 615
User Group on page 617
Backup Config on page 617

General

Navigation: **Applications** > **Voicemail Pro - System Preferences** > **General**

Field	Description
Default Telephony Interface	Default = Intuity. Use this field to select the mailbox operation mode for all mailboxes. The options are: • Intuity • IP Office

Table continues…

Field	Description
Min. Message Length (secs)	Default = 0 seconds (in IP Office mode) and 3 seconds (in Intuity mode). Use this field to set a restriction on the minimum length for a message. The minimum value that you can set is 0 seconds, and the maximum value is 10 seconds. Messages that are of shorter length than the set minimum length are deleted immediately. In IP Office mode, this field is unavailable.
Voicemail Password	Default = Blank. Range = exactly 31 characters. For IP Office 11.1 FP1 and higher versions, the password for voicemail connection is enforced to 31 characters. This password is also set through the Voicemail Pro client application. When no password is set, an auto generated password is automatically set on both Voicemail Pro client and Web Manager systems.
Max. Message Length (secs)	Default = 120 seconds. Use this field to set a restriction on the maximum length for a message. The maximum value that you can set is 3600 seconds (60 minutes). A message with the message length of 1 minute occupies approximately 1MB of disk space.
Max. Call\VRL Record Length (secs)	Default = 3600 seconds. Use this field to set a restriction on the maximum recording length for the calls. The minimum value that you can set is 5 seconds. The maximum value that you can set is 18000 seconds (300 minutes).
Play Advice on Call Recording	Default = On Sets whether an advice warning is played to all callers when their call is being recorded. It is a legal requirement in some countries to inform the callers before recording their calls, therefore you must get confirmation before you turn this option off.
Failback Option	Default = Graceful Use this field to configure the mode of failback operation in a voicemail system with a backup Voicemail Pro server. Note that this field is unavailable if you are not using a voicemail system with a backup Voicemail Pro server and not logged on to the active Voicemail Pro server using an Administrator account. Failback is only considered if the preferred and back-up voicemail servers have started their synchronization operation (SMTP exchange of messages, etc). • **Manual**: The system administrator has to initiate the failback operation. • **Graceful**: The backup server initiates the failback operation once all current calls on the backup voicemail server end. • **Automatic**: The backup server initiates the failback operation once all current calls on the backup voicemail server end or, if exceeded, after the specified timeout period set (maximum 60 minutes).

Table continues…

Field	Description
System Fax Number	Default = Blank Use this field to set the number of the fax machine to which all incoming faxes are to be directed. If you are using a fax board, the number that you enter must match the extension number that is connected to the fax board of the fax server computer.
Use as a Prefix	If your fax system does not use prefix addressing, leave this box unchecked. For this feature to work, you also need to set up a short code.
Enable Fax Sub-Addressing	Most fax servers perform fax forwarding based on DTMF signaling received with the fax call. Select the Enable Fax Sub-Addressing check box so that the DTMF signal is passed to the fax server after the call has been answered so that the fax can be forwarded to the e-mail address of the intended recipient.
Archive Solution	Sets how the voicemail server should treat call recordings when VRL is selected as the recording destination: • **Media Manager**: Save the recordings in `.opus` format for collection by the system's VRL application, for example Media Manager. - When using this format, all recordings are authenticated. That is, the **VRL** and **VRLA** methods of recording are the same. • **External**: Save the recordings in `.wav` format for collection by a 3rd-party call archiving application.
Enable Voicemail Pro Client Interface	Default = Yes. Used to manage communication between the Voicemail Pro server and the client. When set to No, Voicemail Pro clients cannot connect to this Voicemail Pro server. When set to Yes, communication between the server and clients is allowed.
Minimum Protocol Version	Sets the minimum TLS protocol used for TLS links to the voicemail server. The options are TLS 1.0 or TLS 1.2. Note that changes to this setting require the voicemail service to be restarted to take effect.

Related links

Voicemail Pro - System Preferences on page 605

Email

Navigation: **Applications** > **Voicemail Pro - System Preferences** > **Email**

Note:

If you are using Voicemail Pro in a distributed environment, a distributed server delivers a recorded message to the central Voicemail Pro server on completion of the recording. However, the presentation to the Voicemail Pro server for message waiting indication (MWI) and access via telephone might be delayed because of the internal processing of the message and the network latency. The delay might be up to 2 minutes in high traffic situations.

Field	Description
Enable MAPI/EWS	Default = MAPI <Description> The options are: • MAPI • EWS • None
MAPI Service	
Address	Default = Blank.
Port	Default = 50792
SMTP Sender These settings are used to configure the SMTP server and the server account that Voicemail Pro server uses for sending e-mails through SMTP. Multiple servers can be configured. The first entry specifies the default SMTP server used for sending e-mails if there is no other entry matching the domain specified in the e-mail destination address. Additional servers can be added when different settings are required for sending e-mails to specific domains. For example, the default can be configured for the customer's internal network exchange server with additional entries added for e-mails to external e-mail domain addresses such as yahoo.com. VPNM, distributed Voicemail Pro servers, and primary/backup Voicemail Pro servers all use SMTP to exchange information and messages between Voicemail Pro servers. When that is the case, the first entry in the SMTP Sender list must be the one used and needs to be configured for that service with the domain and server setting both matching the IP address or fully-qualified domain of the Voicemail Pro server.	
Logging	Default = No. Set to Yes to enable SMTP logging. For information on SMTP logging see *Avaya IP Office Platform Voicemail Pro Administration*.
Add SMTP Sender	Click to open the SMTP Sender Configuration window.
Test Connection	Click to validate the SMTP configuration. When clicked, Voicemail Pro serves the SMTP server test connectivity request based on the input provided in the SMTP Sender Configuration window and provides a success or failure response. You must fill up all the four fields to test the connection. However, Voicemail Pro uses the values provided in the **Mail Server** and **Port** fields to validate the connection.

Table continues…

Field	Description
Mail Domain	Default = Blank. This field is used differently depending on whether it is the first entry in the list or not. **First server entry in the list:** This is the default outgoing e-mail setting. It also sets the mail destination domain on which the Voicemail Pro server filters incoming messages (see below) and so is repeated in the SMTP Receiver settings. For messaging between Voicemail Pro servers, the first entry in the SMTP Sender list must be the one configured and used. Each server uses the SMTP server service on the same server computer as the voicemail service. For example a Windows-based server uses the SMTP e-mail provided by the IIS on the same server. The voicemail service also uses the domain set to filter incoming SMTP mails received by the SMTP server. For this to work, the domain entered should be the fully-qualified name of the server on which the Voicemail Pro server is running, for example vmpro1.example.com. Any incoming messages where the recipient mail domain is not exactly the same as the specified domain are ignored. The recipient can either by vmsyncmaster, vmsyncslave, or the name or extension of a mailbox on the Voicemail Pro server, for example `Extn201@vmprocentral.example.com` or `201@vmprocentral.example.com`. **Subsequent entries:** The domain specifies that these settings should be used for e-mails sent to the matching domain. The entry must be a fully-qualified name resolvable by DNS or an IP address.
Mail Server	Default = Blank. Specifies the IP address or fully-qualified domain name of the SMTP server to which messages are sent. Voicemail Pro supports SMTP communication over both - SSL/TLS and plain text. **First server entry in the list:** Where messaging between Voicemail Pro servers is being used (central, backup and or distributed servers), the first entry is used and will match the domain set above. **Subsequent entries:** It will be the address of the e-mail server that will handle e-mails for recipients other than another Voicemail Pro server on the network.
Port	Default = Blank. The port number on the SMTP server to which the messages are sent. Port number for an external SMTP server can be different depending on whether you want to send the messages in secure mode or non-secure

Table continues…

Field	Description
Sender	Default = Blank. Note that some servers will only accept e-mails from a specific sender or sender domain. If left blank, the Voicemail Pro server will insert a sender using either the e-mail address set for the voicemail mailbox user if set or otherwise using the best matching name it can resolve from the IP Office.
Server Requires Authentication	Default = No. Indicates whether the connection to send SMTP messages to the mail server requires authentication with that server. The authentication will typically be to the name and password of a mailbox account configured on that server. Setting to **Yes** enables the **Account Name** and **Password** fields.
Account Name	Default = Blank. Sets the name to use for authentication.
Password	Default = Blank. Set the password to use for authentication.
SMTP Receiver These settings are used to set where the Voicemail Pro server checks for incoming SMTP messages.	
SMTP Receiver	Default = Internal. The options are: • **Internal**: Use this option for Voicemail Pro servers running on the IP Office Application Server. The Internal setting can also be used when the Voicemail Pro server should check the appropriate account on an SMTP server for waiting messages. The server settings will be pre-populated using the **SMTP Sender** settings. • **External**: Use this option when the Voicemail Pro server is on a server where is co-exists with a third-party SMTP application, for example an IIS server with SMTP enabled.
Port	Default = 25 The port on which the Voicemail Pro server listens for incoming messages.
Domain	Default = The domain set by the first server entry in the **SMTP Sender** list. The domain destination address for which the server will accept incoming e-mails.

Related links

Voicemail Pro - System Preferences on page 605

Gmail Integration

Navigation: **Applications** > **Voicemail Pro - System Preferences** > **Gmail Integration**

Additional configuration information

For additional information, see Configuring Gmail Integration on page 833.

Field	Description
Enable Gmail Integration	Default = No. This setting only applies to Server Edition systems. The system setting to enable the use of Gmail for voicemail. When set to Yes, you can configure users for Gmail on **Call Management** > **Users** > **Add/Edit Users** > **Voicemail**.
Upload Google Service account generated keys	You must register the Voicemail Pro application for the Gmail API in the Google Developer's console. You must create a Google service account and generate the JSON and P12 key files. Use the **JSON Key File** and **P12 Key File** buttons to upload the files to Web Manager. Web Manager transfers the files to the Voicemail Pro application.

Related links

Voicemail Pro - System Preferences on page 605

Housekeeping

Navigation: **Applications** > **Voicemail Pro - System Preferences** > **Housekeeping**

Use the Housekeeping settings to:

- Set the duration after which the Voicemail Pro server deletes messages and recordings automatically.
- Set the default playback order of messages. Playback can be set to **Oldest First** or **Newest First**.

Note:

The housekeeping deletion settings do not apply to the messages forwarded to an Exchange server. The messages that are forwarded to an Exchange server are deleted from the Voicemail Pro server in accordance with the **Deleted messages** settings.

Field	Description
New Messages	This status is applied to messages where neither the header nor the message content has been played.
Old Messages	This status is applied to messages where the user has played the message content but has not marked the message as saved.
Saved Messages	This status is applied to messages that have been marked as saved by the user.
Unopened Messages	This status is used for messages where, in Intuity emulation mode, the user has played the message header but has not played the message content.
New Recordings	This status is used for recordings that have not been played.

Table continues…

Field	Description
Old Recordings	This status is used for recordings that have been played.
Deleted Messages	This status is used for messages that have been marked as deleted through mailbox access.

Related links

Voicemail Pro - System Preferences on page 605

SNMP Alarm

Navigation: **Applications** > **Voicemail Pro - System Preferences** > **SNMP Alarm**

IP Office can be configured to generate alarms. These alarms can be sent using SNMP, SMTP e-mail, or Syslog alarm formats. These settings are used to set the levels at which the Voicemail Pro server will indicate to the IP Office to send an alarm.

Field	Description
Alarm Threshold Unit	Default = Recording Time Left (mins). The units, minutes or MB, used to set the alarm. The options are: • Recording Time Left (mins) • Disk Space Left (MB)

Table continues…

Field	Description
Alarm Threshold Level	Default = 60. The level at which SNMP alarms are to be triggered. The minimum value that you can enter is 11. the following additional alarms are set based on the **Alarm Threshold Level**. • **Space OK Alarm**: Triggered when the amount of available space returns to above a level set at **Alarm Threshold Level** plus 30. • **Critical Alarm**: This alarm is set at 30. If the **Alarm Threshold Level** is set at less than 40, the critical alarm is set at **Alarm Threshold Level** minus 10. Note that the critical alarm value decreases if you decrease the **Alarm Threshold Level**, but the critical alarm value does not increase if you increase the **Alarm Threshold Level**. So, the critical alarm value keeps on decreasing and remains set at the least value that it takes. To reset the critical alarm back to 30, click **Default Settings**. • For Voicemail Pro Server Edition, IP Office sends SNMP alarms based on the percentage of the available free space of the total disk space. The SNMP alarms are as follows: - **Disk State Critical**: Free disk space is less than 5% - **Disk State OK**: Free disk space is between 5 to 10% - **Disk State Free**: Free disk space is greater than 10% - **Disk State Stop Recording**: Free disk space is 0.
Default Settings	Return to the default alarm settings. Alarm Threshold Level is reset to 60. The Space OK level is reset to 90. The Critical Alarm level is reset to 30.

Related links

Voicemail Pro - System Preferences on page 605

Outcalling

Navigation: **Applications** > **Voicemail Pro - System Preferences** > **Outcalling**

Field	Description
System Times **Prime Time** is the period that outcalling is to be active as default for the system. **Peak Time** is the busiest working hours.	
From Prime Times	Default = 7:30. Set the beginning of the prime time interval.

Table continues…

Field	Description
To Prime Times	Default = 19:30 Set the end the prime time interval.
From Peak Times	Default = 7:30. Set the beginning of the peak interval.
To Peak Times	Default = 19:30 Set the end the peak interval.
System Retries Settings	
Number of Retries	Default = 5. Range = 0 to 10. If the message is not collected after the last retry, no notification is sent until another new message is delivered in the user's mailbox.
Retry Interval	The interval between each successive try. The interval is the length of time between each attempt to connect to the target number again. The 6th to 10th retries use the default retry interval.

Related links

Voicemail Pro - System Preferences on page 605

Voicemail Recording

Navigation: **Applications** > **Voicemail Pro - System Preferences** > **Voicemail Recording**

Use the Voicemail Recording page to configure an SFTP connection on a Linux-based Voicemail Pro server to transfer call recordings to the Voice Recording Library (VRL) application Avaya IP Office ContactStore .

Before you configure the Voicemail Recording settings, you must have configure an SFTP server running on the computer that runs the ContactStore application. For details on the SFTP server requirements.

Field	Description
FTP User Name	The user name used to log in to the FTP server.
FTP Password	The password used to log in to the FTP server.
Remote FTP Location	<IP address>?
Remote FTP Host	The FTP server host name.
Test Connection	Click to test the connection.

Related links

Voicemail Pro - System Preferences on page 605

Syslog

Navigation: **Applications** > **Voicemail Pro - System Preferences** > **Syslog**

You can configure the Voicemail Pro server to write syslogs to a syslog server.

Field	Description
Enable Syslog	Default = No. Click Yes to enable logging.
IP Address	Default = Blank. The IP address of the syslog server.
Port	Default = 514 A UDP port number on which target syslog server is listening for syslog records.

Related links

Voicemail Pro - System Preferences on page 605

Alarms

Navigation: **Applications** > **Voicemail Pro - System Preferences** > **Alarms**

The Voicemail Pro client can display the alarm calls that have been configured for the Voicemail Pro to perform.

The Voicemail Pro is limited to 2 outgoing alarm calls at the same time (subject to voicemail port availability). Any additional alarm calls are delayed until the existing alarm calls have been completed.

Field	Description
Add Alarm Click to configure the following alarm settings.	
Target	
Time	Default = 00:00. Set the alarm time in 24-hour format (hh:mm or hhmm). A time value can be entered or a call variable can be used. If left blank or if the call variable used is not a valid time value, the call flow user will be asked to enter a time the same as if **Ask Caller** was selected.

Table continues…

Field	Description
Frequency	Default = Single. Sets how often the alarm should occur. The options are: • **Single** • **Daily** • **Weekly**
Day	Default = Today. Set the day for the alarm. You can select a specific day or **Today**.
File	Default = Blank. Optional. If a file is specified here it is used for the alarm call. If no file is specified the default alarm message "This is an alarm call, please hang up" is used.
Display Text	Default = Blank. By default the alarm will display "Alarm" on the target if it is an Avaya display telephone. This field can be used to customize the text used.
Ring Time	Default = 60 seconds. Range = 5 to 120 seconds. Set the length of ring time used for the alarm call if not answered.
Retries	Retries: Default = 0 (Off). Range = 0 to 10. Used to specify how many times the alarm should be repeated if it is not answered and cleared. When a value other than 0 is selected, the Interval option becomes available to specify the interval between repeats.
Interval	Default = Blank (Off). If a number of retires is specified, this option can be used to select the number of minutes between repeated alarm attempts until the alarm is cleared.
Enable Cancel Code	Default = No. When off, the alarm is cleared if the alarm call is answered. When on, a dialing code can be specified. If the correct code is not dialed in response to an alarm, the alarm is not cleared and will repeat if retries have been specified.
Cancel Code	Default = * , Range = Up to 4 digits. used to enter the dialing required to clear the alarm call. The value * will match any dialing. To cancel the alarm, the cancel code must be entered followed by the hash key (#). The file used to play the alarm message must mention the cancel code and the fact that cancel code must be followed by the hash key (#).
Alarms The following additional fields are displayed in the Alarms table.	
Created	Time on phone when the alarm was created
Next Activation	When the next alarm is going to get triggered
Type	
When	

Table continues…

Field	Description
Number	

Related links

Voicemail Pro - System Preferences on page 605

User Group

Navigation: **Applications** > **Voicemail Pro - System Preferences** > **User Group**

Field	Description
User Group	
Name	Used to configure which mailboxes are included in a backup when **Selective Voicemail Users** is selected as one of the backup options.

Related links

Voicemail Pro - System Preferences on page 605

Backup Config

Navigation: **Applications** > **Voicemail Pro - System Preferences** > **Backup Config**

These settings are shown on the subscription systems. They set which voicemail elements should be included in the automatic daily backup of those systems to COM.

Field	Description
Configuration Backup	If enabled, it includes the voicemail service configuration in the automatic backups.
Custom Prompts Backup	If enabled, it includes the custom prompts folder in the automatic backups.
Selective Mailboxes Backup	If enabled, it includes the messages from the mailboxes defined by the **User Group** preferences tab

Related links

Voicemail Pro - System Preferences on page 605

Chapter 45: Voicemail Pro - Call Flow Management

Solution > **Applications** > **Voicemail Pro - Call Flow Management**

This option displays a menu to download the voicemail call flow for local editing and to upload the edited call flow.

Option	Description
Download Voicemail Pro Offline Configuration File	This option downloads the voicemail server's call flow. It can then be edited and uploaded back to the system.
Upload Voicemail Pro Offline Configuration File	This option uploads an edited offline call flow back to the server.

- For further details, refer to Administering IP Office Voicemail Pro.
- To download and install the Voicemail Pro client, select **Solution** > ☰ > **Platform View** > **AppCenter**.

Chapter 46: WebRTC Configuration

Solution > **Applications** > **WebRTC Configuration**

These menus are supported on the same server as the Avaya one-X® Portal for IP Office service. The settings are used by the **WebRTC Gateway** services. For details, refer to the Deploying IP Office Server Edition manual.

The **WebRTC Gateway** service is used for WebRTC clients connecting through Avaya one-X® Portal for IP Office. For example:

- The Avaya one-X® Portal for IP Office Chrome browser client.
- The Avaya Spaces Chrome browser extension for Space Calling.

Note:

- IP Office User Portal uses the separate WebRTC gateway provided by the IP Office service rather than Avaya one-X® Portal for IP Office. Refer to the **System Settings** > **System** > **LAN1** > **Network Topology** menu settings. See Network Topology on page 495.

Related links

System Settings on page 619
SIP Server Settings on page 620
Media Gateway Settings on page 621

System Settings

Navigation: **Applications** > **WebRTC Configuration** > **System Settings**

The system settings which are applicable to all components of the WebRTC Gateway.

File	Description
Network Interface	Default = eth0. A list of available network interfaces on the Server. It is recommended to use the same network interface selected at IP Office configuration.
Local IP Address	Default = IP address of default network interface. A read-only field to show the IP address of the selected network interface.

Table continues…

File	Description
Gateway Listen Port	Default = 42004. The local listen port used by the WebRTC Gateway to accept SIP connections.
SIP Trunk Listen Port	Default = 42008. Local listen port used by WebRTC Gateway to accept SIP trunk connections.
Logging Level	Default = Info. Available log levels for the WebRTC Gateway. Changing the log level causes the WebRTC Gateway to restart. The options are • **Error** • **Warn** • **Info** • **Debug** • **Trace**
Allow Origins	Default = * Type the Domain names and IP addresses you want IP Office to accept connections from. If there are more than one entry, separate the entries by a semicolon (;). These Domain names and IP addresses are added to the WebRTC Gateway's CORS filter. WebRTC Gateway accepts WebSocket connections only from the Domain names and IP addresses whitelisted in the field. The Gateway maintains a list of Domain names and IP addresses to comply with Cross-Origin Resource Sharing (CORS) that enables cross-domain requests from Web browsers to servers and Web APIs. The `*` in this field allows connections from all Domains and IP addresses including Chrome extensions. Example: "`203.0.113.56`"; "`203.0.113.57`"; "`*.example.com`" If the above values entered in the field, connections from the IP addresses `203.0.113.56`, `203.0.113.57`, and any domains ending with `example.com` is allowed.

Related links

WebRTC Configuration on page 619

SIP Server Settings

Navigation: **Applications** > **WebRTC Configuration** > **SIP Server Settings**

The IP Office SIP settings used by WebRTC Gateway.

Field	Description
Configuration Mode	Default = Auto. The options are: • **Auto**: The settings are automatically populated and read-only. • **Manual**: Set to **Manual** to change any automatically populated value.
Domain Name	Default = Automatically populated value or blank. The SIP domain name of the Server Edition Primary server.
Private IP Address	Default = Automatically populated value or blank. Private IP address of the Server Edition Primary server.
Private TCP Port	Default = Automatically populated value or blank. Private TCP port of the Server Edition Primary server.
Private UDP Port	Default = Automatically populated value or blank. Private UDP port of the Server Edition Primary server.
Private TLS Port	Default = Automatically populated value or blank. Private TLS port of the Server Edition Primary server.
Public IP Address	Default = Automatically populated value or blank. Public IP address of the Server Edition Primary server.
Public TCP Port	Default = Automatically populated value or blank. Public TCP port of the Server Edition Primary server.
Public UDP Port	Default = Automatically populated value or blank. Public UDP port of the Server Edition Primary server.
Public TLS Port	Default = Automatically populated value or blank. Public TLS port of the Server Edition Primary server.
Transport Type	Default = Automatically populated value or blank. Transport type used by the WebRTC gateway, to connect to IP Office. The options are: • TCP • TLS

Related links

WebRTC Configuration on page 619

Media Gateway Settings

Navigation: **Applications** > **WebRTC Configuration** > **Media Gateway Settings**

File	Description
RTP Port Range (Private) Minimum	Default = 58002. Minimum RTP port value used for WebRTC media termination from the private interface.
RTP Port Range (Private) Maximum	Default = 60002. Maximum RTP port value used for WebRTC media termination from the private interface.
RTP Port Range (Public) Minimum	Default = 56000. Minimum RTP port value used for WebRTC media termination from the public interface.
RTP Port Range (Public) Maximum	Default = 58000. Maximum RTP port value used for WebRTC media termination from the public interface.
Codecs — Audio	The audio codecs used by the WebRTC Gateway, listed by priority. Use the arrows to change the priority. The options are: 1. PCMU 2. PCMA 3. telephone-event
Codecs — Video	The audio codecs used by the WebRTC Gateway. The options are: 1. VP8
DTMF Payload Type	Default = 101. RFC2833 default payload type used by the WebRTC Gateway.
STUN Server Address	Default = Blank. STUN server address (optional).
STUN Server Port	Default = Blank. STUN server port (optional).
TURN Server Address	Default = Blank. TURN server address (optional).
TURN Server Port	Default = Blank. TURN server port (optional).
TURN User Name	Default = Blank. TURN user name (optional).
TURN Password	Default = Blank. Password for Turn user name, if used.
Enforce TURN	Default = No. When set to Yes, enforces media traffic via the TURN server.

Related links

WebRTC Configuration on page 619

Chapter 47: Web License Manager

Navigation: Solution > **Applications** > **Web License Manager**

On systems using PLDS licensing, this option opens the admin menus for the WebLM service running on the server.

Login Credentials

WebLM credentials are managed separately from IP Office system passwords and are not part of single sign on. You must change the default password for the admin user after the first login. The default credentials are:

- User ID: `admin`
- Password: `weblmadmin`

Chapter 48: Media Manager

Solution > **Applications** > **Media Manager**

This set of menus are shown if the server is running the Media Manager service for the archiving of call recordings. That option is supported on the Server Edition primary server and on IP Office Application servers. Refer to Administering Avaya IP Office™ Platform Media Manager.

- Systems running in subscription mode can use either Media Manager or Centralized Media Manager as their service for archiving call recordings.

  For details of the later, see Centralized Media Manager on page 708.

Related links

Media Manager Configuration Settings on page 625
Connectors on page 627
Alarms on page 628
Recordings on page 628
Migration on page 630
Audit Trail on page 631

Media Manager Configuration Settings

Applications > **Media Manager** > **Configuration**

Name	Description
Profile	Default = Blank The unique name that identifies the configuration profile.
Log Level	Default = INFO The selected log level for the Media Manager service. The options are **INFO**, **DEBUG** and **ERROR**.
Handover Folder	Default = `/opt/vmpro/MM/VRL` The Voicemail Pro path from where Media Manager picks up the recordings. Voicemail Pro writes call recording files to this folder.

Table continues…

Name	Description
Days to Retain Calls	Default = 180 days. Range = 0 to 180 days. The number of days for which the database retains the call details. After this, Media Manager deletes the call recordings. • To disable the deletion, enter 0. • Note: Media Manager also starts deleting call recordings as soon as the allocated storage is full.
Audit Retain Period (Days)	Default = 180 days The number of days for which the Audit Trail or recordings are retained in IP Office Media Manager. The minimum value for this field is 1 day and the maximum 365 days.
Active Connector	Default = Blank The connector being used for remote archiving copies of recordings. The drop-down menu lists all the available connectors that have been configured. Changing the connector results in a change in the archive destination. However, the recordings from the previous archives are still available.
Call Storage Type	Default = Local Hard Drive Sets the destination that Media Manager use as its primary storage for recordings collected from the **Handover Folder**. • **Local Hard Drive** - Use the local hard drive partition specified by the **Call Storage Path** setting. • **Hosted Storage** - Use the cloud-based storage specified by the **Hosted Storage Type** settings.
Call Storage Path	Default = Blank. This field is available when the **Call Storage Type** is set to **Local Hard Drive**. • If the additional drive was added using the path `/additional-hdd#1`, enter `/additional-hdd#1/partition1`. The additional drive path used can be seen in the server's **Platform View** menus. • If you must change the value after you have already started recording, copy all the sub-directories and files from the old directory to the new directory before you resume recording.
Hosted Storage Type	This field is available when the **Call Storage Type** is set to **Hosted Storage**. The supported options are **Amazon S3 Bucket**, **Google Cloud Storage Bucket**, and **Microsoft Azure Blob Storage** Additional fields are shown depending on the selected **Call Storage Type**. For details, see the Administering Avaya IP Office™ Platform Media Manager manual.
Send Email	Default = No The option to select whether the system must send emails for alarms and events.

Table continues…

Name	Description
SMTP Mail Server	Default = Blank The SMTP mail server that IP Office Media Manager uses to send email messages about alarms and events. If you leave this field blank, system cannot send email messages for alarms and events.
SMTP Port	Default = Blank The SMTP port to which the service sends email messages.
Secured Connection	Default = No The option to indicate whether the connection is secured. A secured connection uses Transport Layer Security (TLS) protocol to communicate.
SMTP User Name	Default = Blank The user's name for the SMTP server. You can leave this field blank if SMTP server does not require sender authentication. If required, set the user's name here.
SMTP Password	Default = Blank The password for the SMTP server. You can leave this field blank if SMTP server does not require sender authentication. If required, set the password here.
SMTP Mail "From" Address	The address from which the SMTP emails containing the alarms and events originate.
Send Alarm/ Event Emails To	The email addresses to which alarms and events must be sent. You can add more than one email address by adding a semi-colon (;) between two email addresses.

Related links

Media Manager on page 625

Connectors

Applications > **Media Manager** > **Connectors**

For details of adding and editing connectors, see the Administering Avaya IP Office™ Platform Media Manager manual.

Name	Description
Add	The drop-down menu to select a connector. The options are **DVD**, **NAS**, **Google drive**, **Amazon S3 Bucket**, **Google Cloud Storage Bucket** and **Microsoft Azure Blob Storage**.
Name	The name of the connector.
Type	The type of connector selected.
Active	The state of the connector.
Reachable	The field that indicates whether the connector is reachable.

Table continues…

Name	Description
Pending Files #	The files that are yet to be archived.
Last Successful Archive Time	The time the connector was last used successfully.

Related links

Media Manager on page 625

Alarms

Applications > **Media Manager** > **Alarms**

Name	Description
Date	The date on which the alarm was generated.
Severity	The severity of the alarm. The options are **Information**, **Warnings**, **Minor Alarms**, **Major Alarms**, and **Critical Alarms**.
Description	A brief description about the alarm.

Related links

Media Manager on page 625

Recordings

Applications > **Media Manager** > **Recordings**

System administrators can use this menu to view and manage call recordings. Access to call recordings for individual users should be configured through their web self-administration settings.

Name	Description
Call Date	The date of the call.
Length	The duration of the recording.
Parties	The users that participated in a conference call.
Call Direction	The field indicates whether the call was Internal, Incoming, or Outgoing.
Agents	The agents involved in the call.

Table continues…

Name	Description
Owner	The owner of the recording. Each recording has an owner; the owner is the number of the extension that recorded the call. Any one of the following can be an owner: • Calling party extension • Called party extension • Hunt group extension • A line number • An account code • An agent extension
Targets	The phone numbers of the recipients of the call.
Skills	The skill set of the agent involved in the call.
Call ID	The unique identification number associated with the call recording.

Filter

Name	Description
Recording Range (Date and Time)	The date and time range between which the call was recorded. Use the calendars to select the dates and the adjacent drop-down menus to specify the time.
Recording Length	The length of the recording. Select one of the signs and enter the time in seconds. The available signs are: • **=** Equal to the recording length you have specified. • **<** Less than the recording length you have specified. • **>** Greater than the recording length you have specified. • **>=** Greater than or equal to the recording length you have specified. • **<=** Less than or equal to the recording length you have specified.
Call Direction	The direction of the call, that is, whether the call is Internal, Incoming, or Outgoing. Use the drop-down menu to select a Filter criterion.
Parties	The parties involved in the call. Type the names of the parties. For more than one party, type the names separated by a comma.
Agents	The agents involved in the call. Type the names of the agents. For more than one agent, type the names of agents separated by a comma.
Target Number	The phone number of the recipient of the call. Type the target number.
Skills	The skill set of the agent involved in the call.
Call ID	The unique identification number associated with the call recording.

Button	Description
Apply Filter	Click to apply the filter. All the recordings matching your search criteria are displayed on the right pane.
Show All	The system displays all the recordings on the right pane.
Delete	Use the button to delete the selected recordings. You can select one or more recording using the check boxes corresponding to the recordings.
Download	Use the button to download multiple recordings to your computer. 1. Select the recordings and click the **Download** button. 2. Type a password to protect the recordings. 3. You browser downloads the selected recordings as a zipped file.

Related links

Media Manager on page 625

Migration

Applications > **Media Manager** > **Migration**

IP Office Release 11 does not support Contact Recorder. However, existing customers of Contact Recorder can migrate their call record database to Media Manager, which is the only archiving solution in IP Office Release 11. The migration process includes migration of only the metadata of the call records stored in Contact Recorder locally, or remotely on DVD or NAS. The migration process does not move the actual media files. Using the migrated metadata, Media Manager identifies the call recordings and provides playback, downloading, and housekeeping facility. VRLA records migrated from Contact Recorder can still be verified for tampering using the Media Manager interface Thus Media Manager becomes a single interface for all call records, whether archived through Media Manager for newer recordings or the older recordings archived through Contact Recorder.

Existing Contact Recorder users can migrate to Media Manager through Web Manager. Administrators can migrate the Contact Recorder database to Media Manager using **Applications** > **Media Manager** > **Migration**. For detailed instructions, refer to the Administering Avaya IP Office™ Platform Media Manager guide.

Note:

Contact Recorder customers must back up their database prior to upgrading to IP Office Release 11.

Related links

Media Manager on page 625

Audit Trail

Applications > **Media Manager** > **Audit Trail**

Name	Description
Search on "User Name"	The Search text box to search the audit records of a User. Type the User Name to search the users activities in the recording library.
User Name	The name of the user who used the recording.
Timestamp	The time when the recording was used.
User Action	The type of user action on a recording. This specifies whether a recording was replayed, downloaded, deleted, or searched.
Details	The details of a recording such as owner of the recording, media name, calling party name, and so on.
Start Date	The date and time after which the event has occurred. Use the calendar to select the date and the adjacent drop-down menu to specify the time.
End Date	The date and time before which the event has occurred. Use the calendar to select the date and the adjacent drop-down menu to specify the time.
Event Type	The type of events you want to view. IP Office Media Manager keeps track of the following type of operation on the recordings: • **Delete**: Displays the recordings that are deleted. • **Download**: Displays the recordings that are downloaded. • **Replay**: Displays the recordings that are replayed. • **Search**: Displays the recordings that are searched.
Export	The option to export the filtered audit results as a zipped `.CSV` file on your computer. The file contains four columns with the following information: • **User Name** • **Timestamp** • **User Action** • **Details**

Filter

Button	Description
Apply Filter	Use the button to refine your search. You can filter your search based on any one of the following criteria or both: • **Start Date and End Date**: Filters the recordings used between these two dates. • **Event Type**: Filters the recordings based on the type of use.
Clear Filter	Use the button to clear the filter.

Related links

Media Manager on page 625

Chapter 49: Centralized Media Manager Audit Trail

Applications > **Centralized Media Manager Audit Trail**

This menu is available on subscription mode system's configured to use Centralized Media Manager as their archiving solution for call recordings.

See Centralized Media Manager on page 708.

The menu allows the audit trail of activity to be viewed.

Name	Description
Search on "User Name"	The Search text box to search the audit records of a User. Type the User Name to search the users activities in the recording library.
User Name	The name of the user who used the recording.
Timestamp	The time when the recording was used.
User Action	The type of user action on a recording. This specifies whether a recording was replayed, downloaded, deleted, or searched.
Details	The details of a recording such as owner of the recording, media name, calling party name, and so on.
Start Date	The date and time after which the event has occurred. Use the calendar to select the date and the adjacent drop-down menu to specify the time.
End Date	The date and time before which the event has occurred. Use the calendar to select the date and the adjacent drop-down menu to specify the time.
Event Type	The type of events you want to view. IP Office Media Manager keeps track of the following type of operation on the recordings: • **Delete**: Displays the recordings that are deleted. • **Download**: Displays the recordings that are downloaded. • **Replay**: Displays the recordings that are replayed. • **Search**: Displays the recordings that are searched.

Table continues…

Name	Description
Export	The option to export the filtered audit results as a zipped `.CSV` file on your computer. The file contains four columns with the following information: • **User Name** • **Timestamp** • **User Action** • **Details**

Filter

Button	Description
Apply Filter	Use the button to refine your search. You can filter your search based on any one of the following criteria or both: • **Start Date and End Date**: Filters the recordings used between these two dates. • **Event Type**: Filters the recordings based on the type of use.
Clear Filter	Use the button to clear the filter.

Chapter 50: Centralized Media Manager Recordings

Applications > **Media Manager** > **Centralized Media Manager Recordings**

This menu allows system administrators to view and manage call recordings. Access to call recordings for individual users should be configured through their web self-administration settings.

Name	Description
Call Date	The date of the call.
Length	The duration of the recording.
Parties	The users that participated in a conference call.
Call Direction	The field indicates whether the call was Internal, Incoming, or Outgoing.
Agents	The agents involved in the call.
Owner	The owner of the recording. Each recording has an owner; the owner is the number of the extension that recorded the call. Any one of the following can be an owner: • Calling party extension • Called party extension • Hunt group extension • A line number • An account code • An agent extension
Targets	The phone numbers of the recipients of the call.
Skills	The skill set of the agent involved in the call.
Call ID	The unique identification number associated with the call recording.

Filter

Name	Description
Recording Range (Date and Time)	The date and time range between which the call was recorded. Use the calendars to select the dates and the adjacent drop-down menus to specify the time.

Table continues…

Name	Description
Recording Length	The length of the recording. Select one of the signs and enter the time in seconds. The available signs are: • **=** Equal to the recording length you have specified. • **<** Less than the recording length you have specified. • **>** Greater than the recording length you have specified. • **>=** Greater than or equal to the recording length you have specified. • **<=** Less than or equal to the recording length you have specified.
Call Direction	The direction of the call, that is, whether the call is Internal, Incoming, or Outgoing. Use the drop-down menu to select a Filter criterion.
Parties	The parties involved in the call. Type the names of the parties. For more than one party, type the names separated by a comma.
Agents	The agents involved in the call. Type the names of the agents. For more than one agent, type the names of agents separated by a comma.
Target Number	The phone number of the recipient of the call. Type the target number.
Skills	The skill set of the agent involved in the call.
Call ID	The unique identification number associated with the call recording.

Button	Description
Apply Filter	Click to apply the filter. All the recordings matching your search criteria are displayed on the right pane.
Show All	The system displays all the recordings on the right pane.
Delete	Use the button to delete the selected recordings. You can select one or more recording using the check boxes corresponding to the recordings.
Download	Use the button to download multiple recordings to your computer. 1. Select the recordings and click the **Download** button. 2. Type a password to protect the recordings. 3. You browser downloads the selected recordings as a zipped file.

Part 7: Backup

Chapter 51: Backup and Restore

This chapter looks at how the web manager menus can be used to configure backup and restore operation between servers.

- If the IP Office server hard disk has sufficient capacity, you can use it to receive backups from other IP Office servers. However, this is not a suitable solution for its own backups. Therefore, the recommendation is to backup to another IP Office server.
- Within a primary/secondary server pair, you can configure reciprocal backups.
- The preferred option is a separate backup server. This can be done by installing an IP Office Application server with a sufficiently large hard disk (see Disk space required for backups on page 641) and no services (Voicemail Pro and Avaya one-X Portal) enabled.

Warning:

- Backup/restore is not supported between different server software release levels. Any exceptions are specifically documented in software release notes and migration documents.
- You cannot restore data to a server unless either the IP Address or the system id (LAN1 MAC address) match the server from which it was backed up.
- Backup and restore action must only be performed using servers inside a secure, trusted network.

Related links

Backup and restore policy on page 639
Backup and restore protocols on page 640
Enabling HTTP backup support on page 640
Disk space required for backups on page 641
Checking the backup server's backup quota on page 642
Backup data sets on page 642
Creating a remote server connection on page 644
Backing up a server/servers on page 644
Restoring from the backup server on page 645
Restoring a failed server on page 646

Backup and restore policy

It is essential to implement a comprehensive, robust and secure backup policy as part of a Business Continuity plan before any failure or other data restoration requirement. It is not possible to define a single approach that would meet all possible customer needs. Each installation should be assessed and an backup policy implemented. .

Backup Key Information

The backup process supported by web manager only includes specific data, see Backup data sets on page 642. There is key information which, though included in the backup data, should also be recorded separately in case it is necessary to rebuild a failed sever:

- The ignition settings for each server should be recorded. For example, IP address and host name settings, server role, etc. These details may be required if a full reinstallation of the server becomes necessary before any data restoration operation.

In addition, the following are not included in the web manager backup processes and so must be backed up using other manual processes.

- Copies of any PLDS license key files used by the system.
- If using web manager to load custom voicemail prompts, copies of those prompt files.
- Copies of any custom phone settings files plus phone screen saver and background images.

Backup Schedule

In addition to performing backups before major system changes such as an software upgrade, you must consider having a regular backup schedule.

- Periodic configuration backup for every IP Office.
- Periodic configuration backup for one X Portal – Server Edition Primary server and Application Server only
- Periodic configuration backup for Voicemail Pro – Server Edition Primary server only
- Periodic voice mailbox and recording data backup – Server Edition Primary server only
- The period and number of unique instances selected should reflect the frequency of change, the consequence due to data loss, and the storage capacity of the backup data server. It should also be bourne in mind that the backup server used will only retain up to 14 backups, after which any further backup will cause the automatic deletion of the oldest previous backup.
- The timing of backup operation: This should be done when little or no traffic is present on the target system(s), but the backup process itself is not service-affecting.

Additional Backup Options

This documentation only looks at the backup/restore process provided through the server's own web manager menus. The IP Office Manager and Voicemail Pro client application also provide methods for backing up the current IP Office service configuration and the voicemail configuration/ mailbox contents respectively. Therefore also consider:

- Manual backup of the IP Office service configurations before major configuration changes.
- Manual backup of the Voicemail Pro before major configuration changes.

Related links

Backup and Restore on page 638

Backup and restore protocols

Backup and restore is only supported using another IP Office server as the backup server. If necessary, an IP Office Application Server can be installed without enabling the Voicemail Pro and one-X Portal for IP Office services on that server.

Warning:

- Backup and restore action must only be performed using servers inside a secure, trusted network.

The server being backed up requires a remote server connection to the backup server. That connection is configured with the settings below (see Creating a remote server connection on page 644). For a set of networked servers, the connection from the primary server is used for all the servers.

Protocol	Port	Path	User Name/ Password	Notes
HTTPS	5443	`/avaya/backup`	none	HTTPS backup is enabled by default.
HTTP	8000	`/avaya/backup`	none	HTTP backup is disabled by default. To enable it on the backup server, see Enabling HTTP backup support.
SFTP	22	`/var/www/html/avaya/backup`	Administrator account.	–

Related links

Backup and Restore on page 638

Enabling HTTP backup support

By default, HTTP support for backup/restore is disabled. You can enable it using the following process on the backup server.

Security alert:

- Backup and restore action must only be performed using servers inside a secure, trusted network.

Enabling HTTP Backup Support on the Backup Server

1. Login to the web manager menus of the backup server.
2. Select the servers **Platform View** option.

3. Within the platform view menus, select **Settings** > **System** > **HTTP Server**.
4. Select the **Enable HTTP file store for backup/restore** option and click **Save**.

Related links

Backup and Restore on page 638

Disk space required for backups

The space required for a backup is highly variable. It depends on the number of servers includes in the backup and the data sets selected. However, the largest and most significant backup is that required for voicemail.

The following tables show the potential space required for a worst case full backup. That is, one that assumes all the users have used their voicemail mailbox and other facilities to their maximum capacity.

The minimum disk size column indicates the disk hard disk size required to have a sufficiently large backup quota (see above) for at least one maximum full backup.

Backup for a Sever Edition Network

Users	Maximum Full backup	Minimum Backup Server Disk Size
100	35GB	160GB
750	78GB	214GB
1500	127GB	275GB
2000	158GB	320GB
2500	189GB	360GB

Backup for an IP Office Application Server/UCM

Users	Maximum Full backup	Minimum Backup Server Disk Size
20	30GB	160GB
50	32GB	160GB
100	34GB	160GB
150	37GB	165GB

Related links

Backup and Restore on page 638

Checking the backup server's backup quota

Backup is supported to a server with a hard disk of 160GB or larger. The actual portion of that space, the backup quota, available for backup usage can be checked using the process below. On servers with a smaller hard disk, no backup quota is supported.

Estimating the Backup Quota

The approximate space that will be allocated for the backup quota can be calculated as follows:

- Backup Quota = (0.8 x Hard Disk Capacity) – 92GB if the Hard Disk Capacity is greater than 160GB, otherwise zero.
  - The capacities are all approximate. The quoted disk capacity from a disk manufacturer or a virtual server platform will differ from the capacity reported by the operating system.
  - For example: For a 500GB hard disk, the backup quota is approximately 308GB.

Checking the Backup Server's Backup Quota

Once a server is installed, the actual space allocated for backups can be checked as follows:

1. Login to the backup server's web manager menus.
2. Click and select **Platform View**.
3. On the **System** tab, note the **Quota available for backup data** value. Note this is the total space usable for backups, it does not account for the space already used by any existing backups.
4. Click **Solution** to exit the platform view.

Related links

Backup and Restore on page 638

Backup data sets

Each backup can include multiple selected servers. Within that backup a number of different data sets can be selected for inclusion in the backup.

The table summarizes the data included in the different backup data sets. Some data sets are greyed out if the related service is not running on one of the servers included in the backup.

When performing a restore it is also possible to select which servers and which data sets are included in the restore operation.

Data Set	Options	Contents
IP Office Sets	**IP Office Configuration**	When selected for Linux-based IP Office servers: • Server Settings • Web Management Settings • IP Office Service Configuration • IP Office Security Settings • DHCP Allocations • Call logs When selected for IP500 V2 Expansion systems: • IP Office Configuration • IP Office Security Settings • DHCP Allocations • Call logs
one-X Portal Sets	**one-X Portal Configuration**	one-X Portal server settings
Voicemail Pro Set	**Voicemail Pro Configuration**	• Voicemail Pro server preferences • Call flows
	Messages & Recordings	• Voicemail mailbox contents
	Voicemail Pro Full	• Voicemail Pro server preferences • Call flows • Mailbox contents including greetings, announcements and name prompts. Note: This does not include any custom prompts from the Web Manager customer prompts folder. Separate manual copies of those prompts must be kept.
	Selective Voicemail Users	This option backups a group of preselected mailboxes. The mailbox group is specified through **Applications** > **Voicemail pro — System Preferences** > **User Group**.
WebLM Sets	**WebLM Configuration**	Note that this data set does not include the license file being used by the server. A separate manual copy of any license file uploaded to the system should be retained.
WebRTC Sets	**WebRTC Configuration**	
Media Manager Sets	**Media Manager Configuration**	This is the configuration of the Media Manager service only. It does not include the call recordings and other data stored on the additional hard drive used for Media Manager.

Related links

Backup and Restore on page 638

Creating a remote server connection

Once the backup server has been configured, a remote server connection is required on the server to be backed up. In a network of servers, the remote connection s defined on the primary server.

Procedure

1. In the Web Manager menu bar, click **Solution**.
2. Click **Solution Settings** and select **Remote Server**.
3. Click **Add Remote Server**.
4. Enter a name that identifies the connections use.
5. Set the **Protocol** to **HTTPS**, **HTTP** or **SFTP** as required.
   - These are the only protocols supported for backup/restore operations.
   - **HTTP** is only supported if the backup server has had HTTP enabled. See Enabling HTTP backup support on page 640.
6. Set the **Port** to match the selected protocol. The default ports are not necessarily correct.
   - For **HTTPS**, set the port to 5443.
   - For **HTTP**, set the port to 8000.
   - For **SFTP**, set the port to 22.
7. Set the **Remote Path** to `/avaya/backup`.
8. For **HTTP**/**HTTPS**, no **User Name** or **Password** details are required. For SFTP, use the details of a Web Manager administrator account.
9. Click **Save**.
10. The new remote server connection is now shown in the list of remote servers. It can now be selected for backup and restore actions.

Related links

Backup and Restore on page 638

Backing up a server/servers

The system backs up the configuration of the server, application and user data in a single file set. You can use this backup file to restore the server or a failed server upgrade. The system backs up the configuration of the application to a local drive, in a predefined directory. You can take a backup of the primary server on a remote file server, which can optionally be the secondary server.

Before you begin

- Create a remote server connection for the backup server. See Creating a remote server connection on page 644.

About this task

You can take a back up of the primary server on a remote file server using Web Manager:

Procedure

1. In the Web Manager menu bar, click **Solution**.
2. In the Solution page, select the servers that you want to backup.
3. Click **Actions** and select **Backup**.
4. Select which data sets you want to include in the backup. See Backup data sets on page 642 for details of the different sets contents.
5. In the **Backup Label** field, type a label for the backup.
6. In **Select Remote Server** drop down list, select the remote server that you have set.
7. To back up at a scheduled time:
    a. In **Select Remote Server** drop down list, select the remote server that you have set.
    b. Under **Schedule Options**, enable **Use Schedule**.
    c. In the **Select Schedule** list, select the schedule option that you created.
    d. Set a **Start Date** and a **Start Time**.
    e. To configure a recurring backup, set **Recurring Schedule** to **Yes** and then set the **Frequency** and **Day of Week**.
8. Click **OK**.
9. The progress of the backup process is shown on the **Solution** menu.

Related links

Backup and Restore on page 638

Restoring from the backup server

The following process is used to restore previously backed up data.

Warning:

- Backup/restore is not supported between different server software release levels. Any exceptions are specifically documented in software release notes and migration documents.
- You cannot restore data to a server unless either the IP Address or the system id (LAN1 MAC address) match the server from which it was backed up.

- Close any Voicemail Pro client before attempting a restore. The restore process requires the voicemail service to restart. That will not occur if the Voicemail Pro client is connected to the service and will lead to incorrect restoration of data.
- During the restore process, the services being restored are restarted. This will end any calls using those services.

Procedure

1. In the Web Manager menu bar, click **Solution**.
2. Select the servers onto which you want to restore data sets.
3. Click **Actions** and select **Restore**.
4. Select the **Remote Server** connection that points to the backup server.
5. Click **Get Restore Points**.
6. The system displays the backup data sets that it has for the selected servers.
7. Highlight the data sets that you want to restore.
8. Click **OK**.
9. The progress of the backup process is shown on the **Solution** menu.

Related links

Backup and Restore on page 638

Restoring a failed server

The backup data can be used to attempt to restore a server that has failed.

Procedure

1. Reinstall the original server software, ensuring that the same original IP address and host name settings are used.
2. Reignite the server back to its original role. If the server includes an additional hard drive containing call recordings for Media Manager, ensure that the option to reformat the additional drive is not selected during the server ignition.
3. Login to the server and complete its initial configuration.
4. If the server was part of a network, use the options within Manager to add it back into the network and ensure that the connections between the primary, secondary and expansions are all present.
5. At this stage, use the restore process (see Restoring from the backup server on page 645) to reload the original data.

Related links

Backup and Restore on page 638

Part 8: VMPro Auto Attendants

Chapter 52: Voicemail Pro Auto-Attendants

From IP Office R11.1 FP2, the system supports auto-attendants provided by Voicemail Pro but configured within IP Office Web Manager (these auto-attendants cannot be configured through IP Office Manager).

- This is separate from the auto-attendant services supported on IP500 V2 systems using embedded voicemail.

An auto-attendant consists of several greeting prompts that the callers hear and a set of definitions of what the system should do when the caller presses any particular telephone key. Once you have configured an auto-attendant, it can be used as the destination for incoming calls.

The system allows you to configure multiple auto-attendants:

- IP500 V2 systems support up to 40 auto-attendants.
- IP Office Server Edition and Select systems support up to 100 auto-attendants.

For each, you can configure which actions are performed when the caller presses a key 0 to 9, * and #.

Feature	Description
Greetings and Time Profiles	Each auto-attendant can use time profiles to control which of up to 3 greeting is played to a caller. This allows different greetings, such as “Good morning”, “Good afternoon” or ““Sorry, we’re closed at the moment”” to be played based on the day of the week, time of day or even specific dates.
The Menu Announcement	Following the currently active greeting (if any), the caller hears the menu announcement. This should list the auto-attendant actions that have been configured. For example “Press 1 for .., press 2 for ....”.
Actions	Separate actions can be defined for each of the standard telephone keys (0 to 9, * and #). Actions include transfer to a specified destination, transfer to another auto-attendant, transfer to an extension specified by the caller, etc.
Text-to-Speech (TTS)	For subscription mode systems, the greetings and menus used by the auto-attendants can be generated using text-to-speech. This provides consistency in the prompt voice used whilst be able to make rapid changes.
Automatic Speech Recognition (ASR)	For subscription mode systems, automatic speech recognition can be used to detect the caller's response to options provided by the auto-attendant.

Related links

Google TTS Prompt Language on page 650
Text-to-Speech (TTS) Prompts on page 650
Enabling Google Speech and the Default Voice on page 651
Auto-Attendant Fallback Options on page 652

Auto-Attendant Callflow on page 652
Auto-Attendant Consent Example on page 653

Google TTS Prompt Language

Whilst the auto-attendant greeting and announcement prompts are recorded in a language of your choice, some of the auto-attendant actions may play additional prompts provided by the system. In that case, the language used for those system provided prompts is determined in several ways.

System Type	Language Setting
Fixed Language	If the system's **Google Speech AI**, or the auto-attendant's/system conferences **Speech AI** is set to a specific language, that language is used for all the system and TTS prompts.
Call Locale Based Language	If the system's **Google Speech AI** language is set to **Off**, the language used for the auto-attendant's system prompts is determined from the locale associated with the call. • **Incoming Call Route Locale**: If the caller is external, the incoming call route locale is used if set. • **User Locale**: If the caller is internal, the user locale is used if set. • **System Locale**: If no user or incoming call route locale is set, the system locale is used unless overridden by a short code locale. • **Short Code Locale**: The short code locale is used, if set, if the call is routed to voicemail using the short code. This overrides the other locale settings.

Related links

Voicemail Pro Auto-Attendants on page 649

Text-to-Speech (TTS) Prompts

Subscription mode systems can use text-to-speech (TTS) generated prompts for a range of features. TTS is supported in a number of languages and with various voice choices, as shown in the table below.

Whenever the settings for a TTS prompt are changed, the next time the prompt is requested, including preview through the web administration menus, the resulting prompt is cached by the system as a local file. This removes the initial delay that can occur the first time a TTS prompt is played.

Language	Number of Voices	Genders
Arabic	3	Female and Male
Czech	1	Female only

Table continues…

Language	Number of Voices	Genders
Danish	1	Female only
Dutch	5	Female and Male
English (Australian)	4	Female and Male
English (United Kingdom)	4	Female and Male
English (United States)	6	Female and Male
Finnish	1	Female only
French (France)	4	Female and Male
French (Canada)	4	Female and Male
German	4	Female and Male
Greek	1	Female only
Hungarian	1	Female only
Italian	4	Female and Male
Japanese	4	Female and Male
Norwegian	5	Female and Male
Polish	5	Female and Male
Portuguese (Brazil)	1	Female only
Portuguese (Portugal)	4	Female and Male
Spanish	1	Female only
Swedish	1	Female only
Turkish	5	Female and Male

Related links

Voicemail Pro Auto-Attendants on page 649

Enabling Google Speech and the Default Voice

About this task

Subscription systems can use Google speech to provide text-to-speech prompts and automatic speech recognition. These can be used with auto-attendants and system conferences.

Note:

- When enabled, the Google TTS is used for all Voicemail Pro TTS functions, overriding any locally installed TTS service.

Procedure

1. Select **System** > **Voicemail**.
2. Enable **Google Speech AI**.

3. Select the default **Speech Language** and **Speech Voice** the system should use.
   - The choices are used as the system defaults. They can be overridden within each auto-attendant. The language can be overridden within Voicemail Pro call flows.
4. Save the updated settings.

Related links

Voicemail Pro Auto-Attendants on page 649
Managing Auto-Attendants (Voicemail Pro) on page 655

Auto-Attendant Fallback Options

Whilst auto-attendants are intended to let callers choose the required destination for their call themselves, there may be cases where this fails. For example, when the system does not detect any response from the caller or when it cannot match the response to any of its configured options.

There are a number of fallback routes that can be applied to calls in such scenarios:

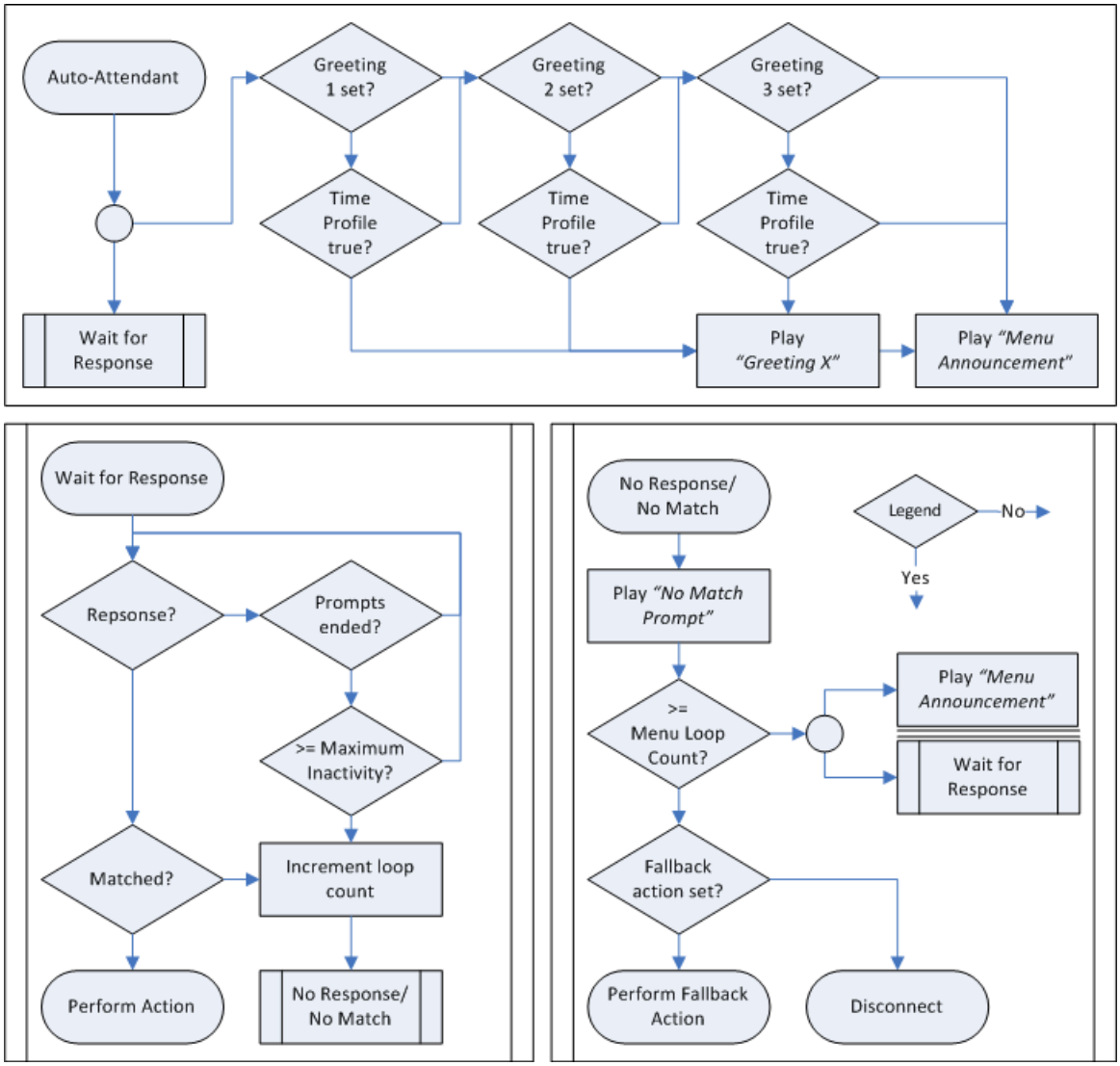
Stage	Fallback Route
Fallback Action	This option is used when the number of times the auto-attendant has waited for a valid response exceeds the **Menu Loop Count**. It can be configured to perform a chosen auto-attendant action. Otherwise, the system ends the call. • Note that is option may be overridden by the **Maximum Inactivity** timeout if it is reached first. See 'External Call Fallback' below.
Park and Page Fallback Number	If the caller selects a **Park & Page** action, their call is parked and waits to be unparked. If the call is still parked after a number of page attempts configured for the action, it is transferred to the action's configured **Fallback Number**.
External Call Fallback Extension	This is an incoming call route setting. For external calls routed to an auto-attendant from an incoming call route, it is used if for some reason the auto-attendant service is not available.

Related links

Voicemail Pro Auto-Attendants on page 649

Auto-Attendant Callflow

This flowchart is a simplified summary of the operation of a Voicemail Pro auto-attendant.



Related links

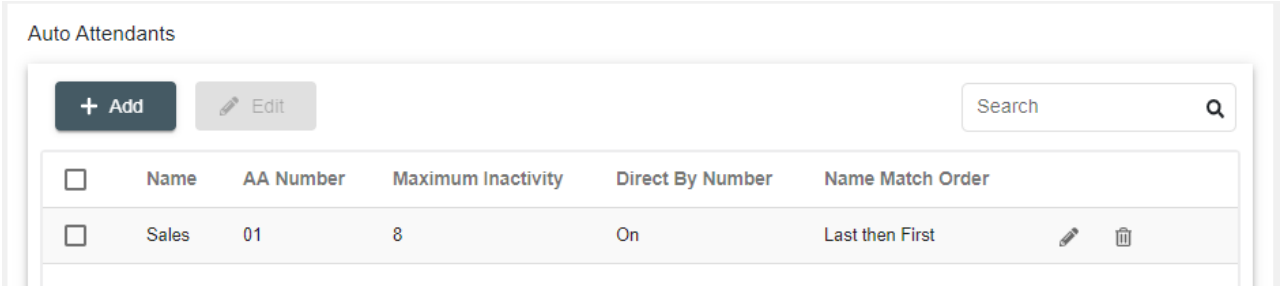
[Voicemail Pro Auto-Attendants](#) on page 649

Auto-Attendant Consent Example

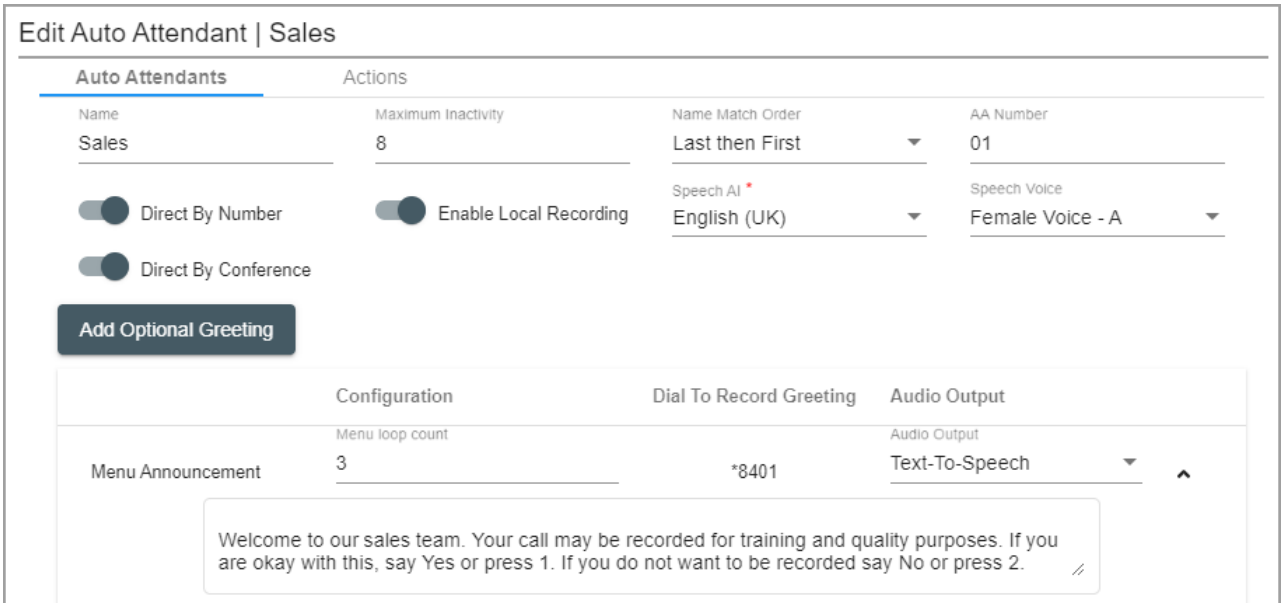
In the following example, the business wants to record external calls to its sales group using the group's automatic recording settings. However, it needs to provide those callers with an option to opt-out of being recorded and to have that choice recorded in the system's log files.

Two sales groups are configured. Each with the same members but only one with automatic call recording of external calls configured.

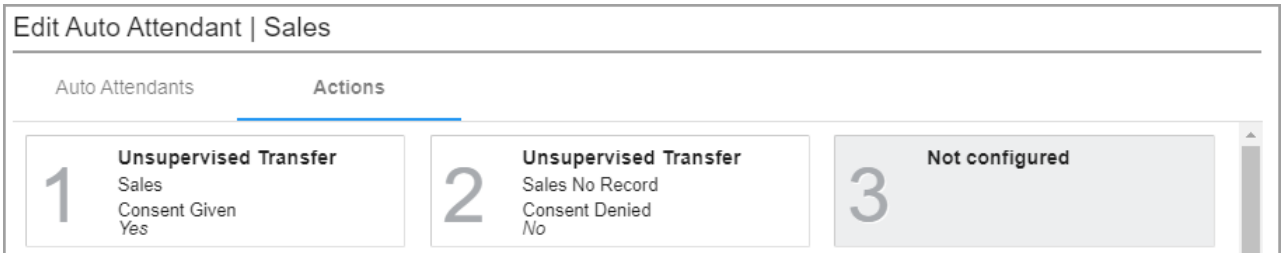
A Sales auto-attendant was added.



Within the auto-attendant, the menu announcement prompt informs the callers of the option to not be recorded.



The auto-attendant's actions then route the caller either to the group that has recording enabled or the group that does not support recording. The consent settings of the actions record the caller's choice in the system's log files.



Related links

Voicemail Pro Auto-Attendants on page 649

Chapter 53: Managing Auto-Attendants (Voicemail Pro)

Using IP Office Web Manager, the following processes can be used to create and manage the system's Voicemail Pro auto-attendants.

Related links

Enabling Google Speech and the Default Voice on page 651
Displaying the list of Auto-Attendants on page 656
Adding a new Auto-Attendant on page 656
Editing an Auto-Attendant on page 656
Deleting an Auto–Attendant on page 657
Deleting multiple Auto–Attendants on page 657

Enabling Google Speech and the Default Voice

About this task

Subscription systems can use Google speech to provide text-to-speech prompts and automatic speech recognition. These can be used with auto-attendants and system conferences.

Note:

- When enabled, the Google TTS is used for all Voicemail Pro TTS functions, overriding any locally installed TTS service.

Procedure

1. Select **System** > **Voicemail**.
2. Enable **Google Speech AI**.
3. Select the default **Speech Language** and **Speech Voice** the system should use.
   - The choices are used as the system defaults. They can be overridden within each auto-attendant. The language can be overridden within Voicemail Pro call flows.
4. Save the updated settings.

Related links

Voicemail Pro Auto-Attendants on page 649

Managing Auto-Attendants (Voicemail Pro) on page 655

Displaying the list of Auto-Attendants

Use the following process to display the list of auto-attendants configured on the system.

Procedure

1. From the menu bar, select **Call Management** and then **Auto Attendants**.
2. The list of auto–attendants already configured on the system is displayed.
   - You can filter the list, for more details see Filtering the list section.
   - You can search the list, for more details see Searching the list section.
   - You can sort the list, for more details see Sorting the list section.
   - To edit a record, click on the pencil icon adjacent to it.
   - To delete a record, click on the trash can icon adjacent to it.
   - To add a new record, click on the **+ Add** button at the top of the list.

Related links

Managing Auto-Attendants (Voicemail Pro) on page 655

Adding a new Auto-Attendant

Use the following process to add a new auto-attendant.

Procedure

1. Click **+ Add Attendant**.
2. Use the form to enter the auto-attendant details. See Voicemail Pro Auto-Attendant Settings on page 659.
3. When you have configured the auto-attendant as required, click **Create**.
4. The new auto-attendant is added to the list.

Related links

Managing Auto-Attendants (Voicemail Pro) on page 655

Editing an Auto-Attendant

Use the following process to edit an existing auto-attendant.

Procedure

1. Click the pencil icon next to the entry.
2. Change the auto–attendant settings as required. The categories shown on the left access different sets of settings. See Voicemail Pro Auto-Attendant Settings on page 659.
3. When completed, click **Update**.

Related links

Managing Auto-Attendants (Voicemail Pro) on page 655

Deleting an Auto–Attendant

Use the following process to delete an auto-attendant.

Important:

- Before deleting an entry, check that it is not being used as the destination for any other functions such as an auto-attendant action or incoming call route.

Procedure

1. Click on the trash can icon next to the entry to delete.
2. Click **Yes** to confirm the deletion.

Related links

Managing Auto-Attendants (Voicemail Pro) on page 655

Deleting multiple Auto–Attendants

- Before deleting an entry, check that it is not being used as the destination for any other functions such as an auto-attendant action or incoming call route.

Procedure

1. Select the check box to the left of each entry that you want to delete.
   - You can select multiple entries. Note that moving to another page clears the existing selections.
   - To select all the entries, click the check box in the header row. You are prompted whether to include all entries on the pages not currently being displayed.
2. Click **Delete**.
3. Click **Yes** to confirm the deletion.

Related links

Managing Auto-Attendants (Voicemail Pro) on page 655

Chapter 54: Voicemail Pro Auto-Attendant Settings

Call Management > **Auto Attendants** > **/+Add**

This section describes the auto–attendant settings used for subscription systems using Voicemail Pro. For auto-attendants provided by embedded voicemail on IP500 V2 systems, see Auto Attendant section.

These are split into two tabs.

Tab	Description
Auto Attendants	This tab defines the general settings of the auto-attendant and its greetings and announcements.
Action	This tab defines the functions provided by the individual telephone keys.

Related links

Auto-Attendant on page 659
Actions on page 663

Auto-Attendant

These settings are used to define the operation of the auto–attendant service whilst it waits for the caller to select an option from the configured actions.

For a visual summary of how these settings interact, see Auto-Attendant Callflow on page 652.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Auto-Attendant Settings

Field	Description
Name	Range = Up to 12 characters The name for the auto-attendant. Set a name that acts as a reminder of the auto-attendants role. The name is then also shown in other menus used to route calls to the auto-attendant.

Table continues…

Field	Description
AA Number	This number is automatically assigned by the system and cannot be changed. It is used in conjunction with short codes to access the auto–attendant service or to record greetings. See Recording Auto-Attendant Prompts Using Short Codes on page 679. • IP500 V2 systems support up to 40 auto-attendants. • IP Office Server Edition and Select systems support up to 100 auto-attendants.
Maximum Inactivity	Default = 8 seconds; Range = 1 to 20 seconds. This value sets how long the attendant should wait for a response from the caller after playing any current prompts. • If the caller responds, their response is checked for a match to a configured action without any further wait. • Note that the caller can respond whilst the prompts are playing. • If the timeout expires, the **Menu Loop Count** is checked to determine the next steps.
Name Match Order	Default = Last then First This setting sets the name order used for the **Dial By Name** action if used.
Direct By Number	Default = No This setting affects the operation keys set to the **Dial By Number** action. • **If enabled:** The caller's key press to select the action is included in the digits they dial for a extension match. For example, if menu key 2 is used for the action, a caller can dial 2 and then 01 for extension 201. • **If not enabled:** The caller's key press to select the action is not included in the digits they dial for extension match. For example, if menu key 2 is used for the action, a caller must dial 2 and then 201 for extension 201.
Direct By Conference	Default = No This setting affects the operation keys set to the **Dial By Conference** action. • **If enabled:** The caller's key press to select the action is included in the digits they dial for a conference match. For example, if menu key 3 is used for the action, a caller can dial 3 and then 01 for conference 301. • **If not enabled:** The caller's key press to select the action is not included in the digits they dial for a conference match. For example, if menu key 3is used for the action, a caller must dial 3 and then 301 for conference 301.
Enable Local Recording	Default = Yes When off, use of short codes to record auto-attendant prompts is blocked. The short codes can still be used to playback the greetings. See Recording Auto-Attendant Prompts Using Short Codes on page 679.

Table continues…

Field	Description
Speech AI	Default = Off This option is only available on subscription mode systems. It sets whether the auto-attendant supports text-to-speech and automatic speech recognition features. • When off, the auto-attendant does not support any text-to-speech and speech recognition features. - The language used for any prompts provided by the system is determined from the call settings. See Google TTS Prompt Language on page 650. • When set to a specific language, the auto-attendant supports text-to-speech and speech recognition features in that language. - It also uses that language for all system prompts it provides regardless of the locale call settings the system has associated with the call.
Speech Voice	This setting is available when **Speech AI** is set to a specific language. It allows selection of a particular voice used for any text-to-speech features. See Text-to-Speech (TTS) Prompts on page 650.

Greeting and Announcement Settings

When a caller reaches an auto-attendant, they first hear the attendant's current greeting (if any) and then the attendant's menu announcement.

- The greeting used is the first one (from up to 3 defined greetings) for which the greeting's associated time profile is currently active. This allows you to define greetings for different times of day (for example *"Good Morning"*, *"Good Afternoon"* and *"Sorry, we are currently closed"*) or different greetings for business and non-business days.
- The menu announcement should contain the instructions for the caller regarding the keys they can press and other actions.
- Each time a caller goes round the auto-attendant loop, they can respond (with key presses or speech) whilst any greeting and announcement menu prompt is being played.

Field	Description
Optional Greeting 1 **Optional Greeting 2** **Optional Greeting 3**	Up to 3 greetings can be defined using the **Add Greeting** button. • Each greeting requires an associated time profile. - **Time Profile:** Default = Off *(Greeting not used)*. • If **Off**, the greeting is not used. • The greeting is only used when defined by its associated time profile. • When multiple greetings are defined, the first one that has an active time profile, in the order 1 to 3, is used as the current greeting. • If no greetings is currently active according to its time profile, then no greeting is played. • If a greeting is no longer required, it can be deleted by clicking on the adjacent icon. • After playing any greeting, the system always then plays the menu announcement.

Table continues…

Field	Description
Menu Announcement	The menu announcement should contain the instructions for callers about the actions they can perform. For example; "*Press 1 for reception. Press 2 for sales, ...*" It is used as follows: • When a call first reaches the auto-attendant, it is played to the caller after whichever greeting is currently active. • If the **Menu Loop Count** is not zero, it is played again at the start of each repeat loop. • The caller can respond by pressing a key whilst the announcement is being played. On subscription mode systems, if **Speech AI** is enabled they can also respond by speaking whilst the announcement is played. • After the announcement is played, the auto-attendant waits for a response for the time set by the **Maximum Inactivity** setting.
Menu Loop Count	Default = 0 *(No Repeat)* This setting sets the number of times the auto-attendant will repeat the **Menu Announcement** and then wait for a valid response. If the caller does not respond or their response is not matched to an action: • If 0, the default, they hear the **No Match Prompt** prompt and the **Fallback Action** setting is used. • If non-zero but the number of repeat loops has not been reached, they hear the **No Match Prompt** and then the **Menu Announcement** again and the auto-attendant waits for a response again. • If non-zero and the number of repeat loops has been reached, they hear the **No Match Prompt** prompt and the **Fallback Action** setting is used.
No Match Prompt	This prompt is heard when the caller does not respond in time or if their response does not match a configured action. For example; "*Sorry, no response was recognized.*" • Note that this prompt is also heard by callers who are about to be redirected to the **Fallback Action**. Therefore a prompt like "*"Please try again"*" would not be appropriate.

The following settings are common to the menu announcement, greetings and error message. The greetings and announcements can be recorded from the phone, use an uploaded file or be provided by text-to-speech. Whichever method was last used or configured overrides any previous prompt.

Field	Description
Dial To Record Greeting	Default = Automatically assigned. Not changeable. This field indicates the short code that can be dialed in order to record the greeting from an internal extension. See Recording Auto-Attendant Prompts Using Short Codes on page 679.

Table continues…

Field	Description
Audio Output	Default = Audio File The field sets the current method used to provide the prompt used for the greeting or announcement. Clicking on the current value allows you to see its current settings and to change them or to change the recording method. • **Audio File (wav)** – Provide the prompt using a pre-recorded audio file. See Using Pre-Recorded Prompt Files on page 680. • **Text To Speech** – Provide the prompt using the text-to-speech service. This option is only available on subscription mode systems with **Speech AI** enabled and set to a specific language. See Recording Auto-Attendant Prompts Using Text-to-Speech on page 681.

Related links

Voicemail Pro Auto-Attendant Settings on page 659

Actions

This tab defines the actions available to callers dependent on which DTMF key they press or, on subscription mode systems, based on automatic speech recognition of keywords. To change an action, click on the appropriate button.

The **Fallback Action** action applied is the user does not make a recognized choice is configured separately through the **No Match Prompt** prompt settings.

These settings can be edited online. Changes to these settings do not require a reboot of the system.

Settings: Keys/Events

The following actions can be assigned to the selected keys.

Action	Description
0 to **9**, *, #	These keys correspond to the standard telephone dial pad key. Clicking on a key allows configuration of its settings.
Fax	If configured, the **Fax** option is used when the system detects fax tone.

Table continues…

Action	Description
Fallback Action	Default = Drop Call This option is used when the number of times the auto-attendant has waited for a valid response from the caller has exceeded the **Menu Loop Count**. It is preceded by the **No Match Prompt** and then the configured action is performed. All actions are supported except **Park & Page**, **Replay Menu Greeting**, **Speak By Name** and **Speak By Number** You can choose whether to mention this option in the **Menu Announcement**. For example, if set to transfer to your receptionist, add "... or wait to for our operator."
Menu Announcement	The menu announcement should contain the instructions for callers about the actions they can perform. For example; "*Press 1 for reception. Press 2 for sales, ...*" It is used as follows: • When a call first reaches the auto-attendant, it is played to the caller after whichever greeting is currently active. • If the **Menu Loop Count** is not zero, it is played again at the start of each repeat loop. • The caller can respond by pressing a key whilst the announcement is being played. On subscription mode systems, if **Speech AI** is enabled they can also respond by speaking whilst the announcement is played. • After the announcement is played, the auto-attendant waits for a response for the time set by the **Maximum Inactivity** setting.

Settings: Key Actions

Action	Description
Not configured	Perform no action.
Dial By Conference	Allow the caller to dial the conference ID they require. See Dial By Conference on page 666.
Dial By Name	Prompt the caller to dial the name of the user they require. See Dial By Name on page 667.
Dial By Number	Allow the caller to dial the extension number they require. See Dial By Number on page 669.
Leave Message	Redirect the caller a specified mailbox to leave a message. See Leave Message on page 670.
Supervised Transfer	Transfer the caller to the specified extension number. See Supervised Transfer on page 671.
Park & Page	Park the call and make an announcement to the a specified group. See Park & Page on page 672.
Replay Menu Greeting	Replay the auto-attendant's menu announcement. See Replay Menu on page 674.

Table continues…

Action	Description
Unsupervised Transfer	Transfers the caller to the specified extension number. See Unsupervised Transfer on page 677.
Transfer To Auto Attendant	Transfers the caller to another auto–attendant. See Transfer to Auto Attendant on page 678.
Speak By Name	Allow the caller to select from listed names using speech. See Speak By Name on page 675.
Speak By Number	Allow the caller to speak the extension number required. See Speak By Number on page 676.
Destination	The destination depends on the action: • **Leave Message**, **Supervised Transfer** and **Unsupervised Transfer** – Use the drop-down to select the target extension. • **Transfer To Auto Attendant** – Use the drop-down to select another existing auto-attendant.
Speech Recognition Keywords	This option is only available on subscription mode systems and when **Speech AI** is set to a specific language. It allows the action to be triggered by speech recognition of keywords. • The keywords must be unique. The same word cannot be used for another key. • Up to 3 keywords are supported per key, separated by commas. Note that using more keywords in total reduces the chances of a match. • Avoid using proper names. These are less likely to be matched as they may not match existing words in the speech recognition dictionaries used by Google. • Encourage matches by ensuring that the keywords are part of the announcements played to callers. For example, “Say whether you want Sales or Support” rather than “Say what department you want”.
Consent Directive	When a caller selects a particular action, the actions **Consent Directive** value is included in the system logs. These options allow you record whether the caller has indicated their consent to some action, for example call recording. See Auto-Attendant Consent Example on page 653. • **Consent Not Applicable** – Indicates that the caller has not been prompted to select whether they consent to call recording. • **Consent Given** – Indicates that the caller has been prompted for their consent and has consented. • **Consent Denied** – Indicates that the caller has been prompted for their consent and has not consented.

Related links

Voicemail Pro Auto-Attendant Settings on page 659

Chapter 55: Voicemail Pro Auto-Attendant Actions

The following sections provide more details on the different auto-attendant actions that can be assigned to the keys 0 to 9, # and *.

Related links

Dial By Conference on page 666
Dial By Name on page 667
Dial By Number on page 669
Leave Message on page 670
Supervised Transfer on page 671
Park & Page on page 672
Replay Menu on page 674
Speak By Name on page 675
Speak By Number on page 676
Unsupervised Transfer on page 677
Transfer to Auto Attendant on page 678

Dial By Conference

This action allows the caller to select the conference they want to join by dialing the conference ID. For example, “If you know the conference you want, dial the conference number.”.

The behavior of the action depends on the auto-attendant’s **Direct By Conference** setting.

- **If enabled:** The caller’s key press to select the action is included in the digits they dial for a conference match. For example, if menu key 3 is used for the action, a caller can dial 3 and then 01 for conference 301.
- **If not enabled:** The caller’s key press to select the action is not included in the digits they dial for a conference match. For example, if menu key 3is used for the action, a caller must dial 3 and then 301 for conference 301.

Action Settings

Key	Description
Speech Recognition Keywords	This option is only available on subscription mode systems and when **Speech AI** is set to a specific language. It allows the action to be triggered by speech recognition of keywords. • The keywords must be unique. The same word cannot be used for another key. • Up to 3 keywords are supported per key, separated by commas. Note that using more keywords in total reduces the chances of a match. • Avoid using proper names. These are less likely to be matched as they may not match existing words in the speech recognition dictionaries used by Google. • Encourage matches by ensuring that the keywords are part of the announcements played to callers. For example, “Say whether you want Sales or Support” rather than “Say what department you want”.
Consent Directive	When a caller selects a particular action, the actions **Consent Directive** value is included in the system logs. These options allow you record whether the caller has indicated their consent to some action, for example call recording. See Auto-Attendant Consent Example on page 653. • **Consent Not Applicable** – Indicates that the caller has not been prompted to select whether they consent to call recording. • **Consent Given** – Indicates that the caller has been prompted for their consent and has consented. • **Consent Denied** – Indicates that the caller has been prompted for their consent and has not consented.

Related links

Voicemail Pro Auto-Attendant Actions on page 666

Dial By Name

This action allows callers to dial the name that want and then hear a list of matches from which they can make a selection. For example, “To select from a list of names, press 1”.

Callers selecting this option are asked to dial the name of the user they require and then press **#**. They then hear a list of possible matches from which they can make a selection. The list uses the recording mailbox name prompts of matched users.

- The name matching uses the auto-attendant’s **Name Match Order** setting to either match against first or last names.
- The name used for matching is the user’s **Full Name** if set, otherwise their **Name** is used.

Users are excluded from matching if they:

- Are marked as **Ex Directory** in their user settings.
- Do not have a recorded mailbox name prompt. Normally user’s are asked to record a name when they first access their mailbox. See Recording User Name Prompts on page 681.

Dial By Name assumes that a standard ITU lettered dialing pad is being used.

How Dial By Name works

1. The caller is prompted to dial the name they require and then press **#**.
   - For example: Dialing **527** matches names starting with JAS (for example "Jason") and KAR (for example "Karl").
   - Callers can also press ***#** to exit without making a selection.
2. Depending on the number of matches found:
   - If no matches are found, the caller is given the option to retry.
   - If 10 or less matches are found, the matching mailbox name greetings are played as part of a list. For example, “”Press 1 for …, Press 2 for …, Press 3 for …””.
   - If more then 10 matches are found, the caller is prompted to either press **#** to hear the first 10 matches or to dial more characters to reduce the number of matches. If they select to play the list, after each set of 10 matches they can either make a selection or follow the prompts for other options.

Action Settings

Key	Description
Speech Recognition Keywords	This option is only available on subscription mode systems and when **Speech AI** is set to a specific language. It allows the action to be triggered by speech recognition of keywords. • The keywords must be unique. The same word cannot be used for another key. • Up to 3 keywords are supported per key, separated by commas. Note that using more keywords in total reduces the chances of a match. • Avoid using proper names. These are less likely to be matched as they may not match existing words in the speech recognition dictionaries used by Google. • Encourage matches by ensuring that the keywords are part of the announcements played to callers. For example, “Say whether you want Sales or Support” rather than “Say what department you want”.

Table continues…

Key	Description
Consent Directive	When a caller selects a particular action, the actions **Consent Directive** value is included in the system logs. These options allow you record whether the caller has indicated their consent to some action, for example call recording. See Auto-Attendant Consent Example on page 653. • **Consent Not Applicable** – Indicates that the caller has not been prompted to select whether they consent to call recording. • **Consent Given** – Indicates that the caller has been prompted for their consent and has consented. • **Consent Denied** – Indicates that the caller has been prompted for their consent and has not consented.

Related links

Voicemail Pro Auto-Attendant Actions on page 666

Dial By Number

This action allows the caller to select the extension they want by dialing the extension number. It can be used to allow callers to directly access user and group extension numbers.

For example, “If you know the extension you want, dial the extension number.” or “If you know the extension you want, press 1 followed by the extension number”.

The behavior of the action depends on the auto-attendant’s **Direct By Number** setting.

- **If enabled:** The caller’s key press to select the action is included in the digits they dial for a extension match. For example, if menu key 2 is used for the action, a caller can dial 2 and then 01 for extension 201.
- **If not enabled:** The caller’s key press to select the action is not included in the digits they dial for extension match. For example, if menu key 2 is used for the action, a caller must dial 2 and then 201 for extension 201.

Action Settings

Key	Description
Speech Recognition Keywords	This option is only available on subscription mode systems and when **Speech AI** is set to a specific language. It allows the action to be triggered by speech recognition of keywords. • The keywords must be unique. The same word cannot be used for another key. • Up to 3 keywords are supported per key, separated by commas. Note that using more keywords in total reduces the chances of a match. • Avoid using proper names. These are less likely to be matched as they may not match existing words in the speech recognition dictionaries used by Google. • Encourage matches by ensuring that the keywords are part of the announcements played to callers. For example, “Say whether you want Sales or Support” rather than “Say what department you want”.
Consent Directive	When a caller selects a particular action, the actions **Consent Directive** value is included in the system logs. These options allow you record whether the caller has indicated their consent to some action, for example call recording. See Auto-Attendant Consent Example on page 653. • **Consent Not Applicable** – Indicates that the caller has not been prompted to select whether they consent to call recording. • **Consent Given** – Indicates that the caller has been prompted for their consent and has consented. • **Consent Denied** – Indicates that the caller has been prompted for their consent and has not consented.

Related links

Voicemail Pro Auto-Attendant Actions on page 666

Leave Message

This action directs the caller to the mailbox of the specified extension (user or group). For example, “To leave a message, press 1”.

The caller hears the mailbox’s prompt and is then asked to leave a message.

Action Settings

Key	Description
Destination	The selected destination for the mailbox into which the message should be left. The feature can be used to leave messages in mailboxes where the user/group does not have **Voicemail On** enabled.

Table continues…

Key	Description
Speech Recognition Keywords	This option is only available on subscription mode systems and when **Speech AI** is set to a specific language. It allows the action to be triggered by speech recognition of keywords. • The keywords must be unique. The same word cannot be used for another key. • Up to 3 keywords are supported per key, separated by commas. Note that using more keywords in total reduces the chances of a match. • Avoid using proper names. These are less likely to be matched as they may not match existing words in the speech recognition dictionaries used by Google. • Encourage matches by ensuring that the keywords are part of the announcements played to callers. For example, “Say whether you want Sales or Support” rather than “Say what department you want”.
Consent Directive	When a caller selects a particular action, the actions **Consent Directive** value is included in the system logs. These options allow you record whether the caller has indicated their consent to some action, for example call recording. See Auto-Attendant Consent Example on page 653. • **Consent Not Applicable** – Indicates that the caller has not been prompted to select whether they consent to call recording. • **Consent Given** – Indicates that the caller has been prompted for their consent and has consented. • **Consent Denied** – Indicates that the caller has been prompted for their consent and has not consented.

Related links

Voicemail Pro Auto-Attendant Actions on page 666

Supervised Transfer

This action transfers the caller to the specified extension number (user or group). Once transferred, the caller is handled the same as a normal call to the same number. For example; queuing, following any forwards, etc.

Action Settings

Key	Description
Destination	The selected destination for the transfer. This action can be used with or without a set destination: • When no destination is set, the action behaves like **Dial By Number** above. • When a destination is set, the action waits for a connection before transferring the call. • Whilst waiting, the caller hears the system’s music on hold.

Table continues…

Key	Description
Speech Recognition Keywords	This option is only available on subscription mode systems and when **Speech AI** is set to a specific language. It allows the action to be triggered by speech recognition of keywords. • The keywords must be unique. The same word cannot be used for another key. • Up to 3 keywords are supported per key, separated by commas. Note that using more keywords in total reduces the chances of a match. • Avoid using proper names. These are less likely to be matched as they may not match existing words in the speech recognition dictionaries used by Google. • Encourage matches by ensuring that the keywords are part of the announcements played to callers. For example, “Say whether you want Sales or Support” rather than “Say what department you want”.
Consent Directive	When a caller selects a particular action, the actions **Consent Directive** value is included in the system logs. These options allow you record whether the caller has indicated their consent to some action, for example call recording. See Auto-Attendant Consent Example on page 653. • **Consent Not Applicable** – Indicates that the caller has not been prompted to select whether they consent to call recording. • **Consent Given** – Indicates that the caller has been prompted for their consent and has consented. • **Consent Denied** – Indicates that the caller has been prompted for their consent and has not consented.

Related links

Voicemail Pro Auto-Attendant Actions on page 666

Park & Page

This action parks the caller’ whilst the system performs a page to a specified user or group extension number. The page message includes the park slot number assigned to the parked call so that anyone who hears the page can unpark it.

- Whilst parked, the caller hears music on hold.
- The system uses the prompt you have configured for the button to announce that there is a parked call. It then states the park slot number which can be used to unpark the call.

Action Settings

Key	Description
Park Slot Prefix	The park slot prefix number. Maximum is 8 digits. A 0-9 will be added to this prefix to form a complete park slot ID for the parked call. The system the park slot prefix to create park slot for a call by adding an extra digit (0-9). For example, if you set 62080 as the prefix, the system uses a number between 620800 and 620809 to park calls.
Paging Number	Select the user or group which the system will page in order to announce the parked caller.
Retry Count	The number of page retries. The range is 0 to 5.
Retry Timeout	Default = 15 seconds. The time, in minutes and seconds, between paging retires. The value can be set in 15 second increments up to a maximum of 5 minutes. The default is 15 seconds.
Fallback Number	The extension number to which the park called should be presented if, after the final page and retry timeout, the call is still parked.
Speech Recognition Keywords	This option is only available on subscription mode systems and when **Speech AI** is set to a specific language. It allows the action to be triggered by speech recognition of keywords. • The keywords must be unique. The same word cannot be used for another key. • Up to 3 keywords are supported per key, separated by commas. Note that using more keywords in total reduces the chances of a match. • Avoid using proper names. These are less likely to be matched as they may not match existing words in the speech recognition dictionaries used by Google. • Encourage matches by ensuring that the keywords are part of the announcements played to callers. For example, “Say whether you want Sales or Support” rather than “Say what department you want”.
Consent Directive	When a caller selects a particular action, the actions **Consent Directive** value is included in the system logs. These options allow you record whether the caller has indicated their consent to some action, for example call recording. See Auto-Attendant Consent Example on page 653. • **Consent Not Applicable** – Indicates that the caller has not been prompted to select whether they consent to call recording. • **Consent Given** – Indicates that the caller has been prompted for their consent and has consented. • **Consent Denied** – Indicates that the caller has been prompted for their consent and has not consented.

Field	Description
Dial To Record Greeting	Default = Automatically assigned. Not changeable. This field indicates the short code that can be dialed in order to record the greeting from an internal extension. See Recording Auto-Attendant Prompts Using Short Codes on page 679.
Audio Output	Default = Audio File The field sets the current method used to provide the prompt used for the greeting or announcement. Clicking on the current value allows you to see its current settings and to change them or to change the recording method. • **Audio File (wav)** – Provide the prompt using a pre-recorded audio file. See Using Pre-Recorded Prompt Files on page 680. • **Text To Speech** – Provide the prompt using the text-to-speech service. This option is only available on subscription mode systems with **Speech AI** enabled and set to a specific language. See Recording Auto-Attendant Prompts Using Text-to-Speech on page 681.

Related links

Voicemail Pro Auto-Attendant Actions on page 666

Replay Menu

This action replays the auto-attendants **Menu Announcement** recording. For example, “To hear the options again, press #”.

Replaying the greeting does not count as a loop for auto-attendant’s **Menu Loop Count**.

Action Settings

Key	Description
Speech Recognition Keywords	This option is only available on subscription mode systems and when **Speech AI** is set to a specific language. It allows the action to be triggered by speech recognition of keywords. • The keywords must be unique. The same word cannot be used for another key. • Up to 3 keywords are supported per key, separated by commas. Note that using more keywords in total reduces the chances of a match. • Avoid using proper names. These are less likely to be matched as they may not match existing words in the speech recognition dictionaries used by Google. • Encourage matches by ensuring that the keywords are part of the announcements played to callers. For example, “Say whether you want Sales or Support” rather than “Say what department you want”.

Table continues…

Key	Description
Consent Directive	When a caller selects a particular action, the actions **Consent Directive** value is included in the system logs. These options allow you record whether the caller has indicated their consent to some action, for example call recording. See Auto-Attendant Consent Example on page 653. • **Consent Not Applicable** – Indicates that the caller has not been prompted to select whether they consent to call recording. • **Consent Given** – Indicates that the caller has been prompted for their consent and has consented. • **Consent Denied** – Indicates that the caller has been prompted for their consent and has not consented.

Related links

Voicemail Pro Auto-Attendant Actions on page 666

Speak By Name

This action is only available on subscription systems and when **Speech AI** is set to a specific language (enabling support for speech recognition).

This action is similar to **Dial By Name**. However, when the caller is presented with a list of name matches, they can indicate their selection by speaking.

Action Settings

Key	Description
Speech Recognition Keywords	This option is only available on subscription mode systems and when **Speech AI** is set to a specific language. It allows the action to be triggered by speech recognition of keywords. • The keywords must be unique. The same word cannot be used for another key. • Up to 3 keywords are supported per key, separated by commas. Note that using more keywords in total reduces the chances of a match. • Avoid using proper names. These are less likely to be matched as they may not match existing words in the speech recognition dictionaries used by Google. • Encourage matches by ensuring that the keywords are part of the announcements played to callers. For example, “Say whether you want Sales or Support” rather than “Say what department you want”.

Table continues…

Key	Description
Consent Directive	When a caller selects a particular action, the actions **Consent Directive** value is included in the system logs. These options allow you record whether the caller has indicated their consent to some action, for example call recording. See Auto-Attendant Consent Example on page 653. • **Consent Not Applicable** – Indicates that the caller has not been prompted to select whether they consent to call recording. • **Consent Given** – Indicates that the caller has been prompted for their consent and has consented. • **Consent Denied** – Indicates that the caller has been prompted for their consent and has not consented.

Related links

Voicemail Pro Auto-Attendant Actions on page 666

Speak By Number

This action is only available on subscription systems and when **Speech AI** is set to a specific language (enabling support for speech recognition).

This action is similarly to **Dial By Number**. However, the caller can dial or speak the extension number that they require. Note that it does not use the **Direct By Number** setting.

Action Settings

Key	Description
Speech Recognition Keywords	This option is only available on subscription mode systems and when **Speech AI** is set to a specific language. It allows the action to be triggered by speech recognition of keywords. • The keywords must be unique. The same word cannot be used for another key. • Up to 3 keywords are supported per key, separated by commas. Note that using more keywords in total reduces the chances of a match. • Avoid using proper names. These are less likely to be matched as they may not match existing words in the speech recognition dictionaries used by Google. • Encourage matches by ensuring that the keywords are part of the announcements played to callers. For example, “Say whether you want Sales or Support” rather than “Say what department you want”.

Table continues…

Key	Description
Consent Directive	When a caller selects a particular action, the actions **Consent Directive** value is included in the system logs. These options allow you record whether the caller has indicated their consent to some action, for example call recording. See Auto-Attendant Consent Example on page 653. • **Consent Not Applicable** – Indicates that the caller has not been prompted to select whether they consent to call recording. • **Consent Given** – Indicates that the caller has been prompted for their consent and has consented. • **Consent Denied** – Indicates that the caller has been prompted for their consent and has not consented.

Related links

Voicemail Pro Auto-Attendant Actions on page 666

Unsupervised Transfer

This action transfers the caller to the specified extension number (user or group). Once transferred, the caller is handled the same as a normal call to the same number. For example; queuing, following any forwards, etc.

Action Settings

Key	Description
Destination	The selected destination for the transfer. Unlike the **Supervised Transfer** action, this action cannot be configured without a destination.
Speech Recognition Keywords	This option is only available on subscription mode systems and when **Speech AI** is set to a specific language. It allows the action to be triggered by speech recognition of keywords. • The keywords must be unique. The same word cannot be used for another key. • Up to 3 keywords are supported per key, separated by commas. Note that using more keywords in total reduces the chances of a match. • Avoid using proper names. These are less likely to be matched as they may not match existing words in the speech recognition dictionaries used by Google. • Encourage matches by ensuring that the keywords are part of the announcements played to callers. For example, “Say whether you want Sales or Support” rather than “Say what department you want”.

Related links

Voicemail Pro Auto-Attendant Actions on page 666

Transfer to Auto Attendant

This action transfers the caller to another auto-attendant. For example, ““For alternate options, press #””.

Up to 40 auto-attendants can be configured and linked.

Action Settings

Key	Description
Destination	The selected auto-attendant.
Speech Recognition Keywords	This option is only available on subscription mode systems and when **Speech AI** is set to a specific language. It allows the action to be triggered by speech recognition of keywords. • The keywords must be unique. The same word cannot be used for another key. • Up to 3 keywords are supported per key, separated by commas. Note that using more keywords in total reduces the chances of a match. • Avoid using proper names. These are less likely to be matched as they may not match existing words in the speech recognition dictionaries used by Google. • Encourage matches by ensuring that the keywords are part of the announcements played to callers. For example, “Say whether you want Sales or Support” rather than “Say what department you want”.
Consent Directive	When a caller selects a particular action, the actions **Consent Directive** value is included in the system logs. These options allow you record whether the caller has indicated their consent to some action, for example call recording. See Auto-Attendant Consent Example on page 653. • **Consent Not Applicable** – Indicates that the caller has not been prompted to select whether they consent to call recording. • **Consent Given** – Indicates that the caller has been prompted for their consent and has consented. • **Consent Denied** – Indicates that the caller has been prompted for their consent and has not consented.

Related links

Voicemail Pro Auto-Attendant Actions on page 666

Chapter 56: Recording Auto-Attendant Prompts (Voicemail Pro)

The prompts used by the auto-attendant can be provided through a number of methods.

Related links

Recording Auto-Attendant Prompts Using Short Codes on page 679
Using Pre-Recorded Prompt Files on page 680
Recording Auto-Attendant Prompts Using Text-to-Speech on page 681
Recording User Name Prompts on page 681

Recording Auto-Attendant Prompts Using Short Codes

The **Dial To Record Greeting** values shown in the auto-attendant menus indicates a short code which can be used to play and record the associated auto-attendant prompt.

- These short codes can be dialed from any internal extension.
- The short codes can only be used if the auto-attendants **Enable Local Recording** setting is enabled.
- Recording a prompt using this method overrides any previously uploaded audio file or TTS settings for the prompt.

Using a Short Code

When using the short codes, you will be prompted as follows:

- Press **1** to hear the current recorded prompt if any.
- Press **2** to record a new prompt.
  - After the tone, record the prompt. Note that the prompt must be at least 3 seconds in length.
  - Press **2** again to end recording.
- Press **3** to save the new prompt.

Short Codes List

- **Optional Greeting 1** – Dial **81* followed by the **AA Number** . For example, **8101* for the first auto-attendant.

- **Optional Greeting 2** – Dial **82* followed by the **AA Number**. For example, **8201*.
- **Optional Greeting 3** – Dial **83* followed by the **AA Number**. For example, **8301*.
- **Menu Announcement** – Dial **84* followed by the **AA Number**. For example, **8401*.
- **No Match Prompt** – Dial **87* followed by the **AA Number**. For example, **8701*.
- **Park & Page Prompts** – Dial **80* followed by the action key being used (0 to 9) and then the **AA Number**. For example, for a park & page action on button 2 of the first auto-attendant, dial *80201. These prompts are used as part of the page call made by the system.
  - For the * key, dial *8510 followed by the **AA Number**. For example, **851001* for the first auto-attendant.
  - For the # key, dial *8511 followed by the **AA Number**. For example, **851101*.

How are the Dialing Codes Configured?

The dialing codes use system short codes which are automatically added to the system configuration when the first auto-attendant is created. Editing or deleting those system short codes will affect the operation of the codes shown in the auto-attendant menus.

These short codes use the **Auto Attendant** feature.

Related links

Recording Auto-Attendant Prompts (Voicemail Pro) on page 679

Using Pre-Recorded Prompt Files

You can use pre-recorded audio files as prompts for the auto-attendant.

- Prompt file uploading is only supported when using IP Office Web Manager. It cannot be done from the IP Office Manager menu.
- The file must be a .wav file in Mono PCM 16-bit format, either 8, 16 or 22KHz. Maximum length 10 minutes.

To upload an audio file:

1. Note that uploading a file will override any previously recorded audio file or TTS setting.
2. For the greeting and menu announcement prompts, click on the **Audio Output** and select **Audio File (wav)**.
3. Click on **Upload** and select the recording file. Alternatively, drag and drop the file into the text box.
4. Click on **Upload**.
5. Use the playback controls to test the recording.

Related links

Recording Auto-Attendant Prompts (Voicemail Pro) on page 679

Recording Auto-Attendant Prompts Using Text-to-Speech

On subscription mode systems, Text-to-Speech (TTS) can be used to provide the auto-attendant greetings and menu announcement prompts.

- TTS prompts are only available when **Google Speech AI** is enabled. See Enabling Google Speech and the Default Voice on page 651.
- The language used for TTS prompts is set by the auto-attendant's **Speech AI** setting.
- The voice used is set by the auto-attendant's **Speech Voice** setting. See Text-to-Speech (TTS) Prompts on page 650.
- You can enter up to 250 words as a prompt.
- Commas are treated as a short pause, semi-colons as a long pause.
- If using IP Office Web Manager, you can preview the prompt by clicking on the icon. Note that there is a short delay whilst the new prompt is created and downloaded.
- Following any changes, once a prompt is played or previewed, it is cached by the system in order to remove any future playback delay.

To create a TTS prompt:

1. Note that configuring TTS will override any previously recorded audio file.
2. Click on the **Audio Output** and select **Text To Speech**.
3. Enter the required text into the text box.
   - Use a comma to add a short pause.
   - Use a period to add a long pause.
   - To add emphasis to a particular word, add _ underscores before and after the word.
4. The following steps are only supported using IP Office Web Manager. Click on the to preview the prompt.
   - There is a short delay the first time the prompt is created following any changes. The prompt file is then cached by the system for future use.
   - For long prompts, use the playback controls to select which part of the prompt is played.
5. Make any changes required to the text.

Related links

Recording Auto-Attendant Prompts (Voicemail Pro) on page 679

Recording User Name Prompts

The **Dial By Name** and **Speak By Name** features only include users who have recorded a mailbox name (and are not set as ex-directory). By default, users are asked to record a name when they first access their mailbox.

However, in some scenarios this may need to be done separately. The method for recording the user name depend on how they access their mailbox and the mode in which the voicemail service is running.

Visual Voice

If the user accesses voicemail mailbox using the visual voice menu on their phone, they can use the following process to record their name:

1. Access visual voice.
2. Scroll down to and select **Name**.
3. Record a name.
4. When happy with the recording, press **Select**.

Intuity Mailbox Mode

If the user access their voicemail mailbox using spoken prompts, for example by dialing *17, they can use the following process to record their name:

1. Access the mailbox prompts.
2. Press **5**.
3. Press **5** again.
4. The user will hear their current name recording, if any.
5. After the tone, record a name and press **1**.
6. The name is played again.
   - To accept the recording, press **#**.
   - To record the name again, press **1**.

IP Office Mailbox Mode

If the user access their voicemail mailbox using spoken prompts, for example by dialing *17, they can use the following process to record their name:

1. Access the mailbox prompts.
2. Press ***05** to select the option to record your name.
3. Press **1** to hear your current recording.
4. Press **2** to record your name. When prompted, speak your name. The maximum recorded length is 5 seconds.
5. Press **2** when you have finished recording your name.
6. Press **1** to listen to your new recording. Review the recording and select one of the following options:
   - To save the new recording: Press **3**.
   - To record your name again: Press **2**.

Related links

Recording Auto-Attendant Prompts (Voicemail Pro) on page 679

Chapter 57: Routing Calls to a Voicemail Pro Auto-Attendant

This section provides notes on the different methods by which calls can be directed to a Voicemail Pro auto-attendant.

Related links

Routing External Calls to an Auto-Attendant on page 683
Routing Internal Calls to an Auto-Attendant on page 683

Routing External Calls to an Auto-Attendant

Once an auto-attendant has been created, it becomes selectable as a destination in other menus, for example incoming call routes. This is shown by entries prefixed with **AA:** in the drop-down lists of selectable destinations.

Related links

Routing Calls to a Voicemail Pro Auto-Attendant on page 683

Routing Internal Calls to an Auto-Attendant

Typically auto-attendants are not used for handling internal calls. However, it can be useful:

- To test the operation of an auto-attendant whilst it is being configured.
- As a number to which users can transfer external caller's who have been misdirected.

Short Codes for Auto-Attendant Access

An internally dialable number to access an auto-attendant can be created using the **Auto Attendants** short code feature. For example:

- **99XX/Auto Attendant/"AA:"N* - This short code will allows calls to any auto-attendant using the **AA Number** when dialing. For example, *9901 for the first auto-attendant.
- **99/Auto Attendant/"AA:AutoAttend01"* - This short code allows calls to a specific auto-attendant using the auto-attendant **Name** setting.

Related links

Routing Calls to a Voicemail Pro Auto-Attendant on page 683

Part 9: Conferencing

Chapter 58: Conferencing

The system supports a range of conference call features.

Related links

Conference Types on page 686
Conference Participants on page 687
User Conference Controls on page 687
Conference Capacities on page 688
Conference ID Numbers on page 689
Conference Notes on page 689
Conference Phones on page 690
Context Sensitive Conferencing on page 691

Conference Types

The system supports conferences consisting of multiple internal and external parties.

Conference Type	Description
Ad-Hoc Conferences	An ad-hoc conference is one created by the system on the fly. For example, when a user with two calls in progress conferences those calls using their phone. For ad-hoc conferences, all internal users are treated as moderators. See Ad-Hoc Conferencing on page 694.
Meet–Me Conferences	A meet-me conference is one started using a specific fixed conference ID number. This allows the use of various features to route and place calls into specific meet-me conferences.
Personal Meet-Me Conference	Each user's own extension number is treated as their personal meet-me conference number. That user is the conference's only moderator. Other participants can join a personal meet-me conference at any time, however the audio conference only starts when the owner also joins. If the user's optional conference PIN has been configured, the system prompts other callers for the PIN when they try to access the personal meet-me conference. See Personal Meet-Me Conferences on page 696.

Table continues…

Conference Type	Description
System Meet-Me Conferences	System meet-me conferences are configured by system administrators. Each system conference has a fixed conference ID and appears in the list of available destinations for auto-attendant actions, DDI numbers, incoming call routes, etc. Each system conference can be configured with multiple moderators, separate PINs for moderators and other participants, etc. See System Conferences on page 700.

Related links

Conferencing on page 686

Conference Participants

The following terms are used for the different roles people can have within a conference.

- **Participant** – Any member of a conference.
- **Delegate** – Any participant of a conference who is not a moderator.
- **Moderator** – Moderators have extra functions. For example they can drop and mute other participants. Who is or can be a moderator depends on the conference type:
  - **Ad-Hoc Conferences** – Any internal participant is automatically also a moderator.
  - **Personal Meet-Me Conferences** – The conference owner is the only moderator.
  - **System Conferences** – A participant of a system conference can be become a moderator is either of 2 ways:
    - Specified internal users can be added to the conference's moderator list. Those users are automatically moderators.
    - If the optional moderator PIN is set, any caller who enters that PIN joins the conference as a moderator. This allows external callers to be moderators (though without ability to drop/mute other participants).
- **Owner** – Personal meet-me conferences are owned by the user with the same extension number as the conference ID. They are also automatically the conference's only moderator.

Related links

Conferencing on page 686

User Conference Controls

Internal users who join a conference may also have access to controls which allow them to mute/unmute other parties and to drop other parties. The range of controls will depend on the conference type and whether the user is a moderator or a delegate.

Phone Controls

Users with Avaya 1400, 1600, 9500, 9600 Series and J100 Series phones (except the J129) can view the list of conference participants. Using the list, they can access options to mute and drop themselves and other participants.

On these phones, programming **Conference Meet Me** buttons allows the user to receive indication of when a particular conference is in progress and to access that conference.

User Portal Controls

Users with access to the User Portal can display details of the access settings for their own personal meet-me conference and for any system conferences for which they have been added to the moderator list. They also receive notification when other participants have joined their personal meet-me conference and are waiting for them to join.

When they join any conference, the portal displays a list of participants and controls for muting/dropping participants.

one-X Portal

This application provides the user with a display of conference participant and controls to manage their conference participation. It can also provide the user with controls for scheduling conferences and sending invitations to other conference participants.

SoftConsole

This application display details of conferences in progress to assist with transferring callers into a conference. It also provides menus for starting two meet-me conferences.

Related links

Conferencing on page 686

Conference Capacities

For full details on system capacities, refer to Avaya IP Office™ Platform Guidelines: Capacity.

The following table summarizes the overall system capacity for conference calls and maximum participants in any individual conference call. This capacity limits apply to all conference types.

System Mode	Total Conference Participants	Maximum Conference Size
IP Office Server Edition	256	256
IP Office Select IP Office Subscription	512	256
IP500 V2	128	64

System Meet-Me Conferences

System meet-me conferences use the same resources as above. However, in addition there are limits on the number that can be configured.

	Maximum Configured
IP500 V2	30
Other networks	120

In an IP Office Server Edition/Select network, these conferences are hosted on the primary server. If a secondary server is present, that server will host the system conferences during primary server resilience.

Related links

Conferencing on page 686

Conference ID Numbers

Every conference is assigned a conference ID number. That number can be used with other features (short codes, programmable buttons) in order to join that conference.

- Ad-hoc conferences are automatically assigned a conference ID number when started. Each ad-hoc conference uses the first available ID from 100 upwards.
- Meet-me conferences use pre-set conference IDs set as follows:
  - Personal meet-me conferences use a conference ID that matches the extension number of the conference owner and moderator.
  - System meet-me conferences use the conference ID specified when the conference settings are configured.
    - It is advisable not to use conference ID's that are near the range that may be in use for ad-hoc conferences as above (100 plus). Once a conference ID is in use by an ad-hoc conference, it is no longer possible to join the conference using the various conference meet me features.

Related links

Conferencing on page 686

Conference Notes

Feature	Details
Other Uses of Conference Resources	System features such as call intrusion, call recording and silent monitoring all use conference resources for their operation. On IP500 V2 systems, each Embedded Voicemail call in progress also reduces the conference capacity.

Table continues…

Feature	Details
Automatically Ending Conferences	The behavior for the system automatically ending a conference varies as follows: • A conference remains active until the last extension or trunk with reliable disconnect leaves. Connections to voicemail or a trunk without reliable disconnect (for example an analog loop-start trunk) will not hold a conference open. • The **Drop External Only Impromptu Conference** setting controls whether a conference is automatically ended when the last internal party exits the conference.
Analog Trunk Restriction	In conferences that include external calls, only a maximum of two analog trunk calls are supported. This limit is not enforced by the system software.
Recording Conferences	If call recording is supported, conference calls can be recorded just like normal calls. Note however that recording is automatically stopped when a new party joins the conference and must be restarted manually. This is to stop parties being added to a conference after any "advice of recording" message has been played.
IP Trunks and Extensions	Conferencing is performed by services on the system's non-IP interface. Therefore a voice compression channel is required for each IP trunk or extension involved in the conference.
Call Routing	A short code routing calls into a conference can be used as an Incoming Call Route destination.
Conference Tones	The system provides conference tones. These will be either played when a party enters/leaves the conference or as a regularly repeated tone. This is controlled by the Conferencing Tone (**System | Telephony | Tones & Music**) option.

Related links

Conferencing on page 686

Conference Phones

The system does not restrict the type of phone that can be included in a conference call.

Feature	Details
Use Mute	When not speaking, use of the mute function helps prevent background noise from your location being added to the conference call. This is especially important if you are attempting to participate handsfree.
Handsfree Participation	While many Avaya telephones can be used fully handsfree during a call, that mode of operation is intended only for a single user, seated directly in front of the phone. Attempting to use a handsfree phones for multiple people to listen to and participate in a call will rarely yield good results. See below for details of conference phones supported by the system.

Table continues…

Feature	Details
Dedicated Conference Phones	To allow multiple people in one room to speak and listen to a conference call, the system supports the following conference phones: • B100 Conference Phones (B179 and B199). • Audio Conferencing Unit (ACU).
Group Listen	The **Group Listen** function can be used via a programmable button or short code. It allows the caller to be heard through a phones handsfree speaker while only being talked to via the phone's handset.

Related links

Conferencing on page 686

Context Sensitive Conferencing

On 1400, 1600, 9500, 9600 and J100 Series telephones there have been changes to the display and handling of calls put on hold pending transfer. For those phones there have also been changes to which calls are conferenced when a **Conference** button or **Conf** display option is pressed on the telephone.

- Previously, pressing **Conference** would put the user's current call and all held calls into a conference. That included any calls that had be put on hold pending transfer by pressing **Transfer**.
- The result of pressing **Conference** on the telephone now depends on which call is currently highlighted on the phone display and what other calls are held or held pending transfer.

Which call is highlighted on the display	Other condition (in priority order)	Result when Conference is pressed:	Calls Conferenced		
			Connected Call	Held Calls	Held Pending Transfer
Connected call	**No call held pending transfer**	Conferences the connected call and all held calls.	✓	✓	–
	Call held pending transfer	Conferences the connected call and the held pending transfer call. Any other held calls are unaffected.	✓	–	✓

Table continues…

Which call is highlighted on the display	Other condition (in priority order)	Result when Conference is pressed:	Calls Conferenced		
			Connected Call	Held Calls	Held Pending Transfer
Held call	**Connected call**	Conferences the held call and the connected call. Any other held calls including held pending transfer are unaffected.	✓	–	–
	Held pending transfer call	Conferences the held and held pending transfer call. All other held calls are unaffected.	–	–	✓
	Held calls	Conferences with all other held calls.	–	✓	–
Held pending transfer call	**Connected call**	Conferences the held pending transfer call to a connected call. Any other held calls are unaffected.	✓	–	✓
	Held calls	Conferences the call held pending transfer with all other held calls.	–	✓	✓

Note that this new behavior only applies to conferences being initiated from the telephone. The original behavior of conferencing all calls still applies if the conference function is initiated from elsewhere such as from an application like one-X Portal.

- **Changing which call is currently highlighted**

  On phones with a set of cursor keys (four cursor keys around an **OK** key), the up and down cursor key can be used to change the current highlighted call (or call appearance if idle). This can be done even whilst there is a currently connected call. On touchscreen phones, the cursor buttons on the right-hand edge of the screen can be used for the same purpose.

  The method of highlighting is:

- - **1400/1600 Series Telephones** - On these phones only details of a single call are shown on the display at any time. The displayed call is the currently highlighted call.
  - **9500/9600/J100 Series Telephones** - On most phones in these series, the background of the shading is changed for the currently selected call. The exceptions are 9611, 9621, 9641, J159 and J179 telephones where a yellow symbol is shown on the right of the highlighted call.

Related links

Conferencing on page 686

Chapter 59: Ad-Hoc Conferencing

An ad-hoc conference is one created by the system on the fly. For example, when a user with two calls in progress conferences those calls using their phone. For ad-hoc conferences, all internal users are treated as moderators.

Related links

Dropping External Party Only Conferences on page 694
Adding Callers to an Ad-Hoc Conference on page 694

Dropping External Party Only Conferences

About this task

It may be desirable to prevent ad-hoc conferences from continuing if there are no internal users involved. This can be enabled for the whole system.

Procedure

1. Select **System Settings**.
2. Click **System**.
3. Select **Drop External Only Impromptu Conference**.
   - If enabled, when the last remaining internal user exits the conference, the conference is ended regardless of whether it still includes other external parties
   - If disabled, the conference is only ended when the last party exits the conference.
4. Click **Update**.

Related links

Ad-Hoc Conferencing on page 694

Adding Callers to an Ad-Hoc Conference

The method of starting an ad-hoc conference depends on the particular phone or softphone being used. It will typically involve putting an existing call on hold, making an additional call and then

selecting a conference option. The same method can usually be used for adding additional parties to an existing conference.

If necessary, controls for starting and adding users to an ad-hoc conference can be created using short codes and programmable buttons. Note that when used to add a party to an existing conference, these controls also work with existing meet-me conferences.

Related links

Ad-Hoc Conferencing on page 694

Chapter 60: Personal Meet-Me Conferences

Each user's own extension number is treated as their personal meet-me conference number. That user is the conference's only moderator. Other participants can join a personal meet-me conference at any time, however the audio conference only starts when the owner also joins. If the user's optional conference PIN has been configured, the system prompts other callers for the PIN when they try to access the personal meet-me conference.

- Participants who join a personal meet-me conference before the owner, are put on hold until the owner joins. Whilst on-hold they hear repeated tones.
- If the user has a audio conference PIN set, callers joining the user's personal meet-me conference are prompted to enter that PIN.
- Personal and system meet-me features can create conferences that include only one or two parties. These are still conferences that are using resources from the system's conference capacity.

Related links

Setting a User's Personal Conference PIN on page 696
Routing Internal Callers to a Meet-Me Conference on page 697
Routing External Callers to a Meet Me Conference on page 697
Personal Meet-Me Conference Callflow on page 698

Setting a User's Personal Conference PIN

About this task

If the user has a audio conference PIN set, other callers attempting to joining their personal meet-me conference are prompted to enter that PIN.

- Putting an **L** before the PIN, disables the user's personal audio conference.

Procedure

1. From the menu bar, select **Call Management** and then **Users**.
2. Locate the user you want to edit and click the icon next to them.
3. On the **User** tab, select **Audio Conference PIN**.
4. Enter a numeric PIN code of up to 15 digits.
5. Click **Update**.

Related links

Personal Meet-Me Conferences on page 696

Routing Internal Callers to a Meet-Me Conference

Internal users can join personal meet–me and system conferences using short codes or a programmable button.

Using Short Codes

The **Conference Meet Me** short code feature can be used to create short codes that put the user into a meet me conference.

The default short code for this is `*66*N#` where `N` is the conference ID of the conference required.

- Internal users can also use the short codes to transfer callers into a conference.
- The same short codes can also be used by external callers to join the conference by setting the short code as the destination in features such as an auto-attendant transfer.
- For personal meet-me conferences, the short code can also specify a music source to use rather than tones if the conference owner has not already joined. System meet-me conferences use the conference's own separate **Hold Music** setting.

Using a Programmable Button

The **Conference Meet Me** button feature can be used to create a programmable button to join a personal meet–me or system conferences. The button can also be used to transfer other caller's into a conference.

- If the button is configured with a specific conference ID, the button also shows the status of the conference.
- If the button is configured without a conference ID, when pressed the user is prompted to enter the required conference ID.

This option is not supported on J139 and non-Avaya phones.

Related links

Personal Meet-Me Conferences on page 696

Routing External Callers to a Meet Me Conference

The same **Conference Meet Me** short codes used for internal callers (see Routing Internal Callers to a Meet-Me Conference on page 697) can also be used for external callers.

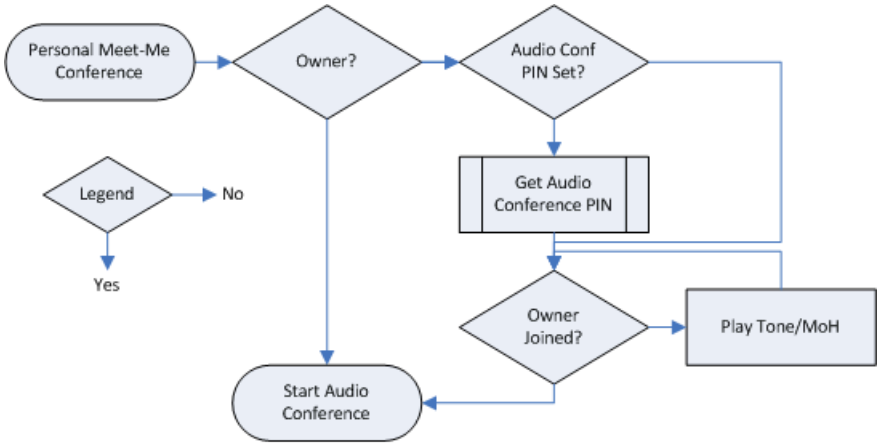
Related links

Personal Meet-Me Conferences on page 696

Personal Meet-Me Conference Callflow

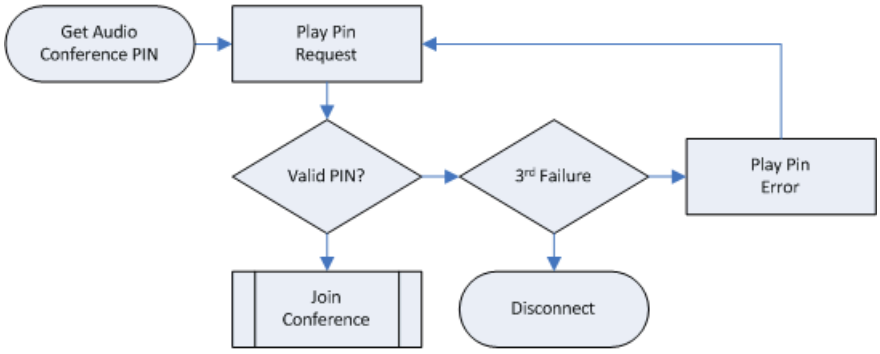
The following flowcharts provide a simplified callflow for a personal meet-me conference.

Personal Meet-Me Conference



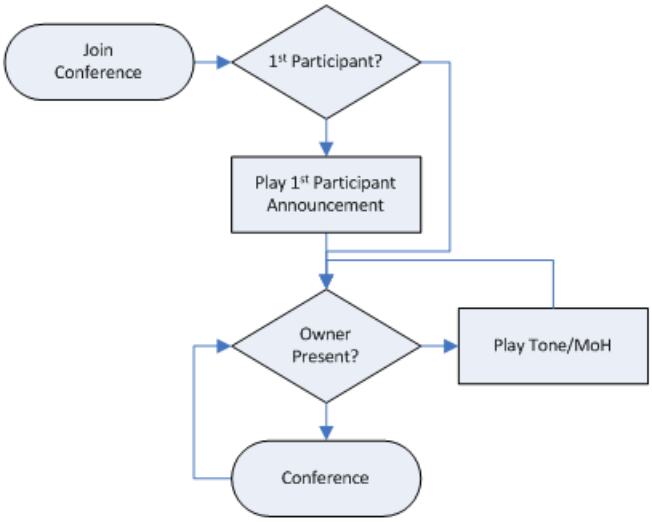
Get Owner's Audio Conference PIN

If the conference owner has an **Audio Conference PIN** set, other participants are required to enter that PIN in order to join the conference.



Join The Conference

Participants can join the conference ahead of the owner. However, if that is the case, they will hear an announcement that the conference will not start until the moderator joins followed by tones or music-on-hold. The conference starts once the owner also joins the conference.



If the owner subsequently leaves the conference, the other participants hear ones or music-on-hold again until the owner rejoins.

Related links

Personal Meet-Me Conferences on page 696

Chapter 61: System Conferences

System meet-me conferences provide:

- Optional participant PIN.
- Multiple optional moderators based on listed internal users and/or caller's who enter the optional moderator PIN.
- Automatic conference prompts for access control in per-conference selectable language.
- Recording per system conference.

System Conference Examples

The system conference features allow the configuration of various different types of conference:

Conference Type	Method
Simple Conference	A conference with no PIN codes, no moderators.
Simple Conference with Access Control	A simple conference with a PIN code required for entry but no moderators.
Moderated Conference	A conference which does not start until a listed moderator joins and ends when no moderator remains.
Moderated Conference with Access Control	As above but with a PIN code required for entry.
External Moderated Conference	Using a moderator PIN to allow external callers to assume the moderator role.

Related links

Adding a System Conference on page 700
Editing a System Conference on page 701
Deleting a System Conference on page 701
System Conference Settings on page 702
Routing External Calls to a System Conference on page 704
System Conference Callflows on page 705

Adding a System Conference

About this task

The number of system conferences that you can configure is limited as follows:

	Maximum Configured
IP500 V2	30
Other networks	120

This is in addition to the overall capacity limits for all conference types. See Conference Capacities on page 688.

Procedure

1. Select **Call Management** > **Conferences**.
2. Click **+ Add**.
3. Configure the system conference settings. See System Conference Settings on page 702.
4. Click **Save**.

Related links

System Conferences on page 700

Editing a System Conference

Procedure

1. Select **Call Management** > **Conferences**.
2. Click the pencil icon next to the entry.
3. Configure the system conference settings. See System Conference Settings on page 702.
4. Click **Save**.

Related links

System Conferences on page 700

Deleting a System Conference

About this task

- Before deleting an entry, check that it is not being used as the destination for any other functions such as an auto-attendant action or incoming call route.

Procedure

1. Select **Call Management** > **Conferences**.
2. Click on the trash can icon next to the entry to delete.

3. Click **Yes** to confirm the deletion.

Related links

System Conferences on page 700

System Conference Settings

Call Management > **Conferences** > **/+Add**

These settings are used to define the operation of a system meet-me conferences.

Field	Description
Conference ID	Range = Up to 15 digits. This ID is shown in the destination list for auto-attendant actions and incoming call routes. The ID can also be used with short code and programmable button features in order to access the conference. • Do not enter a number that matches a user's extension number. Doing so will override that user's personal meet-me conference facility. • It is advisable not to use conference ID's that are near the range that may be in use for ad-hoc conferences as above (100 plus). Once a conference ID is in use by an ad-hoc conference, it is no longer possible to join the conference using the various conference meet me features.
Name	This is a short name to help indicate the system conferences intended use. For example, "Sales Team".
Moderator List	Optional. Default = No moderators. List the internal users who are moderators for this system conference, up to a maximum of 8 moderators. When set: • The conference **Hold Music** is played to other participants when there is no moderator in the conference. • These user's do not need to enter a PIN in order to access the conference. • Listed users using the User Portal application can view the conference PIN details. In addition: • Other participants, including external participants, can become moderators by entering the **Moderator Pin** when they join the conference. • Conferences with no defined moderators (blank **Moderator List** and no **Moderator Pin**) start immediately any caller joins and can have recording started/stopped by any internal user.

Table continues…

Field	Description
Delegate Pin	Optional. Range = Up to 30 digits. If set, the system will prompt callers, other than those in the **Moderator List** list, to enter a PIN before it allows them to join the conference. The system allows 3 PIN entry attempts before disconnecting the caller.
Moderator Pin	Optional. Range = Up to 30 digits. If set, callers who enter this PIN rather than the **Delegate Pin** are added to the conference as a moderator. This allows moderators who are not in the **Moderator List** including external callers. Note however that external callers will not be able to access moderator controls other than starting/stopping the conference by their presence.
Hold Music	Default = **Tone** If the conference has been configured with moderators, this music is played to other participants who join the conference when no moderator is present. The music is also played if any present moderators leave the conference. • **Tone** – Play repeated system tones to participants whilst waiting for a conference moderator. • **System** – Use the system's default music-on-hold. This option is only shown in a music-on-hold file has been uploaded. • If other music sources have been configured, they can also be selected from the drop-down list. Before the hold music is played, participants will hear a prompt informing them of the reason for hearing the music.
Speech AI	Default = Same as system On subscription systems, this and other text-to-speech options are available if the **System | Voicemail** setting for **Google Speech AI** is enabled. • If set to **Same as System**, the settings of the **System | Voicemail** form are used for TTS prompts. • If set to **Custom**, the **Language** and **Voice** fields below can be used.
Language	Default = Matches the system locale. Set the language used for prompts provided by the system for the system conference.
Voice	Sets the voice to be used with the speech language. The number of voices available varies depending on the speech language selected.
Recording Type	Default = **Manual** Sets the method by which recording of the system conference is controlled: • **Manual** – Recording can be started/stopped by moderators. • **Private** – No recording allowed. • **Automatic** – Automatically start recording the conference when started. The recording can be stopped/restarted by moderators.

Table continues…

Field	Description
Recording Destination	Default = **Conference Mailbox** Sets the destination for system conference recordings. Note that the selected option may also affect the maximum recording length: • **Conference Mailbox** - Place calls into a standard group mailbox, using the conference ID as the mailbox number. Maximum recording length 60 minutes. Message waiting indication and visual voice access can be configured by adding **C**<*conference ID*> to a user's source numbers. • **Conference VRL** - Transfer the conference recordings to the systems VRL application (on subscription systems, set by the **System** > **System** > **Media Archival Solution** setting). Maximum recording length 5 hours.
Meeting Arrival Announcement	Default = Off If enabled, the system plays this prompt to callers before they join the conference. If conference PIN codes have been defined, it is played before the request to the caller to enter their PIN code. • **Audio Output** – Use an uploaded audio file. See .The file must be a .wav file in Mono PCM 16-bit format, either 8, 16 or 22KHz. Maximum length 10 minutes. To upload a file click on **Upload** and select the required file. Alternatively, click and drag the file onto the download box. • **Text-to-Speech** – Use a prompt generated using TTS. Up to 200 characters.

Related links

System Conferences on page 700

Routing External Calls to a System Conference

External callers can be routed to a conference using a number of methods:

- The conference ID appears as **Conf:**<*id*> in the **Destination** drop-down list for many functions:
  - From an **Incoming Call Route**, the **Destinations** drop-down includes system meet-me conferences configured on the system.
  - Through an auto-attendant, the configured conferences appear in the list of targets for **Unsupervised Transfer** actions.
- Using the **Dial By Conference** action, callers routed to an auto-attendant can dial the conference ID required.
- For other scenarios, the conference ID can be used as the number to which a call should be routed using the format *<ID>#. For example in the telephone number field of a short code.

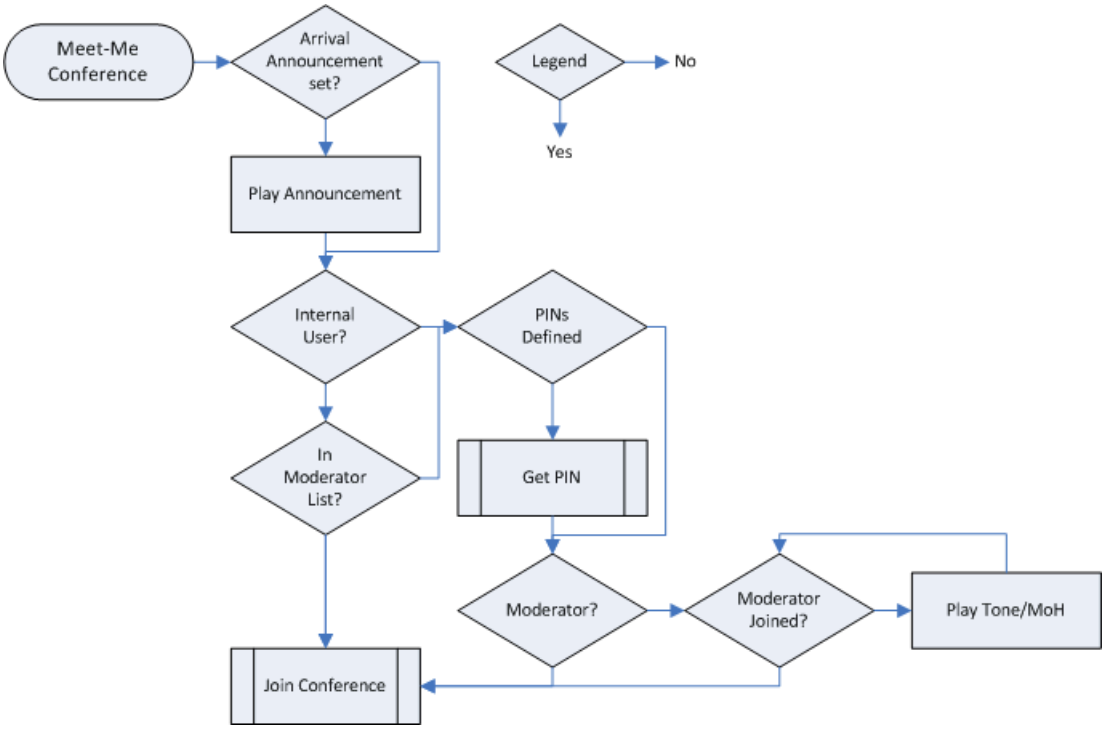
Related links

System Conferences on page 700

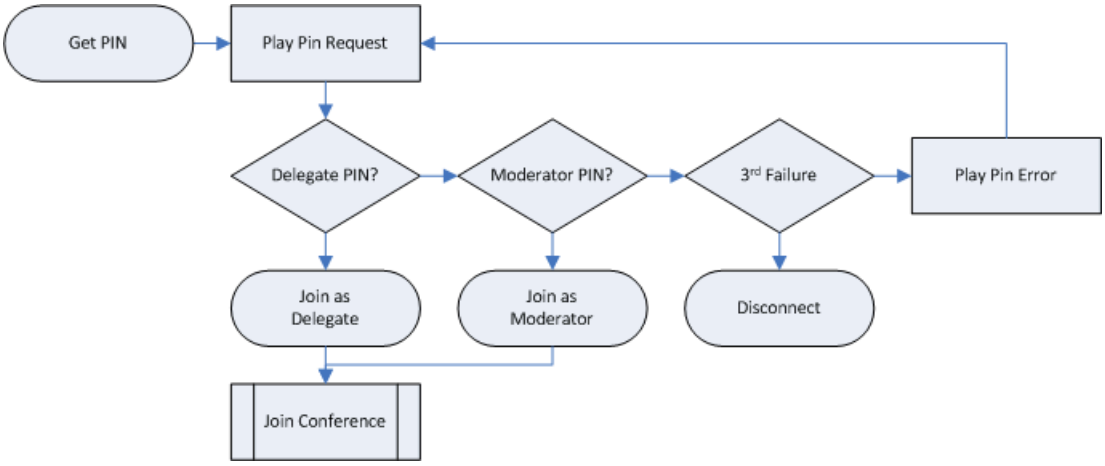
System Conference Callflows

The following flowcharts provide a simplified callflow for system meet-me conferences.

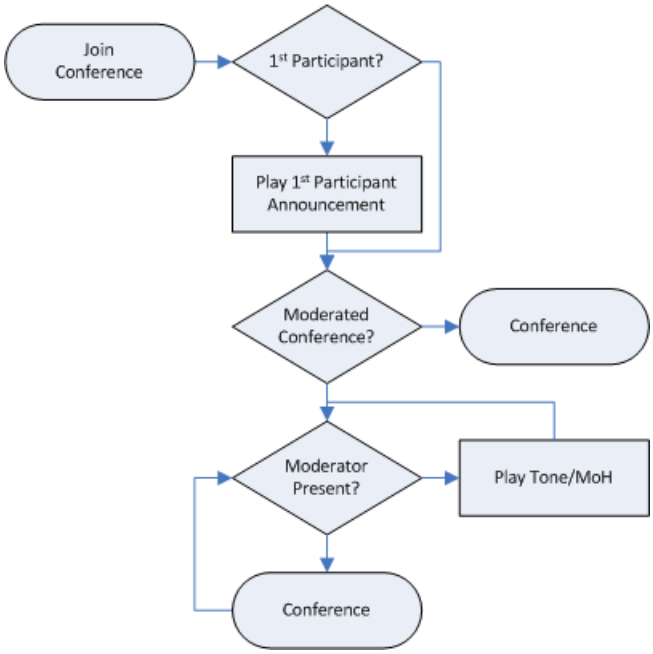
System Meet-Me Conference



Getting Conference PINs



Join the Conference



Related links

System Conferences on page 700

Part 10: Centralized Media Manager

Chapter 62: Centralized Media Manager

Centralized Media Manager is a cloud-based service supported for subscription mode IP Office systems. When supported by a system, the **Voice Recording Library** option becomes available in the IP Office configuration as a destination for manual and automatic call recording.

- **Centralized Media Manager** differs from **Local Media Manager** which runs on the same server as the Voicemail Pro service. For details of **Local Media Manager**, see the Administering Avaya IP Office™ Platform Media Manager manual.
- The **Subscription** menu shows if **Centralized Media Manager** is supported. See Subscription on page 447. The number of subscriptions controls the maximum number of supported recordings.
  1. 150,000
  2. 300,000
  3. 500,000
  4. 750,000
  5. 1,000,000
- **Centralized Media Manager** supports recording of up to 5 hours length.
- Centralized Media Manager automatically deletes each recording after a set number of days. By default that is 30 days. You can increase the retention period to up to 365 days.
  - For longer term storage, the copying of recordings to external Google storage can be configured. See Archiving Recordings to External Storage on page 719.
- Users can access the recording library through their user portal (see Configuring User Access to the Recording Library on page 710).
  - You can configure which users are able to access the library and which recordings they can access.
  - You can configure whether they can download recordings.
- You can access an audit trail that shows who has played and or downloaded recordings.
- If for any reason, connection between the customer system and **Centralized Media Manager** is not available, any new recordings waiting to be collected are deleted after 24-hours.

Related links

Select local or centralized Media Manager on page 709
Setting How Long Recordings are Kept on page 709
Configuring User Access to the Recording Library on page 710
Changing the Recording Source in the User Portal on page 711

Select local or centralized Media Manager

Use the following process to select which application the IP Office uses to store call recordings.

Procedure

1. Select **System Settings** and then **System**.
2. Select **Media Archival Solution** and select the source required:

Option	Description
Local Media Manager	Use the local Media Manager service running on the same server as the voicemail service. • For details of **Local Media Manager** configuration, see the Administering Avaya IP Office™ Platform Media Manager manual.
Centralized Media Manager	Use the centralized service provided by the cloud-based servers for subscription IP Office systems.

3. Click **Update**.

Related links

Centralized Media Manager on page 708

Setting How Long Recordings are Kept

Centralized Media Manager automatically deletes each recording after a set number of days. By default that is 30 days. You can increase the retention period to up to 365 days.

- For longer term storage, the copying of recordings to external Google storage can be configured. See Archiving Recordings to External Storage on page 719.

Procedure

1. Select **System Settings** and then **System**.
2. Select **Voicemail**.
3. Use the **Maximum Recording Retention (Days)** field to set how long recordings should be kept in the recording library before it is automatically deleted. It can be set to a value from 1 to 365 days.
4. Click **Update**.

Related links

Centralized Media Manager on page 708

Configuring User Access to the Recording Library

You can configure access to the voice recording library for individual users. This allows them to list and play recordings through their web browser using the User Portal application. Refer to the Using the IP Office User Portal user guide.

Procedure

1. Access the user's settings through **Call Management | Users**.
2. Select **Web Self-Administration**.
3. Select **Enable Media Manager Replay**.
4. Use the addition options to configure what recordings the user can access:

Name	Description
Enable Media Manager Replay	Default = Off. When enabled, the user can replay call recordings through web self-administration. • Note: For users where Media Manager is provided by a separate application server, recordings are viewed and accessed using the address of the application server rather than that of the IP Office system.
Replay All Recordings	If selected, the user can view and replay all recordings.
Replay Own Recordings	If selected, the user can view and replay their own call recordings. When enabled, the **Replay Recordings For Group** and **Replay Recordings For Others** options are also available.
Replay Recordings For Group	These menus allows the selection of groups for which the user is able to view and replay recordings.
Replay Recordings For Others	The field can be used to enter a list of numbers, separated by semi-colons, for which the user can view and playback recordings. Those numbers can be accounts codes, line numbers, user extensions and group extension numbers. The list can be 127 characters in length.
Download Recordings	If selected, the user is able to download recordings as a separate file. • Downloaded files are outside of the control of the system. Therefore, if you allow users to download files, it is your responsibility to ensure that they comply with local privacy and data protection laws regarding the use of those files.

5. Click **Update**.

Related links

Centralized Media Manager on page 708

Changing the Recording Source in the User Portal

Some systems may have previously used a local server and then switched to a cloud-based server. In that case they will have recordings stored both locally and centrally. In that case, using the process below in their user portal allows a user select from which source they are viewing stored recordings.

Procedure

1. Within the user portal application, click on the logged in user name top-right.
2. Click on **Media Retrieval Preference**.
3. The menu that appears indicates the current recordings source.
4. To change source, click on the current source and select the source required.

Preference	Description
Local Media Manager	Recordings are stored and managed by an application running locally on your system.
Centralized Media Manager	Recordings are stored and managed by an application running on cloud-based servers.

5. Click **Save**.

Related links

Centralized Media Manager on page 708

Chapter 63: Viewing Recordings

Through web manager you can access and manage all recordings in the recordings library.

- Access is controlled by the user rights of the service user account used to log in to web manager. The account must be a member of a rights group that includes **External** > **Media Manager Standard** or **External** > **Media Manager Administrator** permission.

Procedure

1. Click **Applications**.
2. Click **Voice Recordings Library**.
3. By default all recordings are listed. Use the filter settings to change the recordings listed. See Applying a Recording Filter on page 712.

Related links

Applying a Recording Filter on page 712
Playing Recordings on page 713
Downloading Recordings on page 714
Deleting Recordings on page 715
Archiving Recordings to the External Storage on page 715

Applying a Recording Filter

You can apply a filter to the recordings displayed. This allows you to focus on only particular recordings

Procedure

1. Display the recordings library. See Viewing Recordings on page 712.
2. To remove any existing filter settings, click **Show All**.
3. Enter the filter criteria that you want applied. You can use one or all of the following filter options. Any filter left blank is treated as matching all recordings.
   - **Recording Range (Date and Time)** – Select a start and end date and a start and end time for the recordings you want to see. Note that you need to set all 4 settings in order to apply a time and date filter. The values apply to the start of the recording.

- **Recording Length (sec)** – Select an operators and then the length in seconds. The operators are:
  - **<** - Only show calls shorter than the set length.
  - **>** - Only show calls longer than the set length.
  - **=** - Only show calls of exactly the set length.
- **Call Direction** – If set, only show **Internal**, **Incoming** or **Outgoing** calls.
- **Parties** – Only show recordings that involve any of the matching extension numbers as part of the call. You can enter the extension number or numbers of users and groups on your system.
  - To enter multiple numbers, separate each extension number with a , comma. For example 201, 202.
  - To enter a range of numbers, enter the start and end number with a - hyphen between them. For example 201-220.
- **User Name** – The name of the user.
- **Target Number** – The extension number of the original call target. For example, an incoming external call may have been originally targeted to a particular group extension number.
- **Target Name** – The name of the original call target.
- **Call ID** – The unique ID assigned to a recording.

4. Click **Apply Filter**.
   - If required, you can save the filter settings. The settings are then automatically reapplied when you next access the menu. Click **Save Filter**.

Related links

Viewing Recordings on page 712

Playing Recordings

You can playback a recording directly from the browser.

Procedure

1. Sort and filter the list of recordings to display the recording that you want play. See Applying a Recording Filter on page 712.
2. Click on the ▶ icon next to the recording you want to play.
3. The playback bar is displayed and the playback starts automatically.

- Pause and restart the playback by clicking the ⏸ and ▶ icons.
- The slider shows the progress of the playback. You can click the slider to select which part of the recording you hear.
- Use the 🔊 icon to mute/unmute the playback.

Related links

Viewing Recordings on page 712

Downloading Recordings

The recordings are downloaded in Opus file format which can be played back through most browsers and many media applications.

⚠ **Warning:**

- It is your responsibility to ensure that any access to and use of recordings complies with all laws and regulations regarding data privacy and recording of calls with third parties (for example GDPR regulations).

Procedure

1. Sort and filter the list of recordings to display the recording or recordings that you want to download. See Applying a Recording Filter on page 712.
   - To download a single recording, click on the ⬇ icon next to the recording.
   - To download a set of recordings:
     a. Select the check box next to the recording or recordings that you want to download.
     b. Click **Download**.
     c. Enter a password for the zip file that will contain the recordings.
     d. Click **Download**. The file or files are downloaded as single ZIP file containing all the selected recordings.
2. The remaining steps depend on the browser. It will display its normal options for downloading a file.

Related links

Viewing Recordings on page 712

Deleting Recordings

You can manually delete recordings ahead of their automatic deletion. The deletion is recorded as part of the audit trail.

Procedure

1. Sort and filter the list of recordings to display the recording or recordings that you want to delete. See Applying a Recording Filter on page 712.
2. Select the check box next to the recording or recordings that you want to download.
3. Click **Delete**.

Related links

Viewing Recordings on page 712

Archiving Recordings to the External Storage

If separate external storage has been configured (see Configuring Connection to the Google Storage Bucket on page 720), use the following process to copy existing recordings to that external store. Copied recordings are then viewed and managed via access to the external storage rather than through the user portal or web manager menus.

⚠ Warning:

- It is your responsibility to ensure that any access to and use of recordings complies with all laws and regulations regarding data privacy and recording of calls with third parties (for example GDPR regulations).

Procedure

1. Access your system's call recordings. See Viewing Recordings on page 712.
2. Select the calls that you want archived:
   - If you select any files using the check boxes, those are the files copied.
   - If you apply a filter but don't select any files, then all files matching the filter are copied.
   - Otherwise, all current recordings are copied.
3. Click **Archive Recordings** and then **Initiate**.
4. The progress of the file copying is shown.
   - To stop the copying process before it is complete, click **Abort**.
   - Following the process of copying, a listing file is also added to the external storage. See The Archive Listing Page on page 724.

Related links

Viewing Recordings on page 712

Archiving Recordings to External Storage on page 719

Chapter 64: Displaying the Recording Audit Trail

The audit trail allows you to see all activities by users of the recording library. For example, searches for, replaying of and download of recordings. For each event, the user name, date and time and the action are shown.

- Note that audit trail records are only kept for 180 days after which they are automatically deleted.
- Access is controlled by the user rights of the service user account used to log in to web manager. The account must be a member of a rights group that includes **External** > **Media Manager Standard** or **External** > **Media Manager Administrator** permission.

Procedure

1. Click **Applications**.
2. Click **Media Manager Audit Trail**.
3. Use the filter options to select what information you want displayed.
4. Set a **Start Date** and time, and an **End Date** and time. All four values must be set.
5. Click on **Event Type** and select the events that you want included in the audit trail. The options are:
   - **Configuration**, **Delete**, **Download**, **Login**, **Logout**, **Replay**, **Search**.
6. Click **Apply Filter** to display the matching audit trail records.

Related links

Exporting the Audit Trail on page 717

Exporting the Audit Trail

The currently displayed audit trail can be exported as a CSV file within a zipped and password protected file.

Procedure

1. Apply a filter to display the audit trail records required.

2. Click **Export**.
3. Enter a password. This is used to restrict access to zip file that will contain the audit trail.
4. Click **Export**.
5. The file is downloaded by the browser.

Related links

Displaying the Recording Audit Trail on page 717

Chapter 65: Archiving Recordings to External Storage

Centralized Media Manager automatically deletes each recording after a set number of days. By default that is 30 days. You can increase the retention period to up to 365 days. See Setting How Long Recordings are Kept on page 709.

If longer term storage is required, this can be done by configuring external storage.

- Currently the only external storage supported is within a Google Storage bucket. This requires knowledge of configuring and managing Google Storage which is not included in this manual.
- Files that are archived are copied from those currently in the voice recording library. The originals remain available in the library until manually or automatically deleted from it.
- During the process of copying recordings to the external storage, the system also creates a HTML file which can be used to view, sort and playback the recordings in the external storage, see The Archive Listing Page on page 724.
- Access to and use of the list file needs to be configured by the Google Storage bucket administrator, see Allowing Access to the External Storage by Other Users on page 723.

Warning:

- It is your responsibility to ensure that any access to and use of recordings complies with all laws and regulations regarding data privacy and recording of calls with third parties (for example GDPR regulations).

Related links

Configuring Connection to the Google Storage Bucket on page 720
Archiving Recordings to the External Storage on page 715
Google Administrator Access to the External Storage on page 721
Allowing Access to the External Storage by Other Users on page 723
The Archive Listing Page on page 724

Configuring Connection to the Google Storage Bucket

Before You Begin

This process requires you to have a JSON key file. The key file contains details required for the system to access the Google Storage.

- For details of exporting a key file, see Google Documentation.
- JSON key files are available in two format. The format depends on whether the file was created from the Google Control Panel (GCP)/command line or using the REST API. The GCP/command line format should be used. The file should look similar to the following.

```
{
"type": "service_account",
"project_id": "[PROJECT-ID]",
"private_key_id": "[KEY-ID]",
"private_key": "-----BEGIN PRIVATE KEY-----\n[PRIVATE-KEY]\n-----END PRIVATE
KEY-----\n",
"client_email": "[SERVICE-ACCOUNT-EMAIL]",
"client_id": "[CLIENT-ID]",
"auth_uri": "https://accounts.google.com/o/oauth2/auth",
"token_uri": "https://accounts.google.com/o/oauth2/token",
"auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
"client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/[SERVICE-
ACCOUNT-EMAIL]"
}
```

Process

1. Access **System Settings** > **System** > **Recording Archival Configuration**.
2. Enter the **Bucket Name**.
3. Enter the name for the folder that should be used within the bucket for the recordings.
4. Use the **Service Account Details** settings to upload the JSON key file for the bucket.
5. Click on **Test Connection** and wait for confirmation.
6. If successful, click **Save Configuration**.
7. Click **Update**.

Related links

Archiving Recordings to External Storage on page 719

Archiving Recordings to the External Storage

If separate external storage has been configured (see Configuring Connection to the Google Storage Bucket on page 720), use the following process to copy existing recordings to that external store. Copied recordings are then viewed and managed via access to the external storage rather than through the user portal or web manager menus.

Warning:

- It is your responsibility to ensure that any access to and use of recordings complies with all laws and regulations regarding data privacy and recording of calls with third parties (for example GDPR regulations).

Procedure

1. Access your system's call recordings. See Viewing Recordings on page 712.
2. Select the calls that you want archived:
   - If you select any files using the check boxes, those are the files copied.
   - If you apply a filter but don't select any files, then all files matching the filter are copied.
   - Otherwise, all current recordings are copied.
3. Click **Archive Recordings** and then **Initiate**.
4. The progress of the file copying is shown.
   - To stop the copying process before it is complete, click **Abort**.
   - Following the process of copying, a listing file is also added to the external storage. See The Archive Listing Page on page 724.

Related links

Viewing Recordings on page 712
Archiving Recordings to External Storage on page 719

Google Administrator Access to the External Storage

About this task

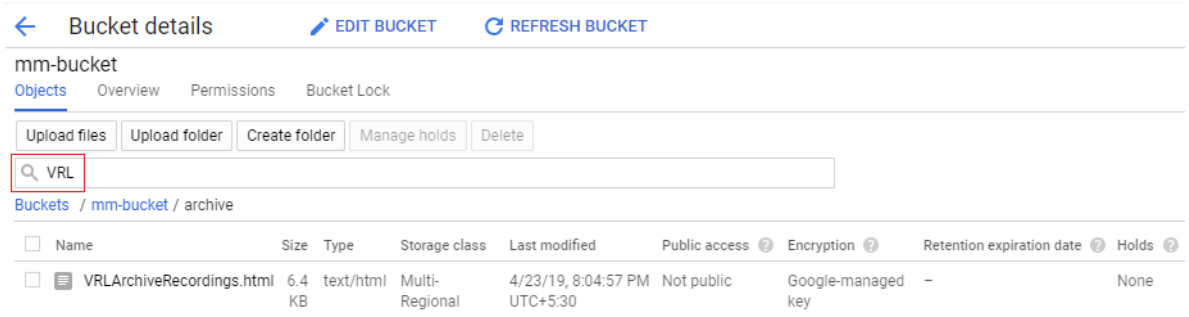
Once some recordings have been copied to the external storage (see Archiving Recordings to the External Storage on page 715), you can access the archive file. When you have the file's URL, you can open the file in a browser window.

You can also share the file URL with other users once you setup permissions for them to access the folder contents.

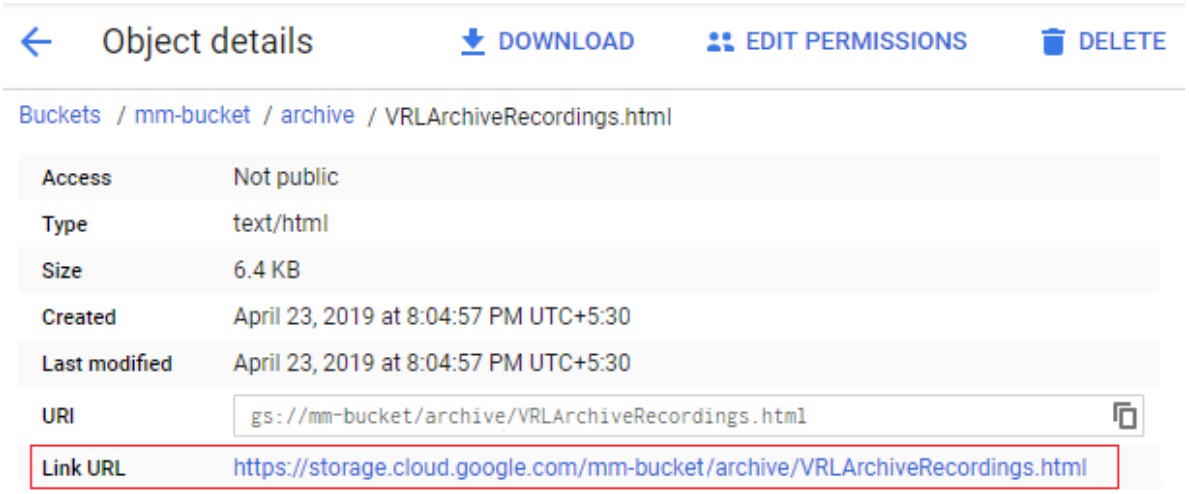
Procedure

1. Log into the Google Cloud Platform using the user account that was used to create the storage bucket.
2. If necessary, select the project under which the storage was created.
3. On the dashboard, locate **Resources** and click on **Storage**.
4. In the objects list, click on the bucket name.
5. Click on the name of the folder used to store the archived recordings.

6. Locate the `VRLArchiveRecordings.html` file. To speed up finding the file, enter `VRL` in the filter box to show only matching file names.



7. Click on the file name to display the file details.



8. The **Link URL** is the value needed for browser access to the list of recordings in the archive.
   - **To open the page in the browser:** Right-click on the value and select **Open link in a new window**. The recordings listing page is displayed, see The Archive Listing Page on page 724. If required, bookmark the address for your future access.
   - **To copy the value in order to share it with another user:** Right-click on the value and select **Copy link address**. Paste the link into the email or document being prepared for the other user. Note that you need to create permissions for the other user to access the files. See Allowing Access to the External Storage by Other Users on page 723.

Related links

Archiving Recordings to External Storage on page 719

Allowing Access to the External Storage by Other Users

About this task

Other users can be granted permission to access the archives listing file. In order to do this, the user will need a Google user account.

Access then requires:

- The email address associated with the Google user account is added to the archive bucket's permissions.
- They access the archive using a browser which is logged in using the Google user account.

Procedure

1. Follow the same process as used for the initial administrator access (see Google Administrator Access to the External Storage on page 721) to obtain the URL of the listing page.
2. Paste the **Link URL** into the document or email being prepared for sending to the other user.
3. Grant the users email account permission to access the archive folder.
4. In the objects list, click on the bucket name.
5. Click on the name of the folder used to store the archived recordings.
6. Select **Permissions**.
   - Note that the following is only an example. Google storage supports a range of methods and levels at which permissions can be granted. However, in all cases, ensure that the permissions cover access to all the files in the storage folder and any sub-folders.
7. Select **Add members**.
   a. In **New Members**, enter the email address of the user's Google account.
   b. From **Select a role**, select `Storage Legacy | Storage Bucket Reader`.
   c. Click **Save**.
8. Locate the `VRLArchiveRecordings.html` file. To speed up finding the file, enter `VRL` in the filter box to show only matching file names.
9. Click on the file name to display the file details.
10. The **Link URL** is the key value required. Right-click on the value and select **Copy link address**. Paste the link into the email or document being prepared for the other user. Note that you need to create permissions for the other user to access the files.
11. Send the details for accessing the listings file to the user.

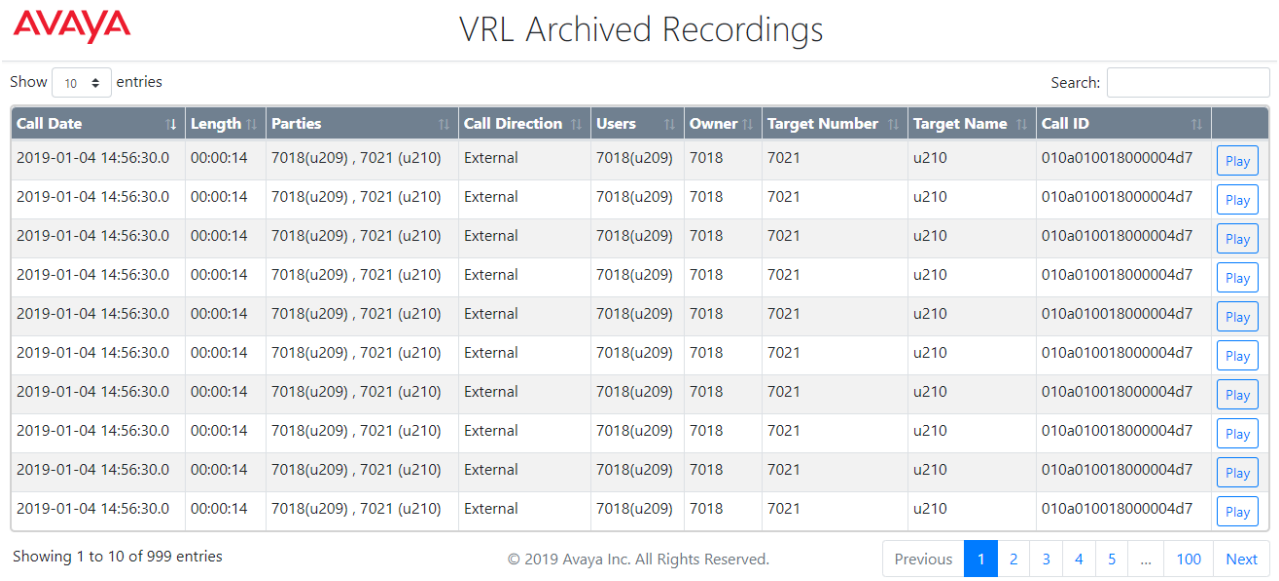
Related links

Archiving Recordings to External Storage on page 719

The Archive Listing Page

In order to access the archive listing, you need to be log in with a Google user account that has been granted permission to access the archive folder. See Allowing Access to the External Storage by Other Users on page 723.

A link for the archive is shown on the **Voice Recordings Library** page. When opened, the archive listing page defaults to showing the recordings in date order.



- You can sort the recordings by clicking on the column headers. The icons in the headers indicate the current column being used for sorting and the direction of the sorting.
- The Play button will begin playing the selected recording and display playback controls. Only one file can be played at a time.
- The search box can be used to filter the displayed recordings to only those that include matching words in their call details. You can enter multiple words separate by spaces.

Related links

Archiving Recordings to External Storage on page 719

Part 11: Configuring Systems

Chapter 66: Subscriptions

Subscriptions are monthly paid entitlements. They can be divided into two main groups;

- per-user per-month user subscriptions
- per-month application subscriptions for selected applications.

In practice, subscriptions are purchased for a specific duration. For example; 6-months, 1-year, 3-years.

During operation:

- If connection to the subscription server is lost, the IP Office system continues running with the existing subscription entitlements it has already received for 30-days.
- If when connected, any subscription expires, the feature or features associated with the expired subscriptions cease operation immediately.
  - The person responsible for ordering subscriptions must ensure that they are aware of subscription expiry dates. They must renew subscriptions in a timely manner, including time for renewal orders to be processed.

Related links

Ordering Subscriptions on page 726
Trial Mode on page 727
User Subscriptions on page 727
Application Subscriptions on page 728
Customer Operations Manager (COM) on page 729
Subscription Connection Operation on page 730
Subscription Network Requirements on page 731
Subscription Mode Ports on page 732
Migrating Existing IP Office Systems to Subscription Mode on page 733

Ordering Subscriptions

Subscription for an IP Office subscription mode system are ordered from the Avaya Channel Marketplace. The subscriptions are ordered against the PLDS ID of the IP Office system.

After ordering the subscriptions, details of the customer number and address of the subscription server are supplied in an email. Those details are required during the initial system configuration.

- The person responsible for ordering subscriptions must ensure that they are aware of subscription expiry dates. They must renew subscriptions in a timely manner, including time for renewal orders to be processed.

Related links

Subscriptions on page 726

Trial Mode

When ordering an IP Office subscription system through the Avaya Channel Marketplace, trial mode can be selected. Trial mode enables the IP Office to operate for up to 30-days using free subscriptions.

- The trial mode IP Office system indicates that it is in 30-day subscription error mode in applications such as the System Status Application and through system alarms.
- Before the 30-day trial period ends, the subscriber can return to Avaya Channel Marketplace and request a conversion to paid-subscriptions mode.

Important:

- To avoid any interruptions to customer telephony services, you must request the change to paid-subscriptions before the end of the 30-day trial period. That request must include allowance for sufficient working time to implement the request.

Related links

Subscriptions on page 726

User Subscriptions

Each user on the system requires a subscription. All subscribed users are then able to use an the system's telephone extension (analog, digital or IP) and voicemail features. The following user subscriptions can be ordered: **Telephony User**, **Telephony Plus User** and **Unified Communications User**. The subscriptions are applied to individual users through their **User Profile** setting.

Feature	Subscription Mode		
	Telephony User	Telephony Plus User	Unified Communications User
one-X Portal Services	–	–	✓

Table continues…

Feature	Subscription Mode		
	Telephony User	Telephony Plus User	Unified Communications User
Telecommuter options	–	–	✓
UMS Web Services	–	–	✓
TTS for Email Reading	–	–	✓
Remote Worker	✓	✓	✓
Avaya Workplace Client	–	✓[1]	✓
WebRTC	–	–	✓
Mobility Features	–	–	✓

- By default, users on a new or defaulted system are configured a **Telephony User** users.
- Users without a subscription are shown as **Non-licensed User** and cannot use any system features.
- If there are insufficient subscriptions for the number of users configured to a particular profile, some of those users will not receive any services. On suitable Avaya phones, they display as logged out and an attempt to log in displays a no license available warning.

1. Only supports Avaya Workplace Client basic mode (telephony and local contacts only).

Related links

Subscriptions on page 726

Application Subscriptions

The following application subscriptions can be ordered for a IP Office subscription system:

Subscription	Description
Receptionist Console	This subscription is used to enable the IP Office SoftConsole application to answer and redirect calls. The number of subscriptions allows the matching number of users to be configured as IP Office SoftConsole users. Those users still require a user subscriptions for their telephone connection (IP Office SoftConsole is not a softphone).
Avaya Call Reporter	This subscription enables support for the Avaya Call Reporter application, hosted on a separate server.
Avaya Contact Center Select	This subscription enables support the Avaya Contact Center Select (ACCS) service hosted on a separate server.

Table continues…

Subscription	Description
Media Manager	This subscription enables support for Media Manager. This can either be locally hosted on an IP Office Application Server or provided centrally by the same cloud-based servers providing the system's subscriptions. In either case: • A local Voicemail Pro service running on an IP Office Application Server is used to do the actual recording. • The recordings are then collected by the Media Manager service for archiving. • This option is not supported if using voicemail provided by a Unified Communications Module.
Third-Party CTI	This subscription enables support for CTI connections by third-party applications. This includes DevLink, DevLink3, Third-party TAPI and TAPI WAV.

Related links

Subscriptions on page 726

Customer Operations Manager (COM)

IP Office subscription services are a set of cloud-based services provided by Avaya to support IP Office subscription systems. A separate set of these services is provided for each geographic region to support Avaya business partners and their customer systems in that region.

The key service is Customer Operations Manager (COM). COM provides:

- Subscriptions to the IP Office systems.
- Displays the status of the IP Office systems and information about current alarms, type of system, software level.
- Each business partner has an account that allows them to access COM but only see their own customer's systems. They can create additional COM user accounts and control which of their customer systems those accounts can see.
- Avaya have access to COM for their support staff in order to manage the COM services and to assists business partners when required.
- COM can provide the files used to customize various features such as phone background and screen saver images. This can be configure to provide common files to all the business partner's systems or individual files to individual end-customer systems.
- COM can act as the file server for firmware files used by Vantage phones and Avaya Workplace Client.
- For full documentation of COM, refer to the Using Customer Operations Manager for IP Office Subscription Systems manual.

Additional Support Features

A number of additional support services can be enabled through settings in the IP Office system configuration.

Feature	Description
Remote Backup/ Restore	Subscription systems can automatically upload daily backups to the cloud. In addition, COM operators can perform both manual backups and restores operation
Remote Upgrade	Avaya provide COM with updated IP Office software images. COM operators can use these to perform immediate or scheduled system upgrades.
Log File Collection	Subscriptions systems can automatically upload all available log files to the cloud each day.
Centralized Management	Administrator connections for IP Office Web Manager, SysMonitor and System Status Application can be routed through COM to the customer's IP Office systems. The connects use the TLS tunnel used for the subscriptions.
Remote Access	Connections for HTTPS and SSH/SFTP connection can also be routed through COM to the customer IP Office systems. The connects use the TLS tunnel used for subscription.
Co-located Servers	When remote access is enabled, access to other servers and services on the same network as the customer IP Office system can be enabled. That includes access to non-IP Office servers and services subject to their own authentication.

Related links

Subscriptions on page 726

Subscription Connection Operation

The connection between the IP Office and COM operates are follows:

Outgoing Connection

For the connection from the IP Office to COM:

- The destination is a single static IP address resolved by DNS of the subscription server address entered during the system's initial configuration.
- The IP Office alternates between TCP ports 443 and 8443 until successful.
- The link uses the HTTP 'WebSocket' protocol and TLS 1.2 with mutual authentication.
- The link carries a regular heartbeat, subscription information and basic details of the IP Office system (type of servers and software version).
- All other traffic on the link is controlled by the IP Office system settings; there are no access controls elsewhere.
- If the link is interrupted, the IP Office system goes into a 30-day error mode with daily alarms.
  - If connection to the subscription server is lost, the IP Office system continues running with the existing subscription entitlements it has received for 30-days.
    - During the error mode period, all operations and features are unaffected. The system outputs daily alarms in the system logs.
    - Successful reconnection clears the alarms and error mode.
    - If the 30-day error mode period expires, all subscription features and telephony are deactivated.

- If when connected, any subscriptions expire, the feature or features associated with the expired subscriptions cease operation immediately.
- • The person responsible for ordering subscriptions must ensure that they are aware of subscription expiry dates. They must renew subscriptions in a timely manner, including time for renewal orders to be processed.

Incoming Connection

All incoming traffic from COM is routed to the IP Office through the existing subscription connection established above. It should not require any additional configuration on the customer network if the system has successfully obtained it subscriptions.

Related links

Subscriptions on page 726

Subscription Network Requirements

In order to obtain its subscriptions and to be remotely monitored and managed through COM , the IP Office systems requires the following:

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>Subscription details</td><td>Details of the customer ID and subscription server address are provided by email. Those details are entered during the system's initial configuration.
• For an IP500 V2 SCN, each IP500 V2 requires a License Server Link.
• For a Server Edition deployment, only the Primary server has a License Server Link.</td></tr>
<tr><td>Internet access</td><td>The system needs to be able to access the external internet. This is normally achieved during initial configuration of the system by entering the default gateway address of the outgoing router on the customer network.
• That value is used to configure an default IP route in the system configuration with the following settings:
<table><tr><th>IP Route Setting</th><th>Value</th></tr><tr><td>IP Address</td><td>0.0.0.0</td></tr><tr><td>IP Mask</td><td>0.0.0.0</td></tr><tr><td>Gateway IP Address</td><td>The address of the external network router on the customer network</td></tr><tr><td>Destination</td><td>The IP Office LAN interface (LAN1 or LAN2) which is connected to the customer network.</td></tr></table>• Maximum round trip delay 200ms.
• Minimum connection bandwidth 128kbits/s.
• If the customer firewall or router controls the ports used for outgoing internet access, ensure that outgoing HTTPS traffic on TCP ports 8443 and 443 are allowed.</td></tr>
</table>

Table continues…

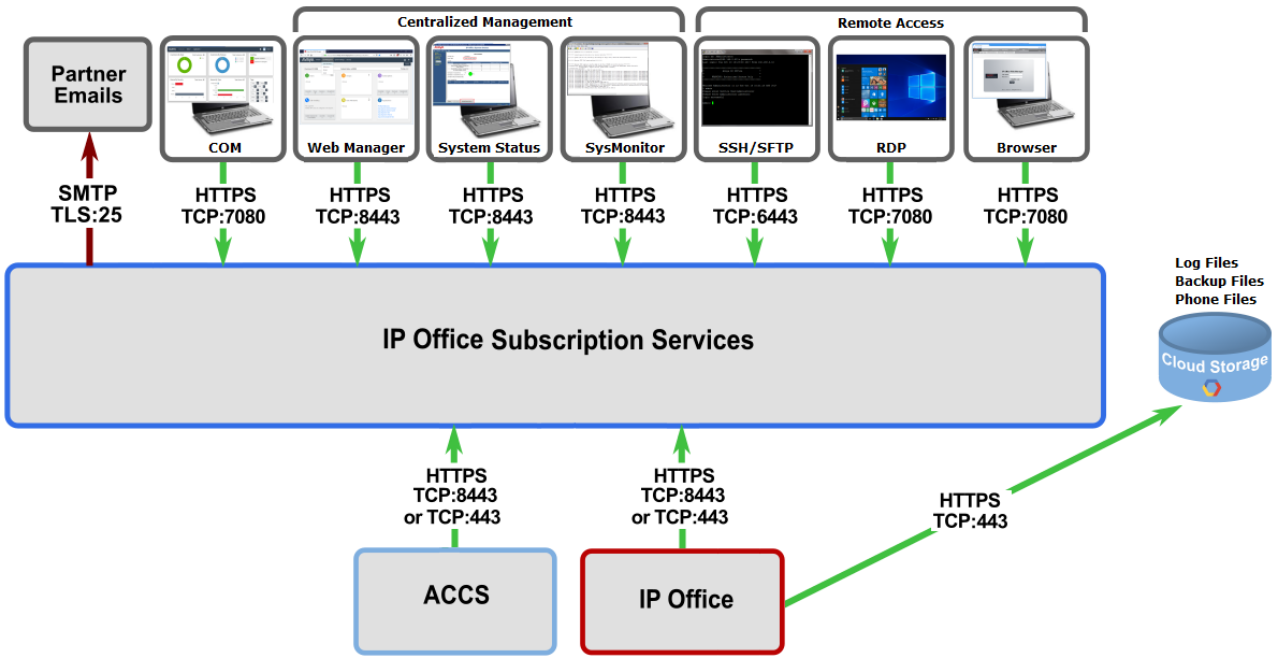
Feature	Description
DNS Service	The address of the customer's DNS server or service. If the customer does not have a specific DNS service, then use 8.8.8.8. If the customer has their own DNS server: • Ensure that it is configured to allow external access to addresses in the `avaya-sub.com` domain. That domain is used to the COM servers that support subscription systems in various geographic regions. For example: `admin.uk1.avaya-sub.com`. • Ensure that it is also configured to allow external access to storage.googleapis.com. This address is used for subscription features that require access to file storage.
Time source	Subscriptions requires an accurate time source. The recommendation is to use the Google time service at `time.google.com`. The system's time zone should also be set correctly.
COMAdmin Security User	The connection from the system to COM uses the security settings of the COMAdmin service user account in the IP Office system's security settings. This account is created by default on new and default systems.

Related links

Subscriptions on page 726

Subscription Mode Ports

The following schematic shows the ports used for connections to and from the subscription service running on COM.



Related links

Subscriptions on page 726

Migrating Existing IP Office Systems to Subscription Mode

The process for migrating an existing IP Office Essential Edition or Preferred Edition system to IP Office system is can be performed by rerunning the initial configuration menu. The assumed mapping of existing user profiles to their subscription equivalents is as follows:

Essential/Preferred Edition Mode	Subscription Mode
Non-Licensed User	Non-Licensed User
Basic User	Telephony User
Mobile User	
Office Worker	UC User
Power User	

Related links

Subscriptions on page 726

Chapter 67: General System Configuration

This section covers various aspects of IP Office system configuration.

Related links

Centralized System Directory on page 734
Advice of Charge on page 738
Using Locations on page 739
Caller Display on page 739
Parking Calls on page 740
Automatic Intercom Calls on page 741
Wide Band Audio Support on page 742
Media Connection Preservation on page 743
Configuring IP Routes on page 744
Creating a Virtual WAN Port on page 745

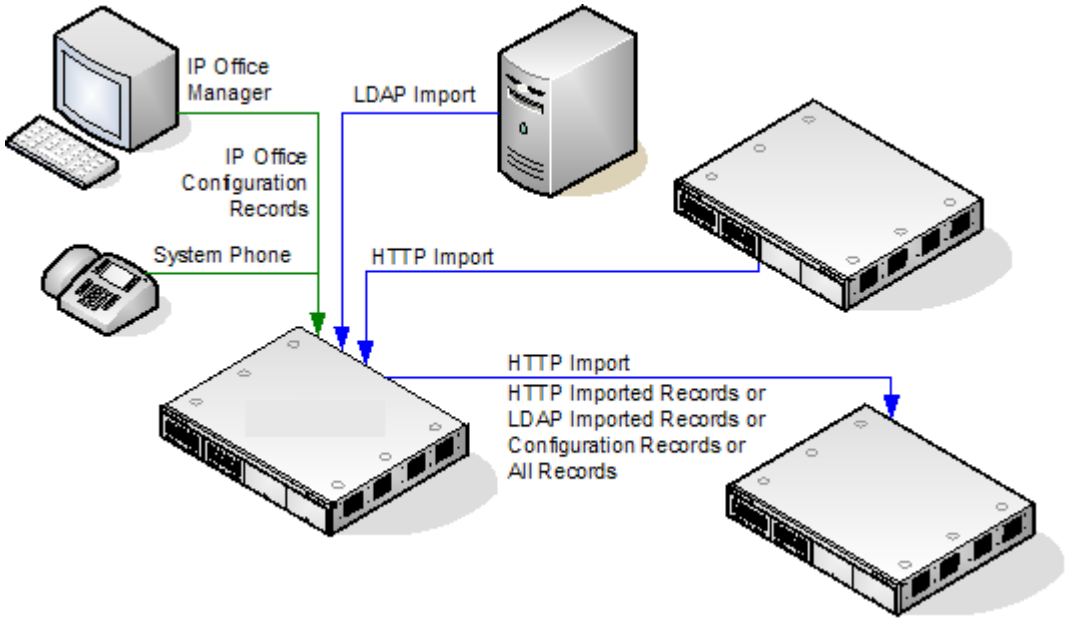
Centralized System Directory

Directory services can be used to import directory records (names and numbers) from external sources. These sets of records are regularly re-imported.

Directory records can come from the following sources:

- **LDAP Import**: The system can import LDAP records for use within directories shown by user phones and applications. LDAP import is configured through the **System Settings** > **System** > **Directory Services** > **LDAP** form. You can use LDAP Version 2 and 3.
- **HTTP Import** : Systems are able to import the directory records from another system using HTTP. HTTP import is configured through the **System Settings** > **System** > **Directory Services** > **HTTP** form by specifying an IP address or multi-site network connection. The records imported can be any or all of the following record types held by the system from which the records are being imported: LDAP imported records, HTTP imported records, configuration records.
- **System Directory Records (Configuration records)**: Records can be entered directly into the system configuration through the **System Settings** > **System Directory** > **Add/Edit Directory Entry** form. System directory records override matching LDAP/HTTP imported records.

Users with system phone rights (see System Phone Features on page 846) and a phones with a **CONTACTS** button can add, delete and edit the system directory records of the system on which they are logged in. They cannot edit LDAP or HTTP imported records.



Server Edition Directory Operation

For a Server Edition network, these settings can only be configured at the network level and they are stored in the configuration of the Primary Server. All other systems in the network are configured to share the directory settings of the Primary Server through the settings at **System Settings** > **System** > **Directory Services** > **HTTP**.

Directory Record Capacity

The directory capacity depends on the type of system. The figures below are applicable for Release 10.0.

	System	Number of Directory Records			Total Number of Directory Records
		Configuration	LDAP Import	HTTP Import	
Standalone Systems	**IP500 V2**	2,500	10,000	10,000	10,000
Server Edition	**Primary Server**	10,000	10,000	10,000	10,000
	Secondary Server	–	–	10,000	10,000
	Expansion System (L)	–	–	10,000	10,000
	Expansion System (V2)	–	–	10,000	10,000

Directory Dialing

Directory numbers and names are displayed by user applications such as SoftConsole. The method by which these directories are searched and used depends on the application. Refer to the appropriate user guide.

Directory entries used for dialing can contain **()** and **—** characters in the number. Those characters are ignored in the dialled output. Directory entries containing **?** in the number (used for directory name matching) are not included in the directory for dialing.

Directory names are also viewable through the **Dir** or **Contacts** function on many Avaya phones. They allow the user to select the name in order to dial its associated number.

The directory function groups directory records shown to the phone user into several categories, for example; system, personal, users and groups. Depending on the phone or application, the user may be able to select the category currently displayed. In some scenarios, the categories displayed may be limited to those supported for the action being performed by the user. The typical categories are:

- **External**: Directory records from the system configuration. This includes HTTP and LDAP imported records.
- **Groups**: Groups on the system. If the system is in a multi-site network, it will also include groups on other systems in the network.
- **Users** or **Index**: Users on the system. If the system is in a multi-site network it will also include users on other systems in the network.
- **Personal**: Available on 1400, 1600, 9500, 9600 and J100 Series phones. These are the user's personal directory records stored within the system configuration.

On phones that support **Dir** or **Contacts**, the user can filter the currently displayed set of directory names by dialing on their keypad. Additional dialing applies a progressive filter. For example, if the user presses the 5 key (JKL), only names with some part beginning with J, K or L remain listed. If the user then presses the 2 key (ABC), only names with some part beginning with JA, JB, JC, KA, etc. remain listed. As the users presses more keys on their phone, the number of remaining matches reduces.

By default the letter matching is performed simultaneously against all parts of the directory name, ie. first, middle and last name. However, this behavior can be modified for all users using a NoUser source number.

Speed Dialing

On M-Series and T-Series phones, a **Speed Dial** button or dialing **Feature 0** can be used to access personal directory records using the record’s index number.

- **Personal**: Dial **Feature 0** followed by ***** and the 2-digit index number in the range 01 to 99.
- **System**: Dial **Feature 0** followed by 3-digit index number in the range 001 to 999.
- The **Speed Dial** short code feature can also be used to access a directory speed dial using its index number from any type of phone.

Caller Directory Name Matching

Directory records are also used to associate a name with the dialled number on outgoing calls or the received CLI on incoming calls. When name matching is being done, a match in the user's

personal directory overrides any match in the system directory. Note that some user applications also have their own user directory.

- The **( )** and **—** characters are not used for directory name matching. Directory entries with those characters are ignored for name matching.
- A ? character can be used to match any digit or digits. For example 91?3 will match 9123. Typically a single ? is used at the end of a known dialing string such as an area code.
- The best match is used, determined by the highest number of matched digits.
- There is no minimum number of matches. For example, a directory entry of 9/External can be used to match any external call unless it has a better match.

Other Name Sources

- SoftConsole has its own directories which are also used for name matching. Matches in the application directory can lead to the application displaying a different name from that shown on the phone.
- Name matching is not performed when a name is supplied with the incoming call, for example QSIG trunks. On SIP trunks the use of the name matching or the name supplied by the trunk can be selected using the **Default Name Priority** setting (**System | Telephony | Telephony**). This setting can also be adjusted on individual SIP lines to override the system setting.
- Directory name matching is not supported for DECT handsets. For information on directory integration, see Deploying Avaya Wireless DECT with IP Office.

Imported Records

Imported directory records are temporary until the next import refresh. They are not added to the system's configuration. They cannot be viewed or edited using Manager or edited by a system phone user. The temporary records are lost if the system is restarted. However the system will request a new set of imported directory records after a system restart. The temporary records are lost if a configuration containing Directory changes is merged. The system will then import a new set of temporary records without waiting for the **Resync Interval**. If an configuration record is edited by a system phone user (see System Phone Features on page 846) to match the name or number of a temporary record, the matching temporary record is discarded.

Importation Rules:

When a set of directory records is imported by HTTP or LDAP, the following rules are applied to the new records:

- Imported records with a blank name or number are discarded.
- Imported records that match the name or number of any existing record are discarded.
- When the total number of directory records has reached the system limit, any further imported records are discarded.

  For capacity information, see the description for the **Directory** tab.

Related links

General System Configuration on page 734

Advice of Charge

The system supports advice of charge (AOC) on outgoing calls to ISDN exchanges that provide AOC information. It supports AOC during a call (AOC-D) and at the end of a call (AOC-E). This information is included in the SMDR output.

AOC is only supported on outgoing ISDN exchange calls. It is not supported on incoming calls, reverse charge calls, QSIG and non-ISDN calls. Provision of AOC signalling will need to be requested from the ISDN service provider and a charge may be made for this service.

The user who makes an outgoing call is assigned its charges whilst they are connected to the call, have the call on hold or have the call parked.

- If AOC-D is not available, then all charges indicated by AOC-E are assigned to the user who dialed the call.
- If AOC-D is available:
  - If the call is transferred (using transfer, unpark or any other method) to another user, any call charges from the time of transfer are assigned to the new user.
  - If the call is manually transferred off-switch, the call charges remain assigned to the user who transferred the call.
  - If the call is automatically forwarded off switch, subsequent call charges are assigned to the forwarding user.
  - AOC-D information will only be shown whilst the call is connected. It will not be shown when a call is parked or held.
  - Call charges are updated every 5 seconds.

For conference calls all call charges for any outgoing calls that are included in the conference are assigned to the user who setup the conference, even if that user has subsequently left the conference.

Enabling AOC Operation

1. **Set the System Currency** The Default Currency (System | Telephony | Telephony) setting is by default set to match the system locale. Note that changing the currency clears all call costs stored by the system except those already logged through SMDR.
2. **Set the Call Cost per Charge Unit for the Line** AOC can be indicated by the ISDN exchange in charge units rather than actual cost. The cost per unit is determined by the system using the **Call Cost per Charge Unit** setting which needs to be set for each line. The values are 1/10,000th of a currency unit. For example if the call cost per unit is £1.07, a value of 10700 should be set on the line.
3. **Applying a Call Cost Markup** It may be a requirement that the cost applied to a user's calls has a mark-up (multiplier) applied to it. This can be done using the Call Cost Markup (User | Telephony | Call Settings) setting. The field is in units of 1/100th, for example an entry of 100 is a markup factor of 1.

Related links

General System Configuration on page 734

Using Locations

Locations are used to apply an number of common settings to lines and extensions that are in the same physical location. For example:

- Apply restrictions to the number of simultaneous calls on internal trunks between different IP Office systems. See Configuring Call Admission Control on page 827.
- Set the outgoing ARS that should be used when an extension associated with the location makes an emergency call. The aim being to ensure that emergency calls use trunks that match their physical location or using a caller ID number registered to the location. See Configuration for Emergency Calls on page 772.

  For SIP trunks, emergency calls can include sending the address information configured for the dialing extension's location.
- Apply location specific time offset settings to the time display on phones in the location.

Related links

General System Configuration on page 734

Caller Display

Caller display displays details about the caller and the number that they called. On internal calls, the system provides this information. On external calls it uses the Incoming Caller Line Identification (ICLID) received with the call. The number is also passed to system applications and can be used for features such as call logging, missed calls and to make return calls.

Analog extension can be configured for caller display via the system configuration (Extension | Extn | Caller Display Type).

Adding the Dialing Prefix Some systems are configured to require a dialing prefix in front of external numbers when making outgoing calls. When this is the case, the same prefix must be added to the ICLID received to ensure that it can be used for return calls. The prefix to add is specified through the Prefix field of each line.

Directory Name Matching The system configuration contains a directory of names and numbers. If the ICLID of an incoming call matches a number in the directory, the directory name is associated with that call and displayed on suitable receiving phones.

Applications such as SoftConsole also have directories that can be used for name matching. If a match occurs, it overrides the system directory name match for the name shown by that application.

Extended Length Name Display

In some locales, it may be desirable to change the way names are displayed on phones in order to maximize the space available for the called or calling name. There are two hidden controls which can be used to alter the way the system displays calling and called information.

These controls are activated by entering special strings on the Source Numbers tab of the NoUser user. These strings are:

LONGER_NAMES This setting has the following effects:

- On DS phones, the call status display is moved to allow the called/calling name to occupy the complete upper line and if necessary wrap-over to the second line.
- For all phone types:
- On incoming calls, only the calling name is displayed. This applies even to calls forwarded from another user.
- On outgoing calls, only the called name is displayed.

HIDE_CALL_STATE This settings hides the display of the call state, for example **CONN** when a call is connected. This option is typically used in conjunction with **LONGER_NAMES** above to provide additional space for name display.

Related links

General System Configuration on page 734

Parking Calls

Parking a call is an alternative to holding a call. A call parked on the system can be retrieved by any other user if they know the system park slot number used to park the call. When the call is retrieved, the action is known as Unpark Call or Ride Call. While parked, the caller hears music on hold if available.

Each parked call requires a park slot number. Attempting to park a call into a park slot that is already occupied causes an intercept tone to be played. Most park functions can be used either with or without a specified park slot number. When parking a call without specifying the park slot number, the system automatically assigns a number based on the extension number of the person parking the call plus an extra digit 0 to 9. For example if 220 parks a call, it is assigned the park slot number 2200, if they park another call while the first is still parked, the next parked call is given the park slot number 2201 and so on.

Park slot IDs can be up to 9 digits in length. Names can also be used for application park slots.

The **Park Timeout** setting in the system configuration (System | Telephony | Telephony | Park Timeout) controls how long a call can be left parked before it recalls to the user that parked it. The default time out is 5 minutes. Note that the recall only occurs if the user is idle has no other connected call.

There are several different methods by which calls can be parked and unparked. These are:

Using Short Codes

The short code features, Call Park and Unpark Call, can be used to create short codes to park and unpark calls respectively. The default short codes that use these features are:

- *37*N# - Parks a call in park slot number N.
- *38*N# - Unparks the call in park slot number N.

Using the SoftConsole Application

The SoftConsole application supports park buttons. SoftConsole provides 16 park slot buttons numbered 1 to 16 by default.

The park slot number for each button can be changed if required. Clicking on the buttons allows the user to park or unpark calls in the park slot associated with each button. In addition, when a call is parked in one of those slots by another user, the application user can see details of the call and can unpark it at their extension.

Using Programmable Buttons

The Call Park feature can be used to park and unpark calls. If configured with a specified park slot number, the button can be used to park a call in that slot, unpark a call from that slot and will indicate when another user has parked a call in that slot. If configured without a number, it can be used to park up to 10 calls and to unpark any of those calls.

Phone Defaults

Some telephones support facilities to park and unpark calls through their display menu options (refer to the appropriate telephone user guide). In this case parked calls are automatically put into park slots matching the extension number.

Related links

General System Configuration on page 734

Automatic Intercom Calls

Automatic intercom functions allow you to call an extension and have the call automatically answered on speaker phone after 3 beeps. The extension called must support a handsfree speaker. If the extension does not have a handsfree microphone then the user must use the handset if they want to talk. If the extension is not free when called, the call is presented as a normal call on a call appearance button if available.

Making Automatic Intercom Calls

The following programmable button functions can be used to make automatic intercom calls:

- **Automatic Intercom**
- **Dial Direct**
- **Dial Intercom**

The following short code function can be used to make automatic intercom calls:

Dial Direct

On M-Series and T-Series phones, the code **Feature 66** followed by the extension number can be used to make a direct voice (automatic intercom) call.

Deny automatic intercom calls

When enabled, any automatic intercom calls to the user's extension are automatically turned into normal calls.

Deny automatic intercom calls can be configured per user on the **User | Telephony | Supervisor Settings** tab. Deny automatic intercom call can also be enabled using the Auto Intercom Deny On short code or the Auto Intercom Deny button action.

Related links

General System Configuration on page 734

Wide Band Audio Support

IP Office systems support the G.722 64K codec for wide band audio. G.722 can be used with H.323 and SIP trunks. If can also be used with some SIP and H.323 IP telephones (see below). G.722 uses a higher speech sample rate (16KHz) than is used by most other audio codecs (8KHz).

G.722 is only supported by systems that are using IP500 VCM, IP500 VCM V2 and or IP500 Combination cards.

Avaya Phone Support

Use of G.722 is supported by the following Avaya phones on a IP Office system: 1100/1200 Series, 9600 Series, J100 Series, B179, B199.

Using the G.722 Codec

The G.722 codec is not available for use by default. If the codec is to be used, it must first be selected in the system's **Available Codecs** list (System | Codecs). The codec can then be used in the system's default codec preference list and or in the individual codec preferences of IP lines and extensions.

The method of codec selection for specific phones will depend on the phone type. Refer to the appropriate installation manual.

Conferencing

Where devices using G.722 are in a system conference, the system can attempt to ensures that the speech between devices using G.722 remains wide-band even if there are also narrow-band audio devices in the same conference. This is done if the system's High Quality Conferencing option is enabled (**System | Telephony | Telephony**).

Known Limitations

The following limitations apply to G.722 wide band audio operation:

- Call recording uses G.711.
- Page calls only use G.722 when all devices being paged can use G.722.

- Fax is not supported in G.722, use G.711 or T38.
- Soft tones provided by the system use G.711.
- A maximum of 15 G.722 devices receiving wide-band audio are supported in conferences.

Related links

General System Configuration on page 734

Media Connection Preservation

Media Connection Preservation maintains calls that experience end-to-end signalling loss or refresh failures but that still have an active media path.

IP Phones:

With IP Office 9.1 and higher, the following Avaya IP phones attempt to maintain calls when the signal from the host IP Office is lost.

- 9608
- 9611
- 9621
- 9641
- J100 Series

When preserving a call, the phone does not attempt to reregister with their call server or attempt to failover to a standby call server, until the call has ended. Softkey call actions and feature menus do not work during this time due to the loss of signalling path. The phone display is not updated and the only permitted action is to terminate the call.

IP Office:

When enabled for a particular IP endpoint type that supports Media Connection Preservation, the call is put into a Preserved state and a Preservation Interval timer is started for that call at the point the signalling loss is detected. The maximum duration of a preserved call on IP Office is two hours. Once put into the Preserved state, a call can only transition to the Terminated state. Call restoration is not supported.

Only the following call types are preserved:

- Connected active calls
- Two party calls where the other end is a phone, trunk, or voicemail
- Conference calls
- Calls on hold and calls to hunt groups are not preserved.

Phone Display:

When a call is in a preserved state but the phone's local signalling connection with its host IP Office is still present, the phone call state display is prefixed with a warning icon. Hold, transfer, and conference actions are not available.

System Configuration

When enabled on **System Settings** > **System** > **Telephony**, Media Connection Preservation is applied at a system level to SCN trunks and Avaya H.323 phones that support connection preservation. All systems in a Small Community Network (SCN) must be enabled for end to end connection preservation to be supported.

When enabled on **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Advanced**, Media Connection Preservation is applied to the SIP trunk. The value of connection preservation on public SIP trunks is limited. Media Connection Preservation on public SIP trunks is not supported until tested with a specific service provider. Media Connection Preservation is disabled by default for SIP trunks.

When enabled on **System Settings** > **Line** > **Add/Edit Trunk Line** > **SM Line** > **Session Manager**, Media Connection Preservation is applied to Enterprise Branch deployments. Media Connection Preservation preserves only the media and not the call signaling on the SM Line. Media Connection Preservation does not include support for the Avaya Aura Session Manager Call Preservation feature.

Related links

General System Configuration on page 734

Configuring IP Routes

The IP Office system acts as the default gateway for its DHCP clients. You can also specify the IP Office as the default gateway statically addressed devices on the same subnet as the IP Office. When those clients and devices want to send data to an IP address on a different subnet, they will send that data to the IP Office system for onward routing.

- **IPv4 Static Routes**

  For IPv4 traffic, the IP Office can use the **System** > **IP Route** configuration settings to determine where to forward traffic. You can configure the following as destinations for IP Office static routes:

  - **LAN1** - Direct the traffic to the IP Office system LAN1.
  - **LAN2** - Direct the traffic to the IP Office system LAN2.
  - **Service** - Direct the traffic to a service in the IP Office configuration. The service settings define the details to connect to a remote data service.
  - **Tunnel** - Direct the traffic to an IPSec or L2TP tunnel in the IP Office configuration.

  The IP Office system provides two methods of defining a default route for IP traffic that does not match any other specified routes.

  - **Default Service** - Within the settings for services, one service can be set as the **Default Route** (**Service | Service**).
  - **Default IP Route** - Create an IP Route record with a blank IP Address, blank IP Mask, and set to the required destination for default traffic.

- **IPv6 Static Routes**

Linux-based IP Office R12.1 systems can support IPv6. In that case, you can configure static routes for IPv6 traffic using the **System** > **IP Route (IPv6)** configuration settings.

- **IPv4 Dynamic Routes (RIP)**

  IP500 V2 IP Office systems can support RIP (Routing Information Protocol). The IP Office can use RIP to automatically learn routes for data traffic from other routers that also support RIP.

  - By default, static routes entered in the IP Office configuration override any dynamic routes learnt using RIP. This Favor RIP Routes over static routes (**System** > **System**) setting control this behavior.

RIP Dynamic Routing

Routers in a network can use Routing Information Protocol (RIP) to automatically advertise details of the routes they know. Through this process, each router can automatically add new network devices to its routing table.

- Each router-to-router link a 'hop'. The routing table can contain routes with up to 15 hops. When more than one route to a destination exists, the IP Office adds the route with the lowest metric (number of hops) to its routing table.
- When an existing route becomes unavailable, after 5 minutes the router marks it as requiring 'infinite' (16) hops. The router advertises this to the network and then removes the route from its routing table.
- The IP Office system also uses 'split horizon' and 'poison reverse' to prevent routes that create loops.
- RIP is a simple method for automatic route sharing and updating within small homogeneous networks. It allows routers to advertise alternate routes when an existing route fails. Within a large network, the exchange of routing information every 30 seconds can create excessive traffic. In addition, the IP Office routing table is limited to 100 static, dynamic, and internal routes.
- When a static route and a dynamic route to the same destination have the same metric, the IP Office uses the static route.
- RIP does not include broadcast (255.255.255.255) and multicast (224.0.0.0) route.

Related links

General System Configuration on page 734

Creating a Virtual WAN Port

Procedure

1. Select **WAN Port**.
2. Click and select **PPP**.

3. In the **Name** field, enter either **LINEx.y** where:
   - **LINE** must be in uppercase.
   - **x** is the line number. For a PRI/T1 module in Slot A, this will be 1. For a PRI/T1 module in Slot B, this will be 5.
   - **y** is the lowest numbered channel number to be used by the WAN link minus 1. For example, if the lowest channel to be used is channel 1 then y = 1 - 1 = 0.
4. In the **Speed** field, enter the total combined speed of the maximum number of channels sets in the Service.

   In this example, 12 channels x 64000 bits = 76800.

   Note:

   The maximum number of channels that can be used will be limited by the number of data channels supported by the system Control Unit and not already in use.
5. In the **RAS Name** field, select the RAS name created when the new Service of that name was created.
6. Click **OK**.

Related links

General System Configuration on page 734

Chapter 68: On-boarding

On-boarding refers to the configuration of an SSL VPN service in order to enable remote management services to customers, such as fault management, monitoring, and administration. You must use the Web Manager client to configure on-boarding.

For full details on how to configure and administer SSL VPN services, refer to Deploying Avaya IP Office™ Platform SSL VPN Services.

The procedure provided below configures IP Office for Avaya support services. Avaya partners can also use an SSL VPN to provide support services.

Related links

Configuring an SSL VPN using an on-boarding file on page 747

Configuring an SSL VPN using an on-boarding file

The on-boarding XML file is available from Avaya. It contains the settings required to establish a secure tunnel between IP Office and an AVG server. When you import the on-boarding XML file, it applies the settings and installs one or multiple TLS certificates.

When you configure the SSL VPN service on a new system, you must begin by generating an inventory file of the IP Office system. When you register your IP Office system, the inventory file that you generated is uploaded to the GRT and the inventory data is populated in the Avaya Customer Support (ACS) database. After you enable remote support, you can download the XML on-boarding file from the GRT web site and upload it into your IP Office system.

The on-boarding process configures:

- SSL VPN service configuration
- short codes for enabling and disabling the SSL VPN service
- SNMP alarm traps
- one or more TLS certificates in the IP Office trusted certificate store

Perform this procedure using the Avaya IP Office Web Manager client.

Warning:

The process of 'on-boarding automatically creates an SSL VPN service in the system configuration when the on-boarding file is uploaded to the system. Care should be taken not to delete or modify such a service except when advised to by Avaya.

Before you begin

Before you begin, you must have the hardware codes and catalog description of your IP Office system. For example, “IP OFFICE 500 VERSION 2 CONTROL UNIT TAA” is a hardware code and catalog description.

Procedure

1. Select **Tools > On-boarding**.

   The On-boarding dialog box displays.

2. If the hardware code for your IP Office system ends with the letters TAA, select the checkbox next to the prompt **Are you using TAA series hardware?**
3. Click **Get Inventory File** to generate an inventory of your IP Office system.
4. Click **Register IP Office**.

   A browser opens and navigates to the GRT web site.

5. Log in to the web site and enter the required data for the IP Office system.
6. Select **Remote Support** for the IP Office system.
7. Click **Download** and save the on-boarding file.
8. Browse to the location where you saved the on-boarding file and click **Upload**.

   A message displays to confirm that the on-boarding file has installed successfully.

Related links

On-boarding on page 747

Chapter 69: Fax Support

Fax on IP500 V2 Systems

IP500 V2 systems can terminate T38 fax calls. For a system with an IP500 VCM, IP500 VCM V2 or IP500 Combo cards, **T38** or **G.711** can be used for fax transmission. Each fax call uses a VCM channel unless it is a T38 fax call between compatibly configured call legs. A SIP line or extension must support Re-Invite.

T38 Fallback can also be specified. On outgoing fax calls, if the called destination does not support T38, a re-invite is sent for fax transport using **G.711**.

Configuring Fax on SIP Lines and Extensions:

To configure Fax on SIP Lines and Extensions:

1. On the **VoIP** page for the line or extension, set **Re-Invite Supported** to **On** in order to enable **Fax Transport Support**
2. Select a value in the **Fax Transport Support** field.

Note the following:

- Direct media is supported.
- If **Fax Transport Support** is set to **T38** or **T38 Fallback**, the T38 Fax page is available. The T38 Fax page provides detailed T38 configuration options.

Configuring Fax on an IP Office Line:

Within a multi-site network, **Fax Transport Support** can also be enabled on the IP Office Lines between the systems. This allows fax calls at one system to be sent to another system.

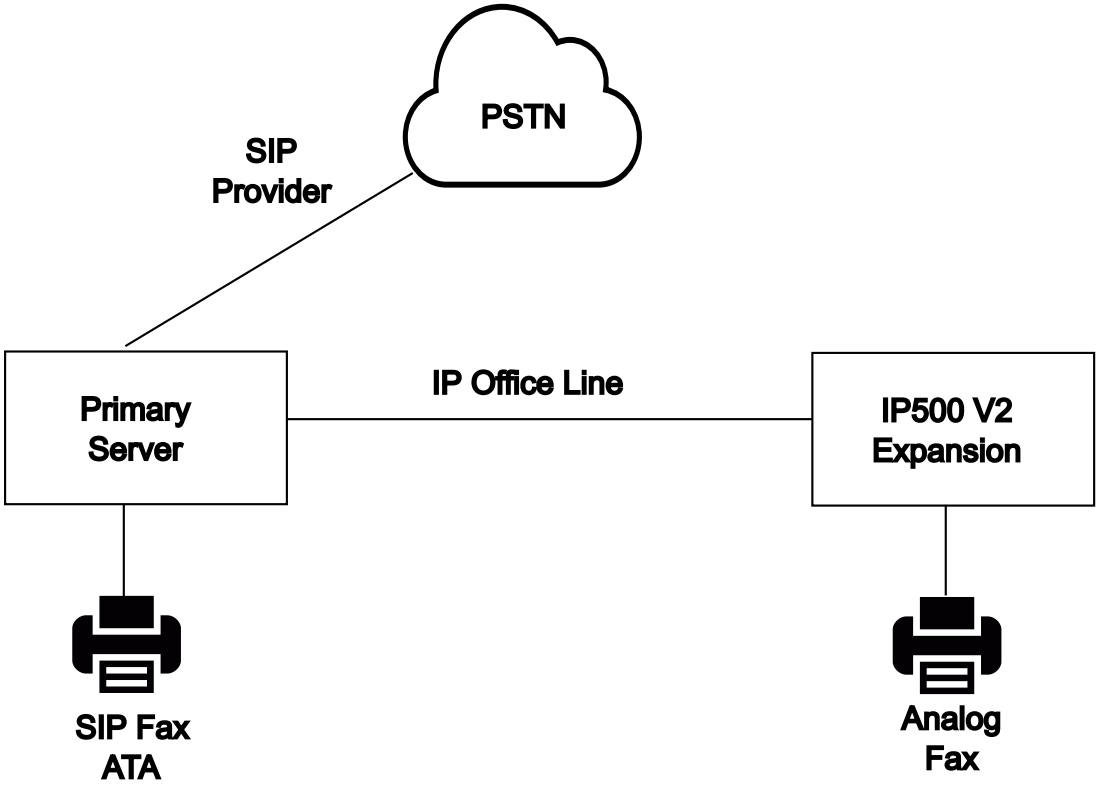
To configure Fax on an IP Office Line:

1. Set **IP Office Line | Line Settings | Networking Level** to **SCN**.
2. Set **IP Office Line | VoIP | Fax Transport Support** to **Fax Relay**.

Related links

Server Edition T38 Fax Support on page 750

Server Edition T38 Fax Support



Fax on Server Edition Linux Servers

IP Office Linux servers cannot terminate T38 fax and therefore, T38 is negotiated end-to-end. When a SIP ATA fax is connected to an IP Office Linux server, the system directly relays negotiation between the SIP ATA Fax and the SIP provider.

Configuring Fax on SIP Lines and Extensions:

To configure Fax on SIP Lines and Extensions, on the **VoIP** page for the SIP line or extension:

1. Set **Re-Invite Supported** to **On** in order to enable **Fax Transport Support**.
2. Select a value in the **Fax Transport Support** field.

Note the following.

- Direct media is supported.
- The **T38 Fax** page is not available.

Fax on Server Edition IP500 V2 Expansion Systems

Since an IP500 V2 system can terminate T38 fax, an analog fax can be connected to an IP500 V2 Expansion system. Fax transport is configured on the IP Office Line connecting the IP500 V2 system to the Server Edition network.

Configuring Fax on an IP Office Line:

To configure Fax on an IP Office Line, on the **Line | IP Office Line | VoIP Settings** page, select a value in the **Fax Transport Support** field. **Fax Relay** is not supported.

Note the following.

- Direct media is supported.
- The **T38 Fax** page is not available.

Related links

Fax Support on page 749

Chapter 70: Paging

The IP Office supports flexible paging to any extensions that support auto-answer and also paging to external paging devices. However, no paging options are configured by default on a newly installed IP Office system.

Paging Scenarios

Paging Scenario	Paged Device Connects to...	Short Code/ Button Feature
Phone to Phone Simple paging to other system extensions.	Digital Station and Avaya H.323 Phones	**Dial Paging**
Mixed Paging Simultaneous paging to phones and a paging speaker.	Analog Extension (Paging Speaker)	**Dial Paging**
Paging Interface Device Paging to a paging interface device such as a UPAM.	Analog Extension (IVR Port)	**Dial Extn**
	Analog Trunk	**Dial**

Related links

Paging Capacity on page 752
Phone to Phone Paging on page 753
Paging to an External Paging Device on page 753
Mixed Paging on page 754

Paging Capacity

For full capacity details, refer to Avaya IP Office™ Platform Guidelines: Capacity.

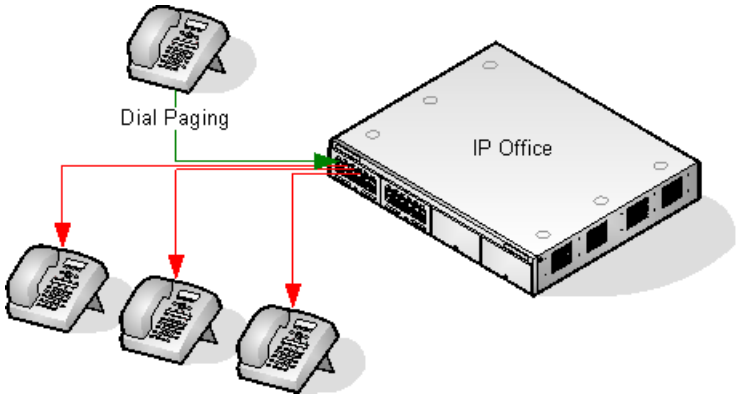
IP Office Type	Paging Group Maximum size
Server Edition/Select	512
IP500 V2	64

- Paging groups that include users on a V2 Expansion are limited to 64 members.
- Paging groups that include SRTP endpoints, the maximum size is reduce by 50%.

Related links

Paging on page 752

Phone to Phone Paging



- Paging is supported from all phone types. A page call can be to a single phone or a group of phones.
  - From analog and non-Avaya phones, use a Dial Paging short code.
  - From Avaya feature phones, a programmable button set to Dial Paging can be used.
- Paging is only supported to Avaya phones that support auto answer.
- The page is not heard on phones that are active on another call.
- The page is not heard on phones where the user is set to Do Not Disturb or has Forward Unconditional active.
- On Avaya phones with a dedicated **Conference** button, the user can answer a page call by pressing that button. This turns the page into a normal call with the pager.

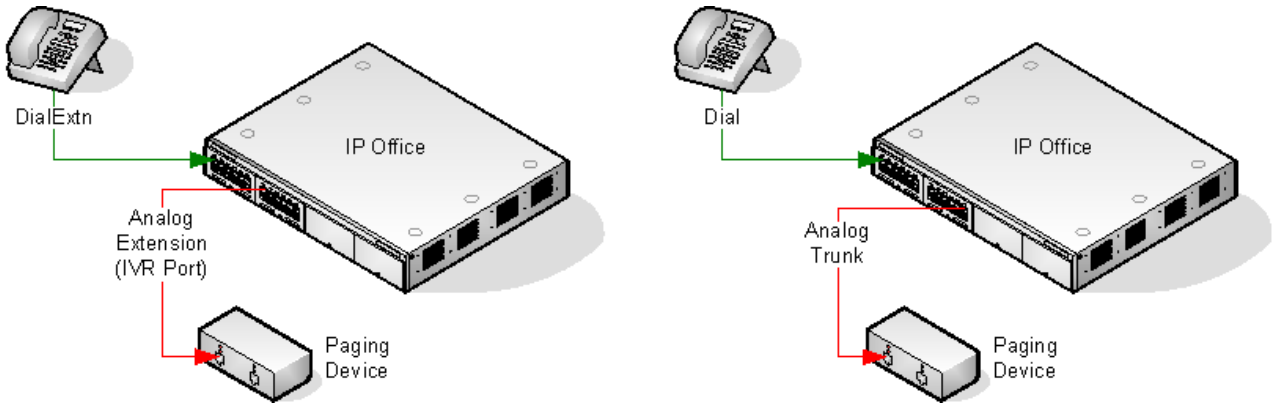
Related links

Paging on page 752

Paging to an External Paging Device

Paging Interface Device

Uses a paging interface device such as a UPAM or amplifier with analog trunk/extension interface. The device can be connected to an analog trunk port or analog extension port.



If connected to a trunk port:

- Use a short code set to **Dial** and the same **Line Group ID** as the **Outgoing Line ID** set for the analog trunk.

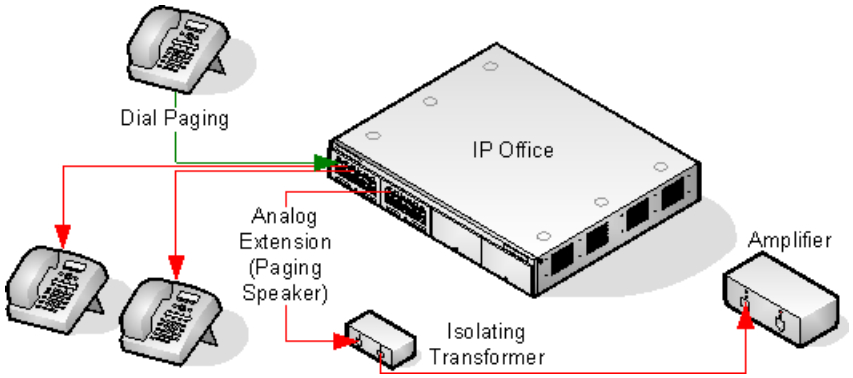
If connected to an extension port:

- Set the analog extension as an **IVR Port** in the system configuration (**Extn** > **Analog** > **Equipment Classification**).
- Use a short code or programmable button set to use **Dial Extn**.

Related links

Paging on page 752

Mixed Paging



Uses an amplifier connected to an analog extension port via a 600ohm isolating transformer. Some amplifiers include an integral transformer. Avaya/Lucent branded amplifiers are designed for connection to special paging output ports not provided on systems. They are not suitable for supporting mixed paging.

The transformer and amplifier must be connected when the system is restarted.

If background music is required between pages, the amplifier must support a separate background music connection and VOX switching.

The analog extension port is set as a Paging Speaker in the system configuration (**Extn | Analog | Equipment Classification**).

Short code/programmable button: Use DialPaging.

Related links

Paging on page 752

Chapter 71: System Events

The system supports a number of methods by which events occurring on the system can be reported. These are in addition to the real-time and historical reports available through the System Status Application (SSA).

SNMP Reporting

Simple Network Management Protocol (SNMP) allows SNMP clients and servers to exchange information. SNMP clients are built into devices such as network routers, server PC's, etc. SNMP servers are typically PC application which receive and/or request SNMP information. The system SNMP client allows the system to respond to SNMP polling and to send alarm information to SNMP servers.

In order for an SNMP server application to interact with a system, the MIB files provided with the Manager installation software must be compiled into the SNMP server's applications database.

Note:

- The process of 'on-boarding' (refer to the Deploying Avaya IP Office™ Platform SSL VPN Services) may automatically configure SNMP and create a number of SNMP alarm traps. These will override any existing SNMP configuration settings.

SMTP Email Reporting

The system can send alarms to an SMTP email server. Using SMTP requires details of a valid SMTP email account user name and password and server address. If SMTP email alarms are configured but for some reason the system cannot connect with the SMTP server, only the last 10 alarms are stored for sending when connection is successful. Use of SMTP alarms requires the SMTP server details to be entered in the SMTP tab.

Syslog Reporting

The system can also send alarms to a Syslog server (RFC 3164) without needing to configure an SNMP server. In addition Syslog output can include audit trail events.

Multiple event destinations can be created, each specifying which events and alarms to include, the method of reporting to use (SNMP, Syslog or Email) and where to send the events. Up to 2 alarm destinations can be configured for SNMP, 2 for Syslog and 3 for SMTP email.

Related links

Configuring Alarm Destinations on page 757

Configuring Alarm Destinations

About this task

The Alarms section of the System Events tab displays the currently created alarm traps. It shows the event destinations and the types of alarms that will trigger the send of event reports. Up to 2 alarm destinations can be configured for SNMP, 2 for Syslog and 3 for SMTP email.

Procedure

1. In the navigation pane, select **System**.
2. In the details pane, select **System Events** and then select the **Alarms** sub-tab.
3. Use the **Add**, **Remove** and **Edit** controls to alter the traps.
4. Click **Add** or select the alarm to alter and then click **Edit**.
5. For a new alarm, set the **Destination** to either **Trap (SNMP)** or **Syslog** or **Email (SMTP)**.

   Note that once a destination has been saved by clicking **OK** it cannot be changed to another sending mode.
6. The remaining details will indicate the required destination information and allow selection of the alarm events to include.
7. When completed, click **OK**.
8. Click **OK**again.

Related links

System Events on page 756

Chapter 72: Certificate Management

This section provides an overview of IP Office certificate support and management. For more comprehensive information, refer to the Avaya IP Office™ Platform Security Guidelines manual.

Related links

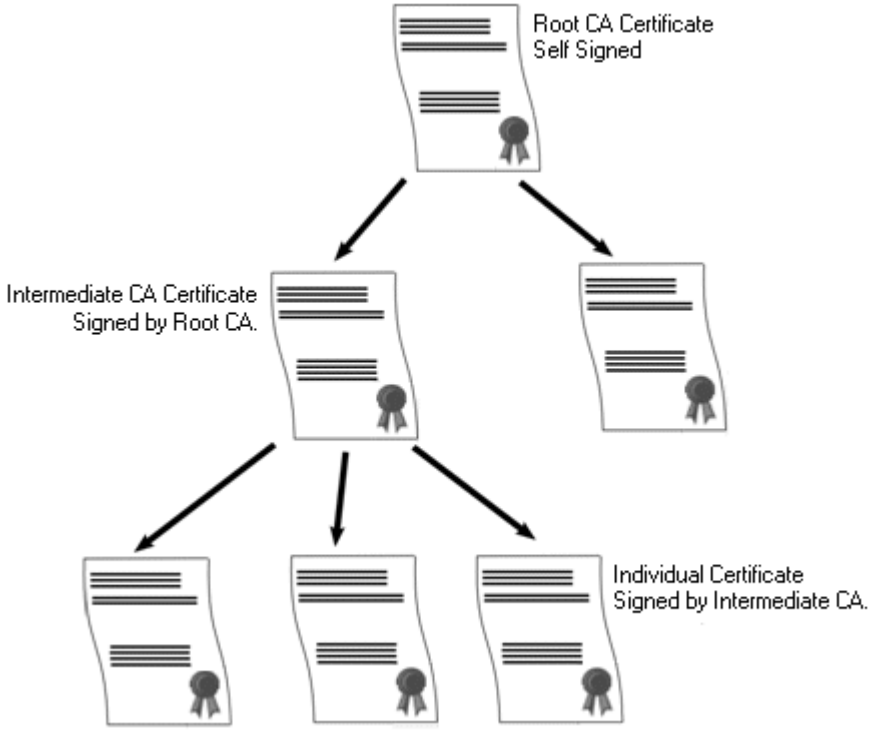
Certificate Overview on page 758
Certificate Support on page 763

Certificate Overview

Public key cryptography is one of the ways to maintain a trustworthy networking environment. A public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

The system used to provide public-key encryption and digital signature services is called a public key infrastructure (PKI). All users of a PKI should have a registered identity which is stored in a digital format and called an Identity Certificate. Certificate Authorities are the people, processes and tools that create these digital identities and bind user names to public keys.

There are two types of certificate authorities (CAs), root CAs and intermediate CAs. In order for a certificate to be trusted and for a secure connection to be established, that certificate must have been issued by a CA that is included in the trusted certificate store of the device that is connecting. If the certificate was not issued by a trusted CA, the connecting device then checks to see if the certificate of the issuing CA was issued by a trusted CA, and so on until either a trusted CA is found. The trusted certificate store of each device in the PKI must contain the required certificate chains for validation.



IP Office Root Certificate Authority

IP Office generates a self-signed certificate. For IP500 V2 systems, a certificate is generated automatically on the first start up. On Linux systems, a certificate is generated during the ignition process.

The following entities can act as the certificate authority.

- The Server Edition Primary Server, an Application Server, or a Unified Communication Module (UCM) can act as the root certificate authority for all nodes in the system.
- In Enterprise Branch deployments, the System Manager can act as the root certificate authority.
- Identity certificates can also be purchased and issued by a third party certificate authority.

Regardless of the method used to provide the IP Office identity, the certificate authority which signs the IP Office identity certificate must be trusted by all the clients and endpoints that need to establish a secure connection with IP Office. They must be a part of the PKI. Therefore, the root CA certificate must be downloaded to client devices and placed in the trusted certificate store. If there are intermediate CAs in the certificate chain, either the intermediate CAs must be added to the client device Trusted Certificate Store or the certificate chain must be advertised by IP Office in the initial TLS exchange.

Certificates and TLS

Telephony signaling like SIP messaging is secured using Transport Layer Security (TLS). TLS provides communication security using certificates to authenticate the other end of the IP Link.

The message exchange in TLS is aimed at verifying the identity of the communicating parties and establishing the keys that will be used to encrypt the signaling data between the two parties.

Typically, the server sends its identity certificate, either self-signed or signed by the CA, to the client. The client must have the CA certificate in its trusted certificate store.

IP Office acts as the TLS server in its interactions with SIP telephony clients. This means that the TLS application on the IP Office must be configured to listen for client connections by enabling TLS in the SIP Registrar on the LAN1 and LAN2 interfaces.

Note:

- Authentication of the client's certificate by the server is not a requirement. IP Office does not support client certificate validation for all SIP endpoint types.
- The E.129 phone does not validate the IP Office identity certificate.

Related links

Certificate Management on page 758
Windows Certificate Store on page 760

Windows Certificate Store

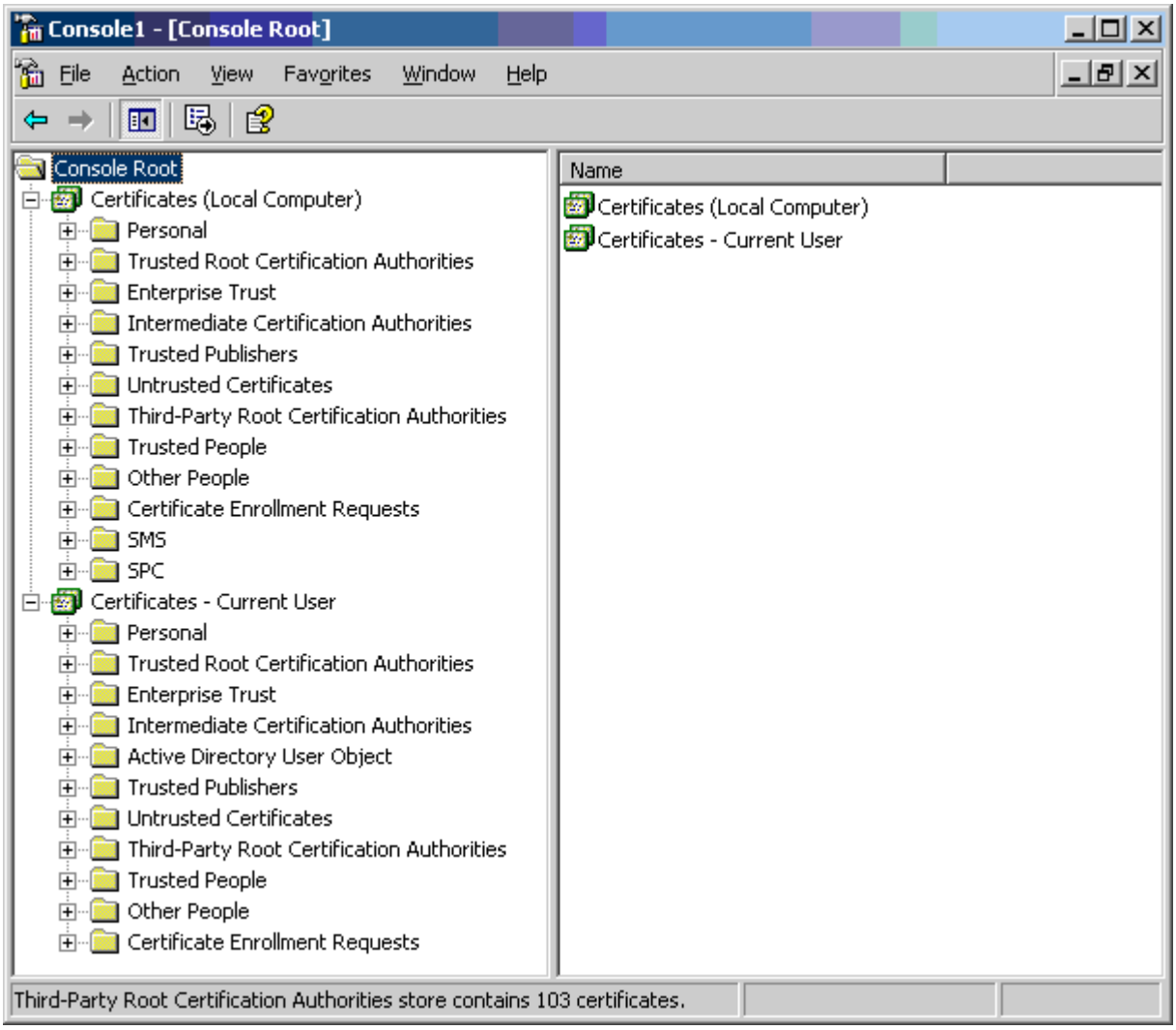
The certificate store used by Manager to save and retrieve X509 certificates is the default one provided by the Windows operating system. The Windows certificate store is relevant to any application running on Windows that uses certificates for security, either TLS or HTTPS.

Warning:

- Avaya accepts no responsibility for changes made by users to the Windows operating system. Users are responsible for ensuring that they have read all relevant documentation and are sufficiently trained for the task being performed.

Windows Certificate Store Organization

By default, certificates are stored in the following structure:



Each of the sub folders has differing usage. The Certificates - Current User area changes with the currently logged-in Windows user. The Certificate (Local Computer) area does not change with the currently logged-in Windows user.

Manager only accesses some of the certificate sub folder:

Certificates (Local Computer) Folder	Manager Use
Personal | Certificates	Folder searched by Manager 1st for matching certificate to send to the system when requested. Certificate matched by the subject name contained in **File | Preferences | Security | Certificate** offered to the system. Folder accessed whenever **'Local Machine certificate store'** used for Security Settings. Folder searched by Manager for matching certificate when certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.
Trusted Root Certification Authorities | Certificates	Folder searched by Manager for matching parent certificates when non-self signed certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.

Certificates – Current User Folder	Manager Use
Personal | Certificates	Folder searched by Manager 2nd for matching certificate (subject name) to send to the system when requested. Certificate matched by the subject name contained in **File | Preferences | Security | Certificate** offered to the system. Folder accessed whenever **'Current User certificate store'** used for Security Settings. Folder searched by Manager for matching certificate when certificate received from IP Office, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.
Trusted Root Certification Authorities | Certificates	Folder searched by Manager for matching parent certificates when non-self signed certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.
Other People | Certificates	Folder searched by Manager for matching parent certificates when non-self signed certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.

Windows Certificate Store Import

In order to use certificates – either for security settings or Manager operation – they must be present in the Windows certificate store. Certificates may be placed in the store by the Certificate Import Wizard. The Certificate Import Wizard can be used whenever a certificate is viewed.
In order for Manager to subsequently access this certificate the **Place all certificate in the following store** option must be selected:

- If the certificate is to subsequently identify the system, the Other People folder should be used.
- If the certificate is to subsequently identify the Manager, the Personal folder should be used, and the associated private key saved as well.

Certificate Store Export

Any certificate required outside of the Manager PC must be first saved in the Certificate store, then exported.

If the certificate is to be used for identity checking (that is, to check the far entity of a link) the certificate alone is sufficient, and should be saved in PEM or DER format.

If the certificate is to be used for identification that is, to identify the near end of a link) the certificate and private key is required, and should be saved in PKCS#12 format, along with a password to access the resultant .pfx file.

Related links

Certificate Overview on page 758

Certificate Support

Related links

Certificate Management on page 758
Certificate File Naming and Format on page 763
Identity Certificate on page 764
Trusted Certificate Store on page 766
Signing Certificate on page 767
Certificate File Import on page 769

Certificate File Naming and Format

DER: Distinguished Encoding Rules (DER) format, which is a binary format used to represent a certificate. Typically used to describe just one certificate, and cannot include a private key.

There are four main encodings/internal formats for certificate files. Note that these are encodings, not file naming conventions.

PEM: Privacy Enhanced Mail (PEM) is a Base 64 (i.e. ASCII text) encoding of DER, one certificate is enclosed between '-----BEGIN CERTIFICATE-----' and '-----END CERTIFICATE-----' statements. Can contain a private key enclosed between '-----BEGIN PRIVATE KEY -----' and '-----END BEGIN PRIVATE KEY -----' statements. More than one certificate can be included. PEM can be identified by viewing the file in a text editor. This is an unsecure format and not recommended for private key use unless it is protected with a password.

PKCS#12: Public Key Cryptography Standard (PKCS) #12. A secure, binary format, encrypted with a password. Typically used to describe one certificate, and its associated private key, but can also include other certificates such as the signing certificate(s). This is the recommended format for private key use.

PKCS#7: A Base 64 (i.e. ASCII text) encoding defined by RFC 2315, one or more certificates are enclosed between '—BEGIN PKCS—' & '—END PKCS7—' statements. It can contain only Certificates & Chain certificates but not the private key. Can be identified by viewing the file in a text editor.

There are many common filename extensions in use:

- .CRT — Can be DER or PEM. Typical extension used by Unix/Android systems' public certificates files in DER format.

- .CER — Can be DER or PEM. Typical extension used by Microsoft/Java systems' public certificates files in PEM format.
- .PEM — Should only be PEM encoded.
- .DER — Should only be DER encoded.
- .p12 — Should only be in PKCS#12 format. Typical extension used by Unix/Android systems' identity certificates/private key pair files. Same format as .pfx hence can be simply renamed.
- .pfx — Should only be in PKCS#12 format. Typical extension used by Microsoft systems' identity certificates/private key pair files. Same format as .p12 hence can be simply renamed.
- .pb7 — Should only be in RFC 2315 format. Typical extension used by Microsoft and Java systems for certificate chains.

Related links

Certificate Support on page 763

Identity Certificate

Feature	Support	Notes
Import: Public key size	Yes	RSA 1024, 2048 and 4096 bit public keys must be supported. Any other sizes are optional. Import of RSA public key less than 1024 or greater than 4096 bits to be rejected with an informative error. Import of certificates with 1024 will be imported after a warning 'The certificate public key may not be of sufficient strength. Do you wish to continue?'
Import: Certificate signature algorithm	Yes	SHA-1, SHA-256 SHA-384, and SHA-512 hashing algorithms must be supported. Any other SHA2 algorithms are optional. Import of certificates with SHA-1 will be imported after a warning 'The certificate signature algorithm may not be of sufficient strength. Do you wish to continue?' Import of certificates with other algorithms (for example MD5, ECC) to be rejected with an informative error.
Import: Must have private key	Yes	Must be supplied. Reject and informative error that private key has not been supplied
Import: Certificate checks	Yes	Minimum checks for: • Version (v3) • Start + end (present) • Subject Name (present) • Issuer Name (present) • Data integrity (e.g. hash) Reject + informative error if a check fails

Table continues…

Feature	Support	Notes
Import: Certificate up to 4KB	Yes	Certificates can be varying sizes
Import: Formats	Yes	• PKCS#12 format. '.p12' and '.pfx' file extension. With or without password. This shall be the preferred/default option • PEM format. '.cer' '.pem' and '.crt' file extension. • Pasted from clipboard in PEM format (optional) NOTE that ONLY PKCS#12 file format is acceptable according to 147434–030–P1, however we cannot control what format customers receive their certificates in, hence all should be supported See section below for certificate file import support
Import: Up to 4 other certificates in same file	Yes	Only supported where management of TCS also available. • Any intermediate and root CA certificate included in the PKCS#12 file to be imported into the Trusted Certificate store • The feature is intended for import of intermediate certificates, but can include unrelated certificates. • An informative message to the admin if any have been imported
Import: Certificate chain support	Yes	Where identity certificate is signed by one or more intermediate CAs, search TCS for matching certificates and include in identity certificate chain.
View: Certificate Contents	Yes	Minimum viewable attributes (From CEC016: 147434–030–P1): • Serial Number • Subject Name • Issuer Name • Validity Period (that includes notBefore and notAfter dates) • Thumbprint (Hash of the certificate) • Subject Alternative Names • Key Usage Extensions • Extended Key Usage Warnings/errors as per 147434–080–P1: • Error displayed that certificate has expired • Warning displayed that certificate is nearing expiry (within 60 days).
View: Private Key	No	Private key must not be viewable
Export: Formats	Yes	Private key must not be exportable Export formats: • DER format. '.cer' '.der' and '.crt' file extension. • PEM format. '.cer' '.pem' and '.crt' file extension. • PKCS#12 (optional)

Related links

Certificate Support on page 763

Trusted Certificate Store

Feature	Support	Notes
Import: RSA 1024-4096 key size	Yes	RSA 1024, 2048 and 4096 bit public keys must be supported. Any other sizes are optional. Import of RSA public key less than 1024 or greater than 4096 bits to be rejected with an informative error.
Import: Optional private key	Yes	No private key will actually be imported. Informative message (neither warning or error) that private key has not been imported
Import: Certificate checks	Yes	Minimum checks for: • Version (v3) • Start + end (present) • Subject Name (present) • Issuer Name (present) • Data integrity (e.g. hash) Reject + descriptive error if a check fails
Import: Certificate up to 4KB	Yes	Certificates can be varying sizes
Import: Formats	Yes	• DER format. '.cer' '.der' and '.crt' file extension. • PEM format. '.cer' '.pem' and '.crt' file extension. • PKCS#12 format. '.p12' and '.pfx' file extension. With or without password. • Pasted from clipboard in PEM format (optional)
Import: Up to 19 other certificates in same file	Yes	All included certificates, up to 20 total. More than 20 in one file can be optionally supported.

Table continues…

Feature	Support	Notes
View: TCS Certificate	Yes	Minimum viewable attributes (From CEC016: 147434–030–P1): • Serial Number • Subject Name • Issuer Name • Validity Period (that includes notBefore and notAfter dates) • Thumbprint (Hash of the certificate) • Subject Alternative Names • Key Usage Extensions • Extended Key Usage Warnings/errors as per 147434–080–P1: • Error displayed that a certificate has expired • Warning displayed that a certificate is nearing expiry (within 60 days).
Export: Formats	Yes	Export formats: • DER format. ‘.cer’ ‘.der’ and ‘.crt’ file extension. • PEM format. ‘.cer’ ‘.pem’ and ‘.crt’ file extension. • PKCS#12 (optional)

Related links

Certificate Support on page 763

Signing Certificate

Feature	Support	Notes
Import: RSA 1024-4096 key size	Yes	RSA 1024, 2048 and 4096 bit public keys must be supported. Any other sizes are optional. Import of RSA public key less than 1024 or greater than 4096 bits to be rejected with an informative error.
Import: Must have private key	Yes	Must be supplied. Reject and informative error that private key has not been supplied

Table continues…

Feature	Support	Notes
Import: Certificate checks	Yes	Minimum checks for: • Version (v3) • Start + end (present) • Subject Name (present) • Issuer Name (present) • Data integrity (e.g. hash) Reject and informative error if a check fails
Import: Certificate up to 4KB	Yes	Certificates can be varying sizes
Import: Formats	Yes	• PKCS#12 format. '.p12' and '.pfx' file extension. With or without password. This shall be the preferred/default option • PEM format. '.cer' '.pem' and '.crt' file extension. • Pasted from clipboard in PEM format (optional) NOTE that ONLY PKCS#12 file format is acceptable according to 147434–030–P1, however we cannot control what format customers receive their certificates in, hence all should be supported
Import: Other certificates in same file	No	Informative warning that other certificates have not been imported
View: TCS Certificate	Yes	Minimum viewable attributes (From CEC016: 147434–030–P1): • Serial Number • Subject Name • Issuer Name • Validity Period (that includes notBefore and notAfter dates) • Thumbprint (Hash of the certificate) • Subject Alternative Names • Key Usage Extensions • Extended Key Usage Warnings/errors as per 147434–080–P1: • Error displayed that certificate has expired • Warning displayed that certificate is nearing expiry (within 60 days).

Table continues…

Feature	Support	Notes
Renew existing:	Yes	Regenerate CA keeping all keys and other contents same except: • notBefore and notAfter dates • Serial Number • Thumbprint (Hash of the certificate) • ?? Can this be done to imported CAs or just internally generated ones?
Create new:	Yes	Regenerate CA, including keys
Export: Formats	Yes	Private key must not be exportable Export formats: • DER format. '.cer' '.der' and '.crt' file extension. • PEM format. '.cer' '.pem' and '.crt' file extension. • PKCS#12 (optional)

Related links

Certificate Support on page 763

Certificate File Import

File Content	Identity Certificate Import Command	Trusted Certificate Import Command	Signing Certificate Import Command	Notes
DER				
DER: 1 certificate	No – attempt rejected with 'Invalid certificate format (DER)'	Yes – attempt accepted with 'N certificate(s) imported into Trusted Certificate Store'	No – attempt rejected with 'Invalid certificate format (DER)'	
DER: Any other content	No – attempt rejected with 'Invalid content (DER)'	No – attempt rejected with 'Invalid content (DER)'	No – attempt rejected with 'Invalid content (DER)'	
PKCS#12				
PKCS#12: 1 certificate + private key	Yes – attempt accepted with 'Certificate import successful' Certificate/key imported as ID certificate	No – p12/pfx should not be offered for file selection	Yes – attempt accepted with 'Certificate import successful'	

Table continues…

File Content	Identity Certificate Import Command	Trusted Certificate Import Command	Signing Certificate Import Command	Notes
PKCS#12: 1 certificate + private key, 1 or more other certificates	Yes – attempt accepted with 'Certificate import successful' Certificate/key imported as ID certificate Other certificates imported into TCS with 'N certificate(s) imported into Trusted Certificate Store'	No – p12/pfx should not be offered for file selection	Yes – attempt accepted with 'Certificate import successful' Certificate/key imported as signing certificate Other certificates ignored	At least 20 certificates supported in the same file
PKCS#12: Any other content	No – attempt rejected with 'Invalid content (PKCS#12)'	No – p12/pfx should not be offered for file selection	No – attempt rejected with 'Invalid content (PKCS#12)'	
PEM: 1 Certificate	No – attempt rejected with 'Invalid certificate format (PEM – no private key)'	Yes – attempt accepted with 'N certificate(s) imported into Trusted Certificate Store'	No – attempt rejected with 'Invalid certificate format (PEM – no private key)'	Certificate can be encrypted on unencrypted
PEM				
PEM: N Certificate	No – attempt rejected with 'Invalid certificate format (PEM – no private key)'	Yes – attempt accepted with 'N certificate(s) imported into Trusted Certificate Store'	No – attempt rejected with 'Invalid certificate format (PEM – no private key)'	At least 20 certificates supported in the same file Certificate can be encrypted on unencrypted
PEM: 1 Certificate + private key	Yes – attempt accepted with 'Certificate import successful' Certificate/key imported as ID certificate	No – attempt rejected with 'Invalid certificate format (PEM)'	Yes – attempt accepted with 'Certificate import successful' Certificate/key imported as signing certificate	Certificate or Key can be encrypted on unencrypted

Table continues…

File Content	Identity Certificate Import Command	Trusted Certificate Import Command	Signing Certificate Import Command	Notes
PEM: 1 Certificate + private key, 1 or more other certificates. Private key must be before or after the first certificate	Yes – attempt accepted with 'Certificate import successful' Certificate/key imported as ID certificate. Other certificates imported into TCS with 'N certificate(s) imported into Trusted Certificate Store'	Yes – attempt accepted with 'N certificate(s) imported into Trusted Certificate Store' First certificate and private key ignored	Yes – attempt accepted with 'Certificate import successful' Certificate/key imported as signing certificate Other certificates ignored	Private key must be before or after the first certificate Certificate or Key can be encrypted on unencrypted
PEM: Any other content	No – attempt rejected with 'Invalid content (PEM)'	No – attempt rejected with 'Invalid content (PEM)'	No – attempt rejected with 'Invalid content (PEM)'	Option to include more detail of the rejection cause.e.g. 'Cannot detect Identity Certificate', 'Too many private keys', 'Unrecognized header' etc.

Related links

Certificate Support on page 763

Chapter 73: Configuration for Emergency Calls

This page provides a summary of IP Office emergency call handling. For full details, refer to the IP Office Emergency Call Configuration manual.

The configuration of every system must contain at least one short code using the **Dial Emergency** feature. **Dial Emergency** overrides all external call barring that may have been applied to the user whose dialing has been matched to the short code. You must still ensure that no other short code or extension match occurs that would prevent the dialing of an emergency number being matched to the short code.

The short code (or codes) can be added as a system short code or as an ARS record short code. If the **Dial Emergency** short code is added at the solution level, that short code is automatically replicated into the configuration of all servers in the network and must be suitable for dialing by users on all systems. Separate **Dial Emergency** short codes can be added to the configuration of an individual system. Those short codes will only be useable by users currently hosted on the system including users who have hotdesked onto an extension supported by the system.

It is the installers responsibility to ensure that a **Dial Emergency** short code or codes are useable by all users. It is also their responsibility to ensure that either:

- the trunks via which the resulting call may be routed are matched to the physical location to which emergency service should be dispatched
- the outgoing calling line ID number sent with the call matches the physical location from which the user is dialing.
- If the system uses external dialing prefixes, you should also ensure that the dialing of emergency numbers with and without the prefix is allowed.

The blocking or rerouting of emergency calls to a intermediate destination other than the emergency response service may be against local and nation laws.

Hot Desking Users

In addition to the location requirements above, you must also remember that for users who hot desk, from the networks perspective the user's location is that of the system hosting the extension onto which the user is currently hotdesked. If that is an IP extension then that location is not necessarily the same as the physical location of the server.

Emergency call setup

Routing of emergency calls is based on a call resolving to a **Dial Emergency** short code. Based on the location value for the extension making the call, routing is performed by the **Emergency**

ARS form configured for that location. You must ensure that the short codes in the ARS use lines appropriate for emergency calls from that location.

Configuring emergency call routing

At its simplest, Create a **Dial Emergency** system short code. Note that the **Line Group ID** value in the **Dial Emergency** short code is overridden if the extension's **Locations** has an **Emergency ARS** defined.

1. Create system short codes for each emergency number used in the system locale. The short codes should use the **Dial Emergency** feature. Add short codes for the same numbers dialed with and without any expected external dialing prefixes.
2. Create an emergency ARS. This should containing shorts codes that take the output of the system short codes created above and dials them to the external trunks that should be used for emergency calls from the system.
3. Create a **Location** for the system and set the **Emergency ARS** to the ARS created above.
4. Set the location as the system's **Location** value on the System | System page.
5. For each **Extn**, set the **Location** defined above.
6. Test the correct operation of emergency dialing.
7. For networks with multiple systems and locations, create additional emergency ARS entries and locations as necessary to ensure that emergency calls from any location are sent using appropriate trunks.

Related links

Emergency Call Indication on page 773
System Alarm Output on page 774

Emergency Call Indication

IP Office R11.1 SP1 added support for a **911 View** or **Emergency View** programmable button.

- A button set to this function indicates to users on the same system when the IP Office has routed an emergency call out one of its external PSTN trunks.
  - The button gives a ring and flashes when there is a connected emergency call in progress.
  - The button remains lit when there are details of previous emergency calls in the IP Office system's emergency call history.
- Pressing the button displays details of currently connected emergency calls (the first 10 such calls).
- After pressing the button, the **History** option displays details of any previously connected emergency calls (the first 30 such calls) and allows deletion of those call details.
- On J189 phones, the details include the location name if the IP Office used a **Location** record as part of the emergency call routing.
- All users on the IP Office share the same emergency call history information. Changes to the emergency call history affect the details shown on all phones on the same system.

Related links

Configuration for Emergency Calls on page 772

System Alarm Output

You can configure the IP Office system to generate a system alarm for any call that uses a **Dial Emergency** short code. In addition to reporting connected calls, the alarms also report emergency call attempts that fail for reasons such as no available trunks.

Unlike SMDR call records which the IP Office system generates at the end of a call, the IP Office generates emergency call system alarms immediately a call matches a **Dial Emergency** short code. This is important, as the PSAP emergency operator can stay on the line until the first responders arrive.

You can configure the IP Office to send system alarms to SNMP, syslog, or email. On-site notification applications can use the alarm message to offer a variety of features. For example:

- Email/IM/SMS/Pager alerts with escalation and acknowledgments.
- Location maps with additional information. For example; hazardous material warnings.
- Emergency call alert displays for reception/security desks.
- Printing of alerts for physical archiving.

Alarm Information

The IP Office provides the following information in the alarm:

- The location name.
- The number dialed by the caller.
- If connected, the called number and ELIN presented on the call. Otherwise, the reason for failure.
- The extension's current logged in user, otherwise `NoUser`. For tandem calls, the *Trunk ID*.
- The extension details and system ID plus:
  - For digital and analog extensions, the physical port details.
  - For telecommuter and mobile call control users, the external phone number.
  - For IP phones and softphone clients, the MAC and IP Address details.

Related links

Configuration for Emergency Calls on page 772

Chapter 74: Ring Tones

Ring tones can be defined in the following terms.

Distinctive Ringing - Inside, Outside and Ringback:

A distinctive ring tone can be given for each of the different call types: an internal call, an external call and a ringback calls (voicemail calls, ringback when free calls, calls returning from park, hold or transfer).

The distinctive ringing patterns used for most non-analog phones are as follows:

- **Internal Call**: Repeated single-ring.
- **External Call**: Repeated double-ring.
- **Ringback Call**: Two short rings followed by a single ring.

Note:

For non-analog extensions, the ringing pattern used for each call type by the system is not configurable.

Personalized Ringing:

This term refers to control of the ringing sound through the individual phones. For non-analog phones, while the distinctive ringing patterns cannot be changed, the ringer sound and tone may be personalized depending on the phone's own options. Refer to the appropriate telephone user guide.

Analog Phone Ringing Patterns

For analog extensions, the ringing pattern used for each call type can be set using the settings on **System Settings** > **System** > **Telephony**. The setting for an individual user associated with an analog extension can be configured using the settings on **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Settings**.

Note that changing the pattern for users associated with fax and modem device extensions may cause those devices to not recognize and answer calls.

The selectable ringing patterns are:

- **RingNormal** This pattern varies to match the **Locale** set in the **System | System** tab. This is the default for external calls.
- **RingType1**: 1s ring, 2s off, etc. This is the default for internal calls.
- **RingType2**: 0.25s ring, 0.25s off, 0.25s ring, 0.25s off, 0.25s ring, 1.75s off, etc. This is the default for ringback calls.
- **RingType3**: 0.4s ring, 0.8s off, …

- **RingType4**: 2s ring, 4s off, …
- **RingType5**: 2s ring, 2s off, …
- **RingType6**: 0.945s ring, 4.5s off, …
- **RingType7:** 0.25s ring, 0.24 off, 0.25 ring, 2.25 off, …
- **RingType8**: 1s ring, 3s off, …
- **RingType9**: 1s ring, 4s off, …
- **RingType0**: Same as **RingNormal** for the United Kingdom locale.
- **Default Ring**: Shown on the User | Telephony | Call Setting tab. Indicates follow the settings on the System | Telephony | Tones & Music tab.

Configuring Ring Tone Override for Groups and Incoming Call Routes

You can configure ring tone override for groups and incoming call routes. **Ring Tone Override** is supported on 1400 and 9500 series phones.

Note that you can use short codes to configure a ring tone plan by using the “r” character as part of the short code telephone number field. See Short Code Characters on page 975.

1. In Web Manager, select **System Settings** > **System** > **Telephony** > **Ring Tones**.
2. In the **Ring Tone Plan** table, enter a **Name** for the ring tone. The **Number** field is populated automatically.
3. Under **Ring Tone**, select one of the eight ring tones from the drop down list.
4. Once configured in this table, ring tone names can be selected from the **Ring Tone Override** field at:
   - **Call Management** > **Group** > **Add/Edit Group** > **Group**
   - **System Settings** > **Incoming Call Route** > **Add/Edit Incoming Call Route**

Chapter 75: Music On Hold

Each system can provide music on hold (MOH) from either internally stored files or from externally connected audio inputs. Each system has one system source and then a number of alternate sources (up to 3 alternate sources on IP500 V2 and 31 alternate sources on Server Edition).

You must ensure that any MOH source you use complies with copyright, performing rights and other local and national legal requirements.

WAV Files

The system can use internal files that it stores in its non permanent memory. The WAV file properties must be in the format listed below. If the file downloaded is in the incorrect format, it will be discarded from memory after the download.

- PCM, 8kHz 16-bit Mono.
- Maximum length: 90 seconds on IP500 V2 systems, 600 seconds on Linux-based systems.

The first WAV file, for the system source, must be called `HoldMusic.wav`. Alternate source WAV file names:

- Up to 27 IA5 characters with no spaces.
- Any file extension.
- On Linux-base systems, the filename is case sensitive.

The files, when specified by the system source or an alternate source setting, are loaded as follows:

- Following a reboot, the system will try using TFTP to download the file or files.
- The initial source for TFTP download is the system's configured **TFTP Server IP Address** (**System | System | LAN Settings**). The default for this is a broadcast to the local subnet for any TFTP server.
- Manager can act as a TFTP server while it is running. If Manager is used as the TFTP server, then the wav file or files should be placed in the Manager applications working directory.

  Note:

  The following Manager settings are disabled by default:

  - **Security Settings | Unsecured Interfaces | Applications Controls | TFTP Directory Read**
  - **File | Preferences | Preferences | Enable BootP and TFTP Servers**
- On Linux based systems, if no successful TFTP download occurs, the system automatically looks for the files in the `opt/ipoffice/tones/mohwavdir` folder (`disk/tones/mohwavdir` when access using file manager).

- The name of the system music .wav file should be **HoldMusic.wav**. The name of alternate source .wav files should be as specified in the **Alternate Sources** table (**System | Telephony | Tones and Music**) minus the **WAV**: prefix.

WAV File Download and Storage:

- If no successful TFTP download occurs:
  - On IP500 V2 systems, the system automatically looks for the file in the `system/primary` folder on the System SD card and downloads it from if found.
  - On Linux based systems, the system automatically looks for the file in the folder `opt/ipoffice/system/primary` folder (`disk/system/primary` when accessed using file manager) and downloads it from there if found.
- If a music on hold file is downloaded, the system automatically write a copy of that file to its memory card, overwriting any existing file of the same name already stored on the card.
- For files downloaded from a System SD card, the system will download the file again if the SD card is shutdown and restarted or if files are uploaded to the card using the Embedded File Manager.
- The system will download the file again if new files are copied to the disk or uploaded using File Manager.

Tone

If no internal music on hold file is available and **External** is not selected as the **System Source**, then the system provides a default tone for music on hold. The tone used is double beep tone (425Hz repeated (0.2/0.2/0.2/3.4) seconds on/off cadence). **Tone** can be selected as the **System Source**, overriding both the use of the external source port and the downloading of **HoldMusic.wav**.

Controlling the Music on Hold Source Used for Calls

Unless specified, the System Source is used for any calls put on hold by system users. For any call, the last source specified for the call is the one used. The following options allow the source to be changed.

- **Hunt Group** Each hunt group can specify a **Hold Music Source** (**Group | Group**). That source is then used for calls presented to the hunt group.

  In a multi system network, a hunt group member will hear the music on hold (MOH) from their local system. For example, a call comes in to site A and rings a hunt group with members from system A and system B. If a hunt group member from system B answers a call and puts the call on hold, the caller hears the MOH from system B.
- **Incoming Call Route** Each incoming call route can specify a **Hold Music Source** (**Incoming Call Route | Standard**). That source is then used for incoming calls routed by that incoming call route.
- **Short Code** The **h** character can be used in the **Telephone Number** field of short codes to specify the hold music to associate with calls routed by that short code. The format **h(X)** is used where **X** is the source number. This method can be used to specify a hold music source for outgoing calls.

Checking Music on Hold

The system short code feature Hold Music can be used to listen to the hold music sources. Dial ***34N#**, replacing **N** with the source number 1 (System Source) or 2 to 32 (Alternate Sources).

Related links

System Source on page 779
Alternate Source on page 779

System Source

The first source is called the **System Source**. This source is numbered source 1. The possible options for this source are:

Setting	Description
WAV	Use the `HoldMusic.wav` file. The IP Office loads the file using TFTP, or you can directly add the file using the embedded file manager.
WAV (restart)	Identical to WAV except that for each new listener, the file plays from the beginning. • Not supported on IP500 V2 systems. • Cannot be used as a centralized source.
External	Applicable to IP500 V2 systems. Use the audio source connected to the **Audio** port on the control unit.
Tone	Use a double beep tone: 425Hz, 02./0.2/0.2/3.4 seconds on/off. • This tone is also used if the system source is set to **WAV File** but the `HoldMusic.wav` file has not been successfully loaded.

Related links

Music On Hold on page 777

Alternate Source

You can specify alternate MOH sources on the **System Settings** > **System** > **Telephony** > **Tones and Music** page.

You can assigned the alternate sources as the **Hold Music Source** for an **Incoming Call Route** or a **Group**.

- That assigned MOH source overrides any current MOH source associated with the call.
- The assigned MOH source remains associated with the call as it moves around the IP Office system. This is done using the number of the MOH source (with 1 being the number of the default system source).

- If the call moves to another IP Office system in a multi-site network, the source with the same number of the other system is used if also configured on that system.
-
-

IP500 V2 Alternate Sources

For IP500 V2 systems, you can specify up to 3 alternate sources. Those different types of alternate source supported are:

Alternate Option	Description
`WAV:<filename>`	Play a specified file from its start or, if already in use, for where it is already playing. • The `<filename>` parameter specifies the file to play: - Up to 27 IA5 characters with no spaces. - Any file extension. - On Linux-base systems, the filename is case sensitive. • The file location is `/system/primary`. • When the source is activated, the playback resumes from where it left off last time, instead of starting every time from the beginning. • At any moment, all users listening to this source hear the same thing.
`XTN:<extension>`	Play the source connected to a analog extension port on a IP500 V2 systems. • You can set any analog extension with its **Equipment Classification** set as **MOH Source** as an alternate source. • The `<extension>` parameter specifies the analog extension's **Base Extension** number. For example: `XTN:224`

Linux-based IP Office system

For a Linux-based IP Office system, you can specify up to 31 alternate sources. The different types of alternate source are:

Alternate Option	Description
LINE:<X>,<Y>	Use an alternate source from another IP Office system in the network. • You specify the line source using two parameters: - <X> = The line number of the connection to the other Linux-based IP Office system (not the outgoing group ID). - <Y> = The MOH source number on the other Linux-based server. • WAVRST and WAVDIRRST alternate sources are not supported. • When the IP Office requires the source, it creates a VoIP call to the source IP Office system. This uses call capacity from the trunk and can be subject to CAC limits. • The IP Office drops calls to the source after 30 seconds of no use. You can change the time using the NoUser source number HOLD_MUSIC_TIMEOUT=x. x is the number of seconds. The range is 1 to 600 seconds.
USB:<n>	Play the music streamed by a USB sound device connected to the IP Office system. • The IP Office supported up to four USB sources. Not supported on virtual IP Office systems. • <n> is the logical USB device number. - USB:1 is the first source found. This IP Office automatically uses this as the **System Source** when that is set to **External**. - Linux servers number additional devices sequentially. For example; USB:1, USB:2, and so on. • The IP Office auto-configures itself as follows: - It selects Line input and sets the volume close to maximum. - If it cannot identify a line input, it uses the microphone input. • External USB sound devices are hot-pluggable. However, you must take care when adding or removing USB sound cards, as this can change the logical number of the device. - When an USB MOH source is unavailable, the default MOH tone is played instead.
WAV:<filename>	Play a specified file from its start or, if already in use, for where it is already playing. • The <filename> parameter specifies the name of the file to played: - Up to 27 IA5 characters with no spaces. - Any file extension. - On Linux-base systems, the filename is case sensitive. • The file location is opt/ipoffice/system/primary. • When the source is used, playback resumes from where it left off last time, instead of starting from the beginning. • At any moment, all users listening to this source hear the same thing.

Table continues…

Alternate Option	Description
`WAVRST:<file>`	Play a specified file, beginning from its start for each caller. • Operates similarly to `WAV:<filename>` above, but for each caller, playback starts from the beginning.
`WAVDIR:`	Play the files located in the IP Office system's `mohwavdir` directory. • The directory used `/disk/tones/mohwavdir` (file manager access). • Supports up to 255 files. Each file up to 10 minutes. • The files are played in filename order (numerical, lower case, then upper case). • At any moment, all users listening to the source hear the same thing. • Only one `WAVDIR:` or `WAVDIRRST:` entry is supported on an IP Office system.
`WAVDIRRST:`	Play the files located in the IP Office system's `mohwavdir` directory, restarting from the first file for each caller. • Operates similarly to `WAVDIR:` above, but for each caller playback starts from the beginning of the first file in the folder. • Only one `WAVDIR:` or `WAVDIRRST:` entry is supported on an IP Office system.

Related links

Music On Hold on page 777

Chapter 76: System Date and Time

IP Office servers can obtain their date and time either automatically from a time server or have it set manually.

How Does the System Use the Date and Time

For files stored on memory cards the system uses the UTC time. For other activities such as call logs, SMDR records, time display on phones; the local system time (UTC + any offsets) is used.

Related links

System Date and Time Options on page 783
Applying Daylight Saving on page 784
Checking Automatic Time and Date Operation on page 785
Manually Changing the System Date and Time on page 786

System Date and Time Options

IP Office servers can obtain their date and time either automatically from a time server or have it set manually.

Important:

- It is strongly recommended to always use the address of an internet time server to automatically obtain the date and time. An accurate time and date is essential to all features that use security certificates. Manually setting the time and date should be avoided.

Linux-based IP Office Systems

The date and time source settings are set through the server's **Platform View** menus using the **Settings | System | Data and Time** settings.

The supported options are:

Option	Description
SNTP	Use the date and time provided by an SNTP time server. The UTC time provided by the time server is then adjusted using the server's timezone setting. If you have a network of servers, it is typical to set the primary server to use an external SNTP source and all other servers are set to use SNTP from the primary server's own address.
Manual	Enter the date and time through the platform view menu.

IP500 V2 Systems

The time and date settings for these systems are configured through their **Time Setting Config Source** settings (**System Settings** > **System** > **System**).

The supported options are:

Option	Description
SNTP	Get the date and time from an SNTP time server in the same way as Linux based systems above do.
Voicemail Pro/ Manager	Get the date and time from the Windows PC running either the Voicemail Pro or IP Office Manager applications. This option requires the application to be running when the IP Office is started and for regular time updates.
None	Get the date and time from values entered via a system phone. See Manually Changing the System Date and Time on page 786.

Related links

System Date and Time on page 783

Applying Daylight Saving

You can have the IP Office apply daylight saving time (DST) changes at certain times of the year. How you do this depends on the type of IP Office server and the type of time source you have configured it to use:

Server Type	Description
Linux-based Server	Daylight saving adjustments are applied to the SNTP time by defining a **Location** for the system. The location settings include the time zone the system it is in and whether to apply daylight saving changes for that location.

Table continues…

Server Type	Description
IP500 V2 Server	The method of applying daylight saving depends on the time source used by the server: • **SNTP/None:** The **System Settings** > **System** > **System** menu includes settings for specifying when to apply daylight saving. - The system can still also use a **Location** to override the timezone and daylight saving settings of the system. • **Voicemail Pro/Manager:** *(Obsolete)* If the system is obtaining its time from a Windows PC running Voicemail Pro or IP Office Manager. The PC needs to be configured to apply DST to the time it provides.

Using Locations to Apply DST

In a network of IP Office systems, it may be necessary for some systems or extensions, to have different time and date settings to match where they are physically located. This can be done by adding **Location** entries to the configuration.

Each location can include a time offset from the UTC time and a set of daylight saving settings for the location. You can then:

- Associate IP Office systems with their locations.
- Associated extension and lines with different locations if they require different settings from their host IP Office system.

Editing the DST Calendar

Based on the system's selected timezone, the IP Office automatically adds a set of dates for when daylight saving is applied and removed. The dates are editable.

- The current dates for applying and removing the DST settings are shown below the **Automatic DST** option on the **System** > **System** and **Location** > **Location** menus.
- Each entry specifies when the IP Office should apply an additional time offset, and when the IP Office should remove the additional time offset.
- You can use the adjacent **Edit** and **Delete** buttons to adjust the calendar entries.
- Note that the list can only include 10 entries (20 for IP Office R11.1.3.2 and higher).
  - To add a new entry, you may need to delete an existing entry. After doing that, **Add New Entry** appears at the bottom of the list.

Related links

System Date and Time on page 783

Checking Automatic Time and Date Operation

Operation of an IP Office server's time and date operation can be checked using the System Status Application. Within System Status Application, the **Resources** > **Time** menu displays the current date and time, the time source, results of the last time request and other settings.

Investigating Potential Time and Date Issues

When using an internet based time server, check the following:

1. Check the configured time server address.
2. Check routing from the server to the internet via the customer's network.
   - For Linux-based servers, check the default gateway address for the customer's network is shown in the server's Platform View menus.
   - For all servers, check that the configuration includes a default IP Route to the customer network's default gateway address.

Related links

System Date and Time on page 783

Manually Changing the System Date and Time

It is strongly recommended that IP Office systems obtain their time and date automatically from an internet based time server. However, if configured otherwise, the following methods can be used to change the current system time and date.

Linux-based IP Office Systems

For a Linux-based IP Office system, the system date and time can be set through the server's **Platform View** menus using the **Settings | System | Data and Time** settings.

IP500 V2 Systems

For IP500 V2 systems set to no time server source, date and time changes can be done though the phone menus of a user who has been give **System Phone Rights** (see System Phone Features on page 846). The user's **Login Code** is used to restrict access to the time and date settings menu on the phone.

How the user accesses the date/time settings depends on the type of phone:

Phone type	Details
1400, 1600, 9500, 9600 and J100 Series	For a user with **System Phone Rights**, on these phones the user can set the system time and date by selecting **Features	Phone User	System Administration**. • This does not include the 1403, 1603 and J129 phones. • If the system has been configured with a time server, this option can still used to display time and date information but cannot be used to change it.

Related links

System Date and Time on page 783

Chapter 77: Configuring Time Profiles

Time profiles are configured on **System Settings** > **Time Profiles**

Time Profiles are used by different services to change their operation when required. In most areas where time profiles can be used, not setting a time profile is taken as meaning 24-hour operation.

Time profiles consist of recurring weekly patterns of days and times when the time profile is in effect.

Time profiles can include time periods on specified calendar days when the time profile is in effect. Calendar records can be entered for the current and following calendar year.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Time profiles are used by the following record types.

Hunt Group:

A time profile can be used to determine when a hunt group is put into night service mode. Calls then go to an alternate Night Service Fallback group if set, otherwise to voicemail if available or busy tone if not.

Setting and clearing hunt group night service can be done using either manual controls or using a system time profile. The use of both methods to control the night service status of a particular hunt group is not supported.

For automatic voice recording, a time profile can be used to set when voice recording is used.

User:

- Users being used for Dial In data services such as RAS can have an associated time profile that defines when they can be used for that service.
- Users can be associated with a working hours and an out of hours user rights. A time profile can then be used to determine which user rights is used at any moment.
- For automatic voice recording, a time profile can be used to set when that voice recording is used.
- For mobile twinning, a time profile can be used to define when twinning should be used.

Incoming Call Route:

Incoming call routes can also use time profiles to specify when calls should be recorded. Multiple time profiles can be associate with an incoming call route, each profile specifying a destination and fall back destination.

ARS:

ARS forms use time profile to determine when the ARS form should be used or calls rerouted to an out of hours route.

Account Code:

Account Codes can use automatic voice recording triggered by calls with particular account codes. A time profile can be used to set when this function is used.

Auto Attendant :

Embedded voicemail auto attendants can use time profiles to control the different greetings played to callers.

Service:

- A Service can use time profiles in the following ways:
- A time profile can be used to set when a data service is available. Outside its time profile, the service is either not available or uses an alternate fallback service if set.
- For services using auto connect, a time profile can be used to set when that function is used. See Service | Autoconnect.

Related links

Overriding a Time Profile on page 788

Overriding a Time Profile

You can use the **System Settings** > **Time Profiles** > **Add/Edit Time Profile** > **Manual Override** setting to manually override a time profile. The override settings allow you to mix timed and manual settings.

The override options are as follows:

- **Set Time Profile Active Until Next Timed Inactive**

  Use for time profiles with multiple intervals. Make the time profile active until the next inactive interval.

- **Set Time Profile Inactive Until Next Timed Active**

  Use for time profiles with multiple intervals. Make the time profile inactive until the next active interval.

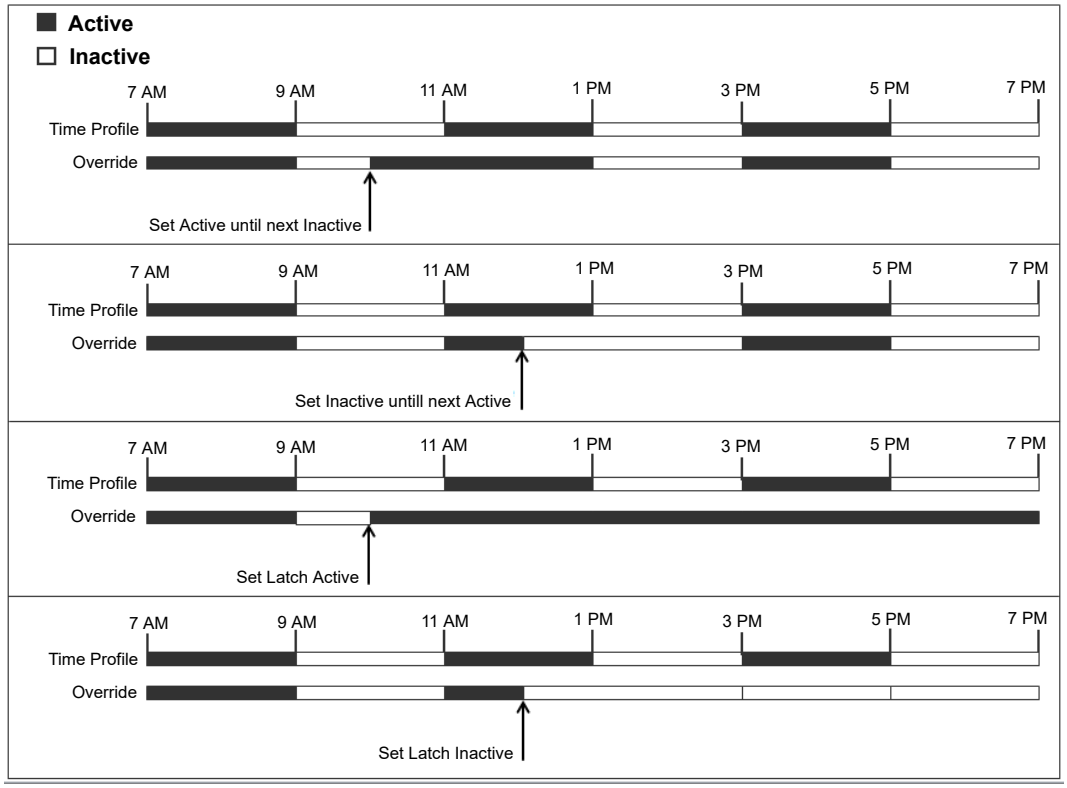
- **Set Time Profile Latch Active**

  Set the time profile to active. Timed inactive periods are overridden and remain active.

- **Set Time Profile Latch Inactive**

  Set the time profile to inactive. Timed active periods are overridden and remain active.

The illustration below provides an example of each override setting.



A time profile can be overridden using the following methods.

- Using the **Override** settings on the Time Profile configuration page.
- Configure short codes for the time profile. See the description for the “Set Time Profile” short code.
- Configure the Time Profile button action for the time profile. See the description for the “Time Profile” button action.

Related links

Configuring Time Profiles on page 787

Chapter 78: Applying Licenses

For a description of IP Office licenses and for information on licensing requirements, refer to the Avaya IP Office™ Platform Solution Description document.

Related links

PLDS licensing on page 790
Web License Manager (WebLM) on page 791
Server Edition Centralized Licensing on page 792
Distributing Server Edition Licenses on page 792
Procedures for Applying Licensing on page 797
Converting from Nodal to Centralized Licensing on page 803
Migrating Licenses to PLDS on page 804

PLDS licensing

IP Office uses the Avaya Product Licensing and Delivery System (PLDS) to manage licenses. PLDS is an online, web-based tool for managing license entitlements and electronic delivery of software and related license files. PLDS provides customers, Avaya Partners, distributors, and Avaya Associates with easy-to-use tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads. You can access PLDS from http://plds.avaya.com/.

PLDS license files

Licenses are delivered from PLDS with license files. A PLDS license file is generated for installing on a specific machine. There are two deployment options:

- PLDS Nodal license files are generated for and installed on particular IP Office nodes.
- PLDS WebLM license files are generated for and installed on a WebLM server that can license multiple IP Office nodes.

WebLM centralized licensing is supported in IP Office Server Edition and in IP Office Branch deployments, but not in non-Branch deployments of IP Office Standard mode.

PLDS host ID

PLDS Nodal license files are machine specific and you must specify the host ID in the **PLDS host ID** field on **System Settings** > **Licenses** > **Systems** > **Manage Licenses**.

System Type	Description
IP500 V2 Systems	You can find the PLDS host ID in the **Licensing** tab of IP Office Manager and Web Manager. The PLDS host ID is made of the two digits “11”, followed by the 10 digit feature key serial number printed on the IP Office SD card. If the SD card is changed, the PLDS host ID will also change.
IP Office Linux Server	The PLDS host ID can be found on the server labeling, the server packaging label, and the system ignition Login screen. The PLDS host ID is derived from the system ID. If the system ID changes, the PLDS host ID will also change.
WebLM	The WebLM host ID is the Mac address of the WebLM server. The WebLM host ID must be used when generating a PLDS license file for the WebLM server in order to implement a centralized licensing scheme for multiple IP Office systems. The WebLM host ID can be found on the server labeling, the server packaging label, the system ignition Login screen, and through the WebLM management interface. In a virtual environment, the WebLM host ID is a virtual Mac address that starts with the letter “V”.

Related links

Applying Licenses on page 790

Web License Manager (WebLM)

The Web License Manager (WebLM) is a web-based application for managing licenses. If you use the WebLM server running on the IP Office server, then you can use IP Office Web Manager to log in to the WebLM server by selecting **Applications** > **Web License Manager**. WebLM credentials are managed separately from IP Office system passwords and are not part of single sign on (SSO).

Note:

- WebLM license management is supported for Server Edition deployments and for Enterprise Branch deployments using the System Manager WebLM server. It is not supported for Standard Mode systems.
- When upgrading from a previous release, all systems must be running the same software level. IP Office Server Edition does not support mixed versioning.

For more information on WebLM, see *Administering standalone Avaya WebLM*.

To establish communication between IP Office and the WebLM server, you must configure the remote server profile on **System Settings** > **Licenses** > **Systems** > **Remote Server** .

Note:

When upgrading from release 9.1, the WebLM server is not started automatically. Perform the following steps to start the WebLM server.

1. Log in to Web Manager.
2. Select **Server Menu** > **Platform View** > **System**.

3. Under **Services**, select the WebLM server and click **Start**.

Related links

Applying Licenses on page 790

Server Edition Centralized Licensing

Before release 10, Server Edition deployments used nodal licensing. This type of licensing can still be used in release 10 and higher. However, it is expected that most deployments will prefer to centralize license management using the Avaya Web License Management (WebLM) server. The WebLM server is automatically installed on the Server Edition Primary server. For newly installed systems, centralized licensing is the default configuration.

All systems in the Server Edition solution must use the same **License Source**.

Nodal licensing

With nodal licensing, license files must be installed on each node in the system. For some licensed features, the required license can be installed on the Server Edition Primary server and used by all nodes in the system. However, for other licensed features, the required license must be installed on the node where the feature is used.

Centralized licensing

As of release 10, you can use the WebLM server running on the Server Edition Primary server to fully centralize license management. With centralized license management, all licenses are contained in a single PLDS file uploaded to WebLM. All nodes in the solution obtain their licenses from WebLM.

The IP Office Secondary server and Expansion systems can be configured to request licenses directly from the WebLM server, or to use a proxy option. When configured to use the proxy option, the license requests are sent through the IP Office Primary server, which proxies the requests to the WebLM server. The Primary server does not allocate licenses, but only acts as a proxy.

Systems using nodal licensing can be converted to use centralized licensing. Since PLDS license files are generated using the host ID of the server where they reside, you must regenerate the license file using the host ID of the WebLM server that will host the license file.

Related links

Applying Licenses on page 790

Distributing Server Edition Licenses

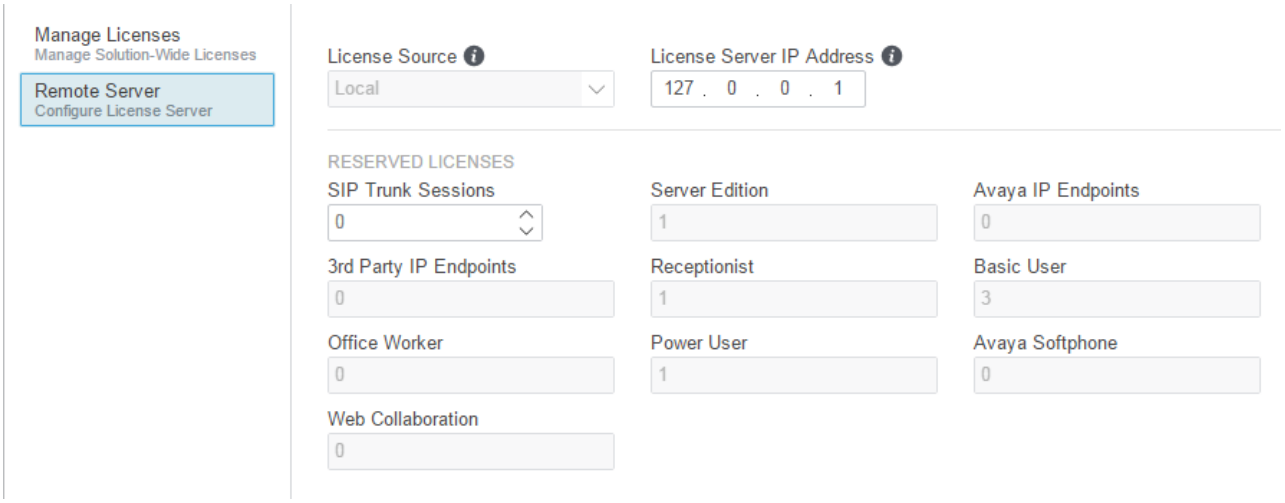
Note:

For a description of IP Office licenses and for information on licensing requirements, see *Avaya IP Office Platform™ Solution Description*.

The **System Settings** > **Licenses** > **Server Menu** > **Remote Server** page displays the **Reserved Licenses** allocated to a Server Edition server.

Note:

The **SIP Trunk Sessions** field has replaced the **System | Telephony | Telephony | Max SIP sessions** setting.



PLDS File Location

How licenses are allocated depends on the location of the PLDS file. For standalone systems, SCN deployments, and Server Edition nodal licensing, each node in the system must have a PLDS file installed.

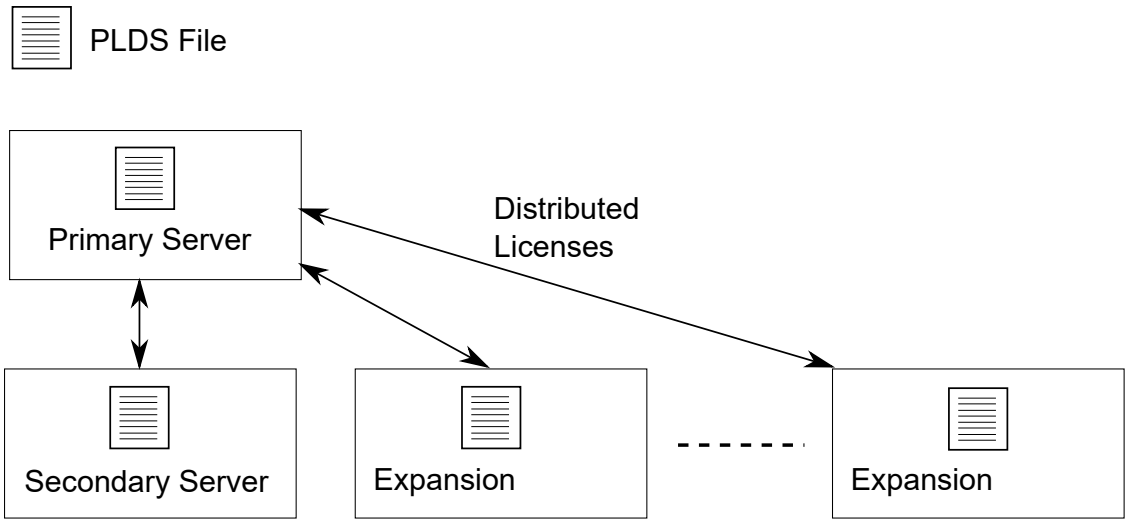


Figure 1: PLDS file location for Server Edition Nodal Licensing

For Server Edition centralized licensing, the PLDS file is located on the WebLM server. The WebLM server can be located on the Primary Server or on a remote server.

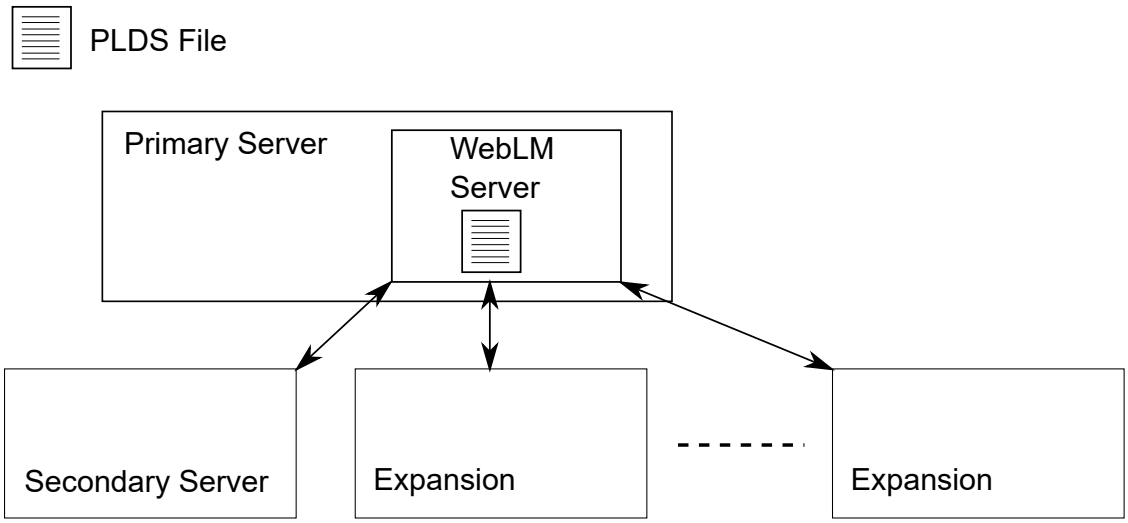


Figure 2: PLDS file location for Server Edition Centralized Licensing

Related links

Applying Licenses on page 790
Nodal license distribution on page 794
Centralized license distribution on page 795

Nodal license distribution

When the **License Source** is **Local**, the **Reserved Licenses** read-only fields indicate licenses that are required for the currently configured features.

Nodal licensing for a Server Edition solution is based on a combination of licensing done through the Server Edition Primary server plus some server-specific licenses. All the user specific and system specific licenses can be managed from the Server Edition Primary server that also acts as a licensing server. Licenses are entered into the configuration of the Server Edition Primary server and are based on the system ID of that server.

Where a license is used to enable features, such as SIP Trunk channels, on other systems, the Server Edition Primary server only allocates those licenses to other systems after it has met its own license needs.

When another system loses connection to the Server Edition Primary server, any license requirements based on those licenses entered in the Server Edition Primary server's configuration are supported for a grace period of 30 days.

Other server specific licenses are entered into the configuration of the server requiring the feature and are based on the System ID of that system.

License	Primary server	Server-specific
Server Edition	✓	✗
Avaya IP endpoints	✓	✗
Third-party IP endpoints	✓	✗
SIP trunk channels	✓	✗
IP500 universal PRI channels	✗	✓
Additional voicemail ports [3]	✓	✗
UMS Web Services [1]	✗	✓
Office Worker	✓	✗
Power User	✓	✗
Office Worker to Power User upgrade	✓	✗
Receptionist	✗	✓
CTI Link Pro	✗	✓
Messaging TTS Pro [3]	✓	✗
Voicemail Pro Recording Administrator [2] [3]	✓	✗
WAV User	✗	✓
IPSec tunneling	✗	✓

1. UMS Web Service licenses are for Hunt Groups only.
2. The Voicemail Pro Recording Administrator license refers to Contact Store. Only one license is required for a Server Edition network.
3. For deployments with dual Voicemail Pro servers, Messaging TTS Pro, Voicemail Pro Recording Administrator, and Additional voicemail ports licenses must be on the Secondary Server.

Related links

Distributing Server Edition Licenses on page 792

Centralized license distribution

When the license source is WebLM, the **Reserved Licenses** read-only fields indicate licenses that are required for the currently configured features. Editable fields can be used to:

- Request additional licenses from the WebLM server.
- Remove licenses from the IP Office node to apply them elsewhere.

Important:

When reallocating licenses, always reduce the number on the IP Office node where they are currently applied before applying them on another node. If you exceed the number of licenses available, you will receive an error message.

Distribution after conversion from Nodal to Centralized licensing

- If the IP Office node needs any of the following licenses, then you must manually configure the respective **Reserved Licenses** editable fields. This will allow the IP Office node to request the licenses from the WebLM server.
  - **VMPro Recordings Administrators**
  - **VMPro TTS Professional**
  - **CTI Link Pro**

Extension Reserved license setting: When the license source is **Local**, the setting **Extension** > **VoIP** > **Reserve License** is set to **None**. Switching the license source to WebLM changes the setting to **Reserve Avaya IP endpoint license**. If required, you must manually change this setting to **Reserve 3rd party endpoint license** or **Both**.

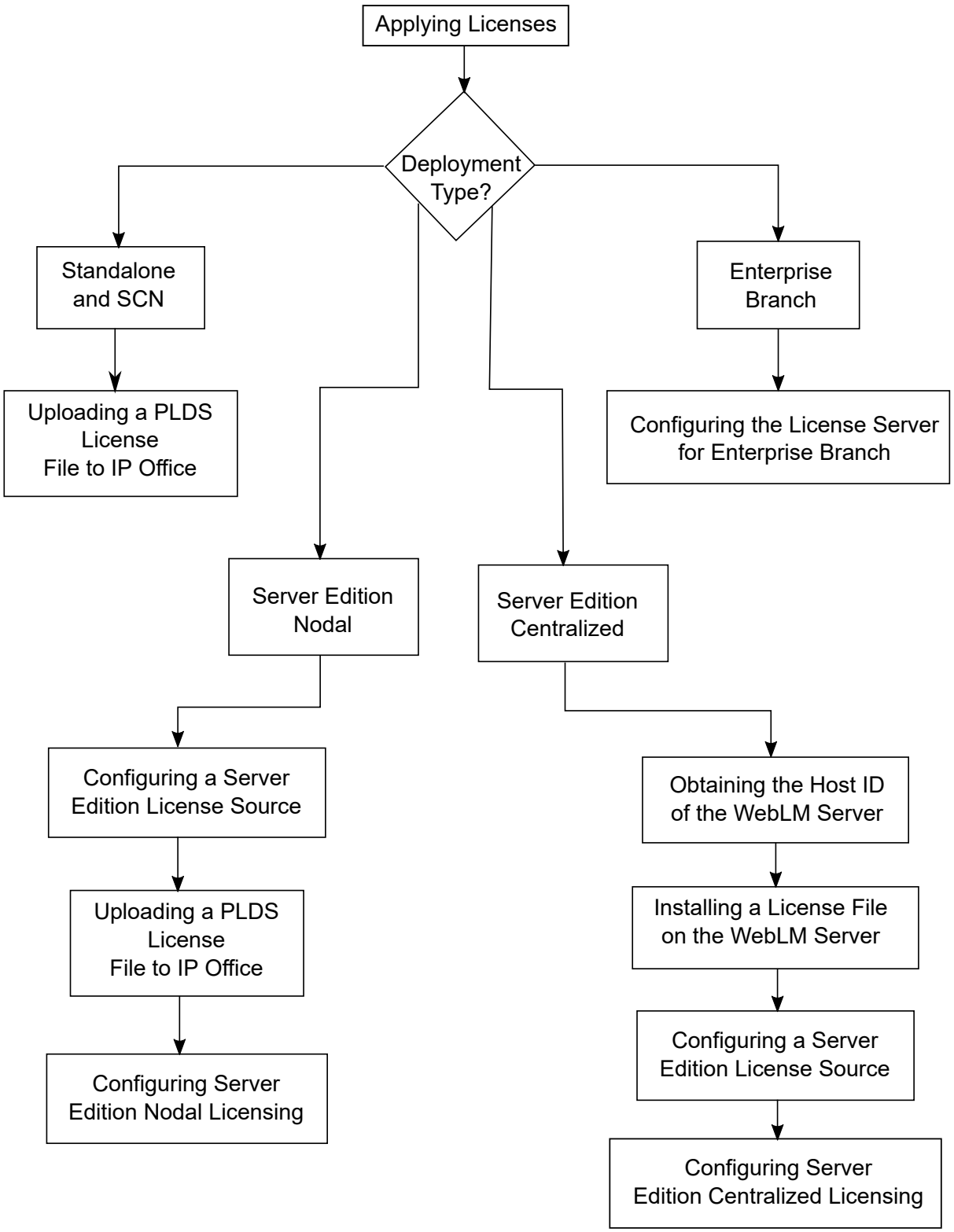
License allocation in WebLM

You can use WebLM to view the licenses used by each node in IP Office Server Edition. In the WebLM navigation pane on the left, click **Licensed Products**. The Acquired licenses table displays information about the licenses acquired for each client ID. In IP Office, the WebLM client ID for each node is displayed on the license Remote Server page.

Related links

Distributing Server Edition Licenses on page 792

Procedures for Applying Licensing



Related links

Applying Licenses on page 790
Obtaining the Host ID of the WebLM Server on page 798
Installing a License File on the WebLM Server on page 798
Configuring the Server Edition License Source on page 799
Uploading a PLDS License File to IP Office on page 799
Configuring Server Edition Nodal Licensing on page 800
Configuring Server Edition Centralized Licensing on page 800
Configuring the License Server in an Enterprise Branch Deployment on page 802

Obtaining the Host ID of the WebLM Server

The WebLM Host ID is required to generate a PLDS license file for centralized licensing. The license file is uploaded to the WebLM server.

Procedure

1. In Web Manager, select **Applications** > **Web License Manager**.
2. Log in to WebLM.
3. In the navigation pane on the left, click **Server Properties**.

   The Server Properties page displays the Host ID. The host ID is the MAC address of the Server Edition Primary server.

   Record the host ID.

Related links

Procedures for Applying Licensing on page 797

Installing a License File on the WebLM Server

Use Web Manager to log in to the WebLM license server and install a license file.

Before you begin

Obtain the license file from the Avaya Product Licensing and Delivery System (PLDS) Web site at https://plds.avaya.com.

You must know the user ID and password for the WebLM server. WebLM credentials are managed separately from IP Office system passwords and are not part of single sign on.

Procedure

1. Log in to Web Manager.
2. Select **Applications** > **Web License Manager**.
3. Log in to the WebLM server.
4. In the left navigation pane, click **Install license**.
5. On the Install license page, click **Browse** to select the license file.

6. Click **Install** to install the license file.

   WebLM displays a message upon successful installation of the license file.

   If the installation is not successful, for troubleshooting information see *Administering Avaya WebLM*, available on the Avaya support site at https://downloads.avaya.com/css/P8/documents/100157154.

Related links

Procedures for Applying Licensing on page 797

Configuring the Server Edition License Source

For Server Edition deployments, the license source can be centralized or nodal.

- With centralized licensing, the PLDS license file resides on the WebLM server. The WebLM server is the license source and all nodes in the solution receive licenses from the WebLM server. The WebLM server can run on a remote machine or on the Primary Server.
- With nodal licensing, a PLDS license file is uploaded to each node.

All systems in the Server Edition solution must use the same license source. The license source is defined by the configuration setting **System Settings** > **Licenses** > **Server Menu** > **Manage Licenses** > **License Source**. Use this procedure to set all nodes to use the same license source.

Procedure

1. Log in to Web Manager.
2. Click **Solution** > **Configure** > **Set All Nodes License Source**
3. In the Select License Source window, select either
   - **Local/Primary Server** for nodal licensing.
   - **WebLM** for centralized licensing.

   All nodes in the solution are set to the same license source.

Related links

Procedures for Applying Licensing on page 797

Uploading a PLDS License File to IP Office

Use this procedure to upload a PLDS license file for nodal license management. Nodal license management is used for standalone IP500 V2 systems and is an option for Server Edition systems.

Before you begin

The PLDS license file must be on the local machine where IP Office Web Manager is running

Procedure

1. In IP Office Web Manager, select **System Settings** > **Licenses** > **Server Menu** > **Manage Licenses**.

2. Click **PLDS Licenses** and select **Send To IP Office** and then click **OK**.
3. In the Select PLDS License File window, click **Browse** and navigate to the license file.
4. Select the file and click **OK**.

Related links

Procedures for Applying Licensing on page 797

Configuring Server Edition Nodal Licensing

With nodal licensing, licenses are managed using license files installed on each node in the system. For information on license distribution, see Distributing Nodal Licenses on page 794.

Procedure

1. In IP Office Web Manager, select **System Settings** > **Licenses**. Click on the **Server Menu** to the right of the Primary Server and then on the License Configuration page, select **Remote Server**.
2. In the **Licence Source** field, select **Primary**.

   Note:

   All systems in the Server Edition solution must use the same **License Source**. In Manager, on the Solution page, you can select **Set All Nodes License Source** to configure the setting for all nodes in the solution.
3. Enter the Server Edition Primary server IP address in the **License Server IP Address** field.
4. Under **Reserved Licenses**, the right hand column indicates which licenses have been reserved for this system. Use the left hand column to request additional licenses for this system.
5. Click **OK**.

   Licenses are displayed in the table.
6. Repeat steps 1 to 5 for the Server Edition Secondary server and all Server Edition Expansion Systems.

Related links

Procedures for Applying Licensing on page 797

Configuring Server Edition Centralized Licensing

With centralized licensing, licenses are managed from a central WebLM server.

Before you begin

You must have a PLDS license file activated with the host ID of the WebLM server

Procedure

1. In IP Office Web Manager, select **System Settings** > **Licenses**. Click on the **Server Menu** to the right of the Primary Server and then on the License Configuration page, select **Remote Server**.
2. Ensure **Licence Source** is set to **WebLM**.

   Note:

   All systems in the Server Edition solution must use the same **License Source**. In Manager, on the Solution page, you can select **Set All Nodes License Source** to configure the setting for all nodes in the solution.
3. The WebLM server can be located on the Server Edition Primary server or on a separate server. Enter the domain name or IP address of the WebLM server in the **Domain Name (URL)** field.

   Note that the domain name URL must use `https://`.
4. If required, change the path to the WebLM server in the **Path** field.
5. Under **Reserved Licenses**, the right hand column indicates which licenses will be automatically requested from the WebLM server. Use the left hand column to request additional license types for this system.
6. Navigate to the **Remote Server** page for the Server Edition Secondary server.
7. Ensure the **Licence Source** is set to **WebLM**.
8. You can choose to enable the **Enable proxy via Primary IP Office line** check box.

Choice Option	Choice Description
Enabled	The WebLM request is sent to the WebLM server via the IP Office line configured to the Server Edition Primary server. The line must be up and in service
Disabled	The WebLM request is sent directly to the WebLM server.

9. If **Enable proxy via Primary IP Office line** is enabled, enter the Server Edition Primary server IP address in the **Primary IP Address** field.
10. If **Enable proxy via Primary IP Office line** is disabled:
    a. Enter the domain name or IP address of the WebLM server in the **Domain Name (URL)** field.
    b. If required, change the path to the WebLM server in the **Path** field.
    c. If required change the default **Port Number**.

       For information on port usage see the IP Office Port Matrix document on the Avaya support site at https://support.avaya.com/helpcenter/getGenericDetails?detailId=C201082074362003.
11. Click **OK**.

    Licenses are displayed in the **License | License** table.

12. Repeat steps 8 to 12 for all Server Edition Expansion Systems.

    Note:

    In Manager, on the Solution page, you can select **Set All Nodes License Source**.

Related links

Procedures for Applying Licensing on page 797

Configuring the License Server in an Enterprise Branch Deployment

Use this procedure to configure WebLM centralized licensing where a shared PLDS license file is installed on the WebLM server. This is the recommended method for installing license files on IP Office systems that are centrally managed by System Manager.

For a complete description of deploying Enterprise Branch, see Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager.

Procedure

1. Log in to Web Manager and select **License | Remote ServerSystem Settings** > **Licenses** > **Systems** > **Remote Server**.
2. Select the **Enable Remote Server** check box.

   The **Reserved Licenses** information is displayed.
3. In the **Domain Name (URL)**, field, enter the domain name or IP address of the WebLM server or the domain name of System Manager if the system is under System Manager control.
4. **(Optional)** If a secondary System Manager is configured, enter the domain name in the **Secondary Domain Name (URL)** field.
5. If required, change the path to the WebLM server in the **Path** field.
6. If required change the default **Port Number**.

   For information on port usage see the IP Office Port Matrix document on the Avaya support site at https://support.avaya.com/helpcenter/getGenericDetails?detailId=C201082074362003.
7. Under **Reserved Licenses**, the right hand column indicates which licenses will be automatically requested from the WebLM server. Use the left hand column to request additional licenses for this system.

Related links

Procedures for Applying Licensing on page 797

Converting from Nodal to Centralized Licensing

If you are upgrading from an earlier release, perform the procedure Migrating Licenses to PLDS on page 804.

Note:

When upgrading from a previous release, all system must be running the same software level. The IP Office Server Edition Solution does not support mixed versioning.

Procedure

1. You must generate a license file using the WebLM host ID. Perform the following steps to find the WebLM host ID.
   a. In Web Manager, select **Applications** > **Web License Manager**.
   b. Log in to WebLM.
   c. In the navigation pane on the left, click **Server Properties**.

      The Server Properties page displays the Host ID. The host ID is the MAC address of the Server Edition Primary server.

      Record the host ID.
2. Generate a PLDS license file using the WebLM host ID.
3. Upload the license file.
   a. In Web Manager, select **ApplicationsWeb License Manager**.
   b. In the navigation pane on the left, click **Install license**.
   c. Click **Browse** to select the license file.
   d. Click **Install** to install the license file.
4. All nodes in the solution must have the same license source. To configure centralized licensing, all nodes must have the **License Source** set to **WebLM**. You can use Manager to set all nodes to the same license source. On the Manager Solution page, on the right hand side, select **Set All Nodes License Source** and then select **WebLM**.
5. If you are performing this procedure after an upgrade, you must ensure that the **Domain Name (URL)** field is populated on the Server Edition Primary server.
   a. In Web Manager select **System Settings** > **Licenses** > **Server Menu** > **Remote Server** for the Server Edition Primary server.
   b. Ensure that the **Domain Name (URL)** field contains the domain name or IP address of the Server Edition Primary server.
6. Reallocate the licenses as required. See Distributing Centralized Licenses on page 795.

   Note that the previously install local licenses are listed as obsolete. You can use this list to determine which licenses to request from the WebLM server. Once licenses have been reallocated, you can delete the obsolete licenses.

Related links

Applying Licenses on page 790

Migrating Licenses to PLDS

IP Office release 10 and higher supports only the Product Licensing and Delivery System (PLDS) to manage license files. If you are upgrading from a previous release, you must migrate all of your pre-R10 licenses (ADI, PLDS, mix of ADI/PLDS, virtual) to R10 PLDS licenses. The license migration tool extracts all the licensing information from an IP Office system and saves it to a file. This file can then be used prepare a software upgrade quote in the Avaya One Source Configurator in order to obtain the required new PLDS R10 licenses.

For Server Edition deployments, the License Migration tool collects licensing information from every node in the solution.

Note:

- You must use the release 10 or higher Manager client to generate the license inventory file.

  You can install Manager before upgrading to release 10. See the procedure “Installing Manager” in Administering Avaya IP Office™ Platform with Manager.
- License migration is supported on all IP Office modes, release 6.0 and higher.
- The license migration tool can only be used with an online configuration. The **Tools** > **License Migration** option is disabled for offline configurations.
- The license migration tool is not available on UCM and Application servers. When you run the license migration tool on a Server Edition server, the tool collects licensing information from every node in the solution.
- The generated file can be read but must not be edited. License migration will fail if the file has been edited.

Before you begin

Ensure all licenses are loaded on the system before performing the license migration. For Server Edition deployments, ensure all nodes are online in order to capture the current view of systems in the solution.

The IP Office configuration must be opened online. The License Migration tool is not available in offline mode.

Procedure

1. Log in to Manager and select **Tools** > **License Migration**.

   The Save As window opens.
2. Select a location to save the file and enter a file name.
3. Click **Save**.

The file is saved with a `.zip` extension.

Next steps

Use the file to prepare a software upgrade quote in the Avaya One Source Configurator in order to obtain the required new PLDS R10 licenses. Once you have the PLDS license files, apply them to the system.

Related links

Applying Licenses on page 790

Chapter 79: Working with Templates

IP Office supports a number of template options. The settings for the following types of configuration items can be saved as template files. New records of those types can then be created from the template file.

- **User** (`.usr`)
- **Extension** (H.323, SIP, IP DECT) (`.ext`)
- **Group** (`.grp`)
- **Service** (`.ser`)
- **Tunnel** (`.tnlt`)
- **Firewall Profile** (`.fpr`)
- **Time Profile** (`.tpr`)
- **IP Route** (`.ipr`)
- **ARS** (`.ars`)
- **Line** (H.323, SIP, IP DECT) (`.lne`)
  - The SIP trunk services from selected SIP providers are tested as part of the Avaya DevConnect program. The results of such testing are published as Avaya Application Notes available from the Avaya DevConnect web site (https://devconnect.avaya.com).

Related links

Saving Template files on page 806
Creating a Template in Manager on page 807
Creating an Analog Trunk Template in Manager on page 807
Creating a New Analog Trunk from a Template in Manager on page 808

Saving Template files

The location used to store template files depends on the type of IP Office system.

- IP500 V2 - IP Office Manager export templates to a `\manager_files\template` sub-folder of the directory where it is installed.
- **Linux-based systems:** - Templates are stored on the Primary Server. When the system configuration is opened by IP Office Manager, those templates are downloaded from server

to the \manager_files\template folder. When the configuration is saved, the templates are uploaded back to server.

Caution:

- If you are using IP Office Manager to manage both IP500 V2 and Linux-based IP Office systems, you need to ensure that you store the IP500 V2 templates in a directory other than the default directory before opening any Linux-based system configuration. When doing so, existing template in the \manager_files\template folder may be overwritten.

Related links

Working with Templates on page 806

Creating a Template in Manager

You can create a template from an existing record.

The options **New From Template** and **Export as Template** are available by:

- right clicking on the record type in the Navigation pane
- right clicking on a record in the Group pane
- using the Details Toolbar in the Details pane

This procedure uses the Group Pane.

Procedure

1. In the Navigation pane, select a record type.
2. In the Group pane, right click on the record on which you want to base your template and select **Export as Template**.
3. The **Save As** window opens at the default template folder. Enter a name for the template.

   A default extension is applied. For example, user templates are saved with the file extension .usr and extension templates are saved with file extension .ext.
4. Click **Save**.

   You can now create new records using the template.

Related links

Working with Templates on page 806

Creating an Analog Trunk Template in Manager

You can create an analog trunk template from an existing trunk..

Procedure

1. In the Navigation pane, select **Line**.
2. In the Group pane, right click on the record on which you want to base your template and select **Generate Analog Trunk Template**.
3. In the Analog Trunk Template window, you can adjust the settings if required. Click **Export**.
4. In the Template Type Selection window, select the **Service Provider** and then click **Create Template**.
5. In the Browse for Folder window, select `Program Files\Avaya\IP Office\Manager\manager_files\template`.
6. Click **OK**.

Related links

Working with Templates on page 806

Creating a New Analog Trunk from a Template in Manager

You can create a new analog trunk from a template.

Procedure

1. In the Navigation pane, right click **Line** and select **New from Template** > **Open**.
2. In the Open window, select a template and click **Open**.
3. In the Template Type Selection window, select the **Service Provider** and then click **Create**.

Related links

Working with Templates on page 806

Chapter 80: Configuring ARS

When a dialed number matches a short code that specifies that the number should be dialled, there are two methods by which the routing of the outgoing call can be controlled.

Routing Calls Directly to a Line

Every line and channel has an Outgoing Group ID setting. Several lines and channels can have belong to the same Outgoing Group ID. Within short codes that should be routed via a line within that group, the required Outgoing Group ID is specified in the short code's Line Group ID setting.

Routing Calls via ARS

The short code for a number can specify an ARS form as the destination. The final routing of the call is then controlled by the setting available within that ARS form.

ARS Features

Feature	Description
Secondary Dial Tone	The first ARS form to which a call is routed can specify whether the caller should receive secondary dial tone.
Out of Service Routing	ARS forms can be taken out of service, rerouting any calls to an alternate ARS form while out of service. This can be done through the configuration or using short codes.
Out of Hours Routing	ARS forms can reroute calls to an alternate ARS form outside the hours defined by an associated time profile.
Priority Routing	Alternate routes can be made available to users with sufficient priority if the initial routes specified in an ARS form are not available. For users with insufficient priority, a delay is applied before the alternate routes become available.
Line Types	ARS can be used with all line types. A SIP line is treated as busy and can follow alternate routes based on the SIP line setting **Call Initiation Timeout**. Previously a SIP line was only seen as busy if all the configured channels were in use. IP lines use the NoUser Source Number setting **H.323SetupTimerNoLCR** to determine how long to wait for successful connection before treating the line as busy and following ARS alternate routing. This is set through the IP line option **Call Initiation Timeout**.
Multi-Site Network Calls	Calls to multi-site extension numbers are always routed using the appropriate network trunk. ARS can be configured for multi-site network numbers but will only be used if the network call fails due to congestion or network failure.
Main Route	The ARS form 50, named "Main" cannot be deleted. For defaulted systems it is used as a default route for outgoing calls.

Routing Calls to ARS

1. Create the ARS form.
2. Create the required system, user or user rights short code to match the user dialing.
   a. In the **Telephone Number** field, define the digits that will be used to match a short code in the ARS form.
   b. Use the **Line Group ID** field drop-down to select the ARS form required for routing the call.

Related links

Example ARS Operation on page 810
ARS Operation on page 811
ARS Short Codes on page 813
Simple Alternate Line Example on page 814
Simple Call Barring on page 815
User Priority Escalation on page 815
Time Based Routing on page 817
Account Code Restriction on page 818
Tiered ARS Forms on page 818
Planning ARS on page 820

Example ARS Operation

The simplest example for ARS operation are the settings applied to a defaulted system. These vary between U-Law systems and A-Law systems. For Server Edition systems refer to Server Edition Outgoing Call Routing.

A-Law Systems

This set of defaults is applied to A-Law systems, typically supplied to locales other than North America. The defaults allow any dialing that does not match an internal number to be routed off-switch as follows:

1. **System Short Code - ?/Dial/./50:Main**

   The default system short code ? will match any dialing for which no other user, user rights or system short code match is found. This short code is set to route all the digits dialed to ARS form 50.

2. **ARS Form - 50:Main**

   This form contains just a single short code.

3. **?/Dial3K1/./0**

   This short code matches any digits passed to the ARS form. It then dials the digits out on the first available line within line group 0 (the default outgoing line group for all lines).

U-Law Systems

This set of defaults is applied to U-Law systems, typically supplied to locales in North America. The defaults route any dialing prefixed with a 9 to the ARS and secondary dial tone.

1. **System Short Code - 9N/Dial/N/50:Main**

   The default system short code 9N is used to match any dialing that is prefixed with a 9. It passes any digits following the 9 to ARS form 50.

2. **ARS Form - 50:Main**

   This form has secondary dial tone enabled. It contains a number of short codes which all pass any matching calls to the first available line within line group 0 (the default outgoing line group for all lines). Whilst all these short code route calls to the same destination, having them as separate items allows customization if required. The short codes are:

   - **11/Dial Emergency/911/0** - This short code matches an user dialing 911 for emergency services.
   - **911/Dial Emergency/911/0** - This short code matches an user dialing 9911 for emergency services.
   - **0N;/Dial3K1/0N/0** - This short code matches any international calls.
   - **1N;/Dial3K1/1N/0** - This short code matches any national calls.
   - **XN;/Dial3K1/N/0** - This short code matches 7-digit local numbers. Note: From October 2021, telephony providers in the US have ceased routing 7-digit local numbers.
   - **XXXXXXXXXX/Dial3K1/N/0** - This short code matches 10-digit local numbers.

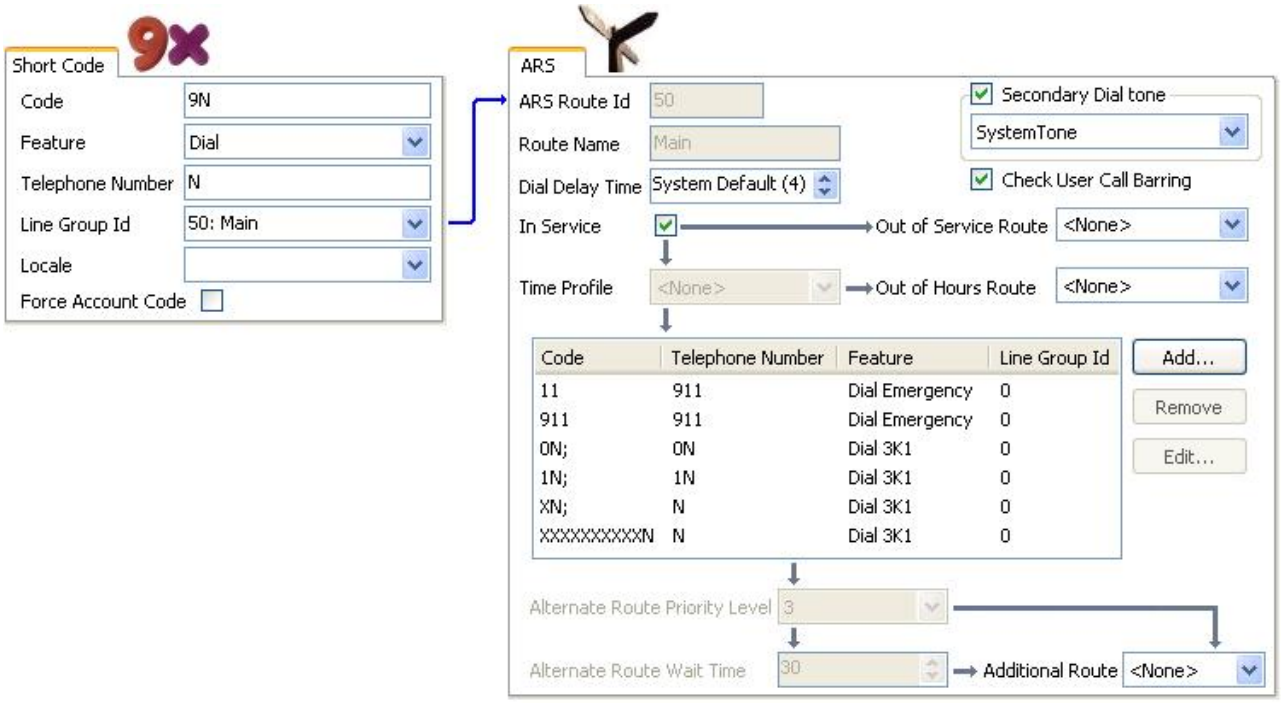
Related links

Configuring ARS on page 809

ARS Operation

The diagram below illustrates the default ARS routing applied to systems defaulted to the **United States** system locale. In summary:

- Any dialing prefixed with 9 will match the default system short code **9N**.
- That short code routes calls to the default ARS form **50:Main**.
- The short codes in that ARS form route all calls to an available line that has its **Outgoing Group ID** set to **0**.



The table describes in more detail the process that the system has applied to the user's dialing, in this example 91555707392200.

The user dials...

9	The **Dial Delay Count** is zero, so the system begins looking for short code matches in the system and user's short codes immediately. Since there is only one match, the **9N** system short code, it is used immediately. The **9N** short code is set to route the call to the ARS form **Main**. It only passes those digits that match the N part of the dialing, ie. the 9 is not passed to the ARS, only any further digits dialed by the user. **Secondary Dial Tone** is selected in the ARS form. Since no digits for ARS short code matching have been received, secondary dial tone is played to the user.
1	Having received some digits, the secondary dial tone stops. The ARS form short codes are assessed for matches. The **11** and **1N;** short codes are possible matches. The **911** and **0N;** short codes are not possible matches. The **XN;** and **XXXXXXXXXXN;** short codes are also not matches because the **1N;** short code is already a more exact match. Since there is more than one possible match, the system waits for further digits to be dialed.

Table continues…

555	The **11** short code is no longer a possible match. The only match is left is the **1N;** short code. The **;** in the short code tells the system to wait for the **Dial Delay Time** to expire after the last digit it received before assuming that dialing has been completed. This is necessary for line providers that expect to receive all the routing digits for a call 'en bloc'. The user can also indicate they have completed dialing by pressing **#**.
707392200	When the dialing is completed, a line that has its **Outgoing Group ID** set to 0 (the default for any line) is seized. If no line is available, the alternate route settings would applied if they had been configured.

Related links

Configuring ARS on page 809

ARS Short Codes

The short codes in the default ARS form have the following roles:

Code	Feature	Telephone Number	Line Group ID	Description
11	**Dial Emergency**	**911**	**0**	These two short codes are used to route emergency calls. A **Dial Emergency** call is never blocked. If the required line is not available, the system will use the first available line. Similarly, calls using **Dial Emergency** ignore any outgoing call bar settings that would be normally applied to the user.
911	**Dial Emergency**	**911**	**0**	
0N;	**Dial 3K1**	**0N**	**0**	Matches international numbers.
1N;	**Dial 3K1**	**1N**	**0**	Matches national numbers.
XN;	**Dial 3K1**	**N**	**0**	Matches 7 digit local numbers.
XXXXXXXXXXN;	**Dial 3K1**	**N**	**0**	Matches 10 digit local numbers.

ARS Short Code Settings

- **Code** The digits used for matching to the user dialing.
- **Feature** ARS short codes can use any of the **Dial** short code features or the **Barred** feature. When a **Barred** short code is matched, the call will not proceed any further.
- **Telephone Number** The number that will be output to the line as the result of the short code being used as the match for the user dialing. Short code characters can be used such as N to match any digits dialed for N or X in the **Code**.
- **Line Group ID** The line group from which a line should be seized once short code matching is completed. Another ARS form can also be specified as the destination.
- **Locale** Not used for outgoing external calls.

- **Forced Account Code** If enabled, the user will be prompted to enter a valid account code before the call can continue. The account code must match one set in the system configuration.

Related links

Configuring ARS on page 809

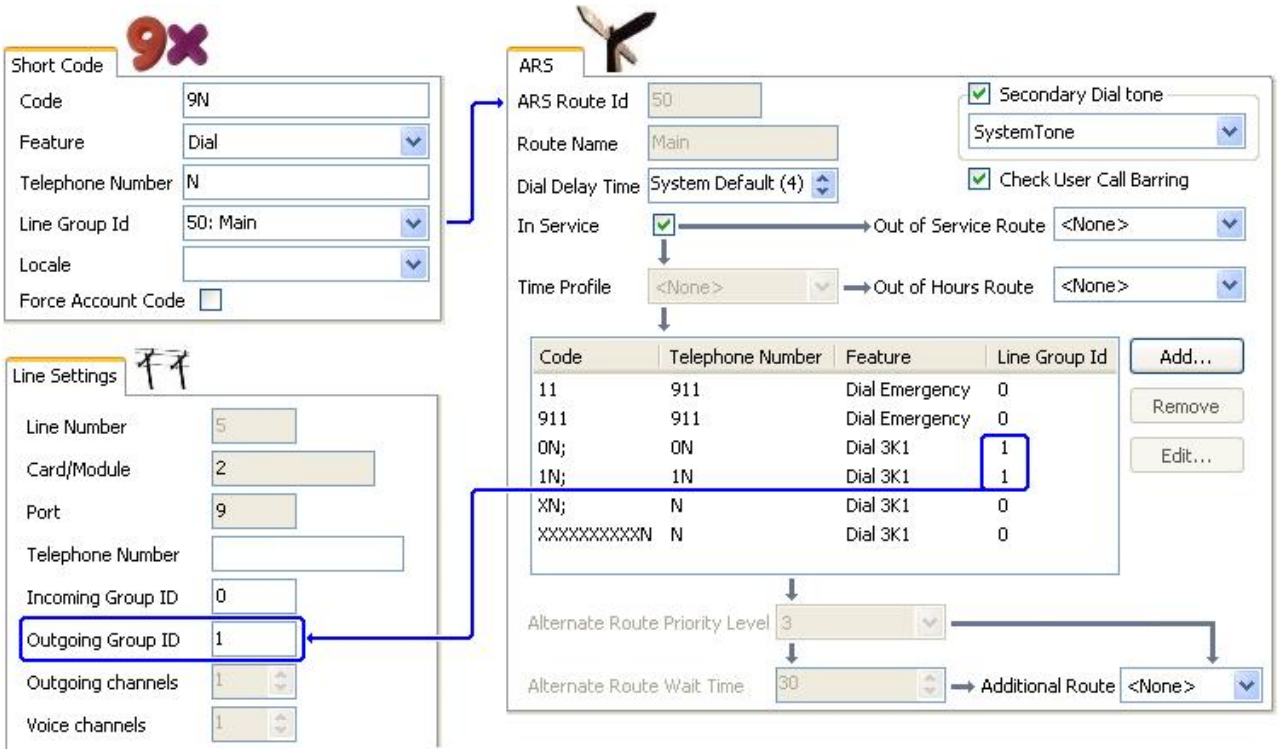
Simple Alternate Line Example

Using the default ARS settings, despite having several short codes in the ARS form, all outgoing calls are actually routed the same way using the same trunks. However, by having separate short codes for different call types present, it is easy to change the routing of each call type if required.

For this example, the customer has separate sets of lines for local calls and for national/ international calls. These have been configured as follows:

- The lines for local and emergency calls have been left with the default **Outgoing Group ID** of **0**.
- The lines for national and international calls have been set with the **Outgoing Group ID** of **1**.

The default ARS can be configured to match this by just changing the **Line Group ID** settings of the default ARS short codes to match.



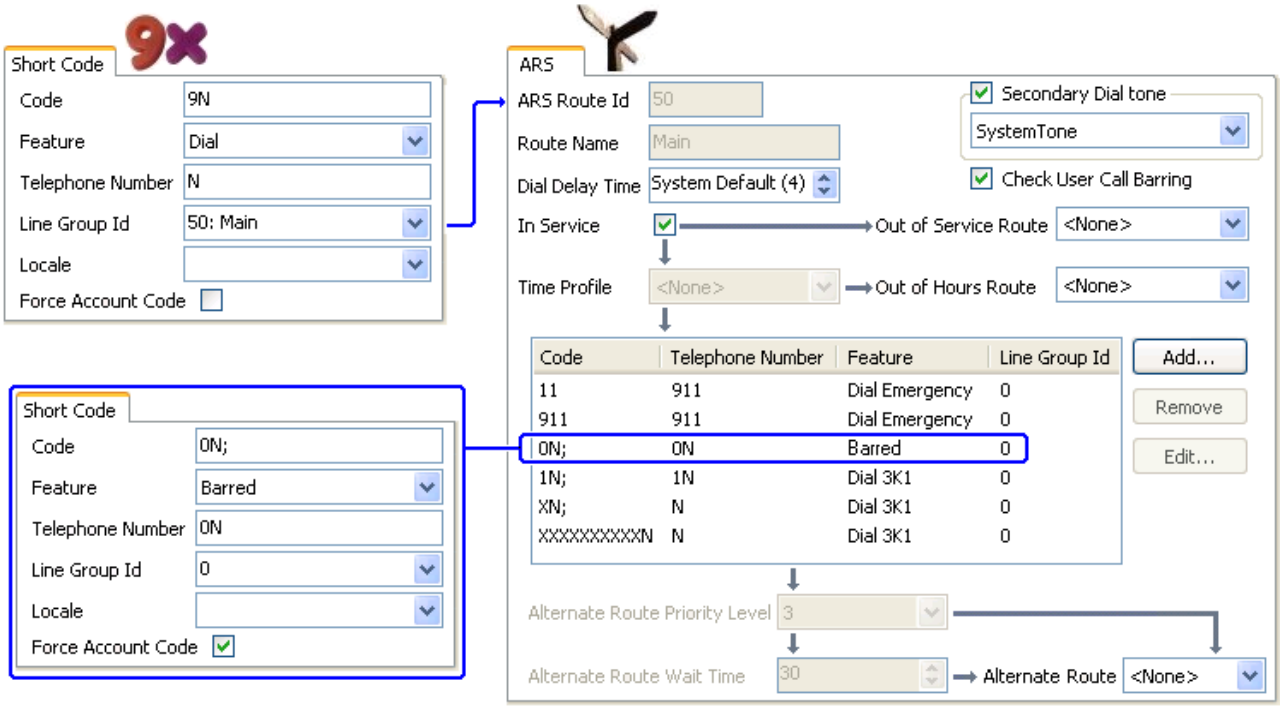
Related links

Configuring ARS on page 809

Simple Call Barring

All ARS short codes use one of the **Dial** short code features. The exception is the **Barred** short code feature. This can be selected for ARS short codes that match dialing that is not allowed.

In the example below, any user dialing an international number will be routed to the **Barred** short code. This prevents the dialing of external numbers prefixed with 0.



To restrict a user from making any outgoing external calls, use the user's Outgoing Call Bar option.

Related links

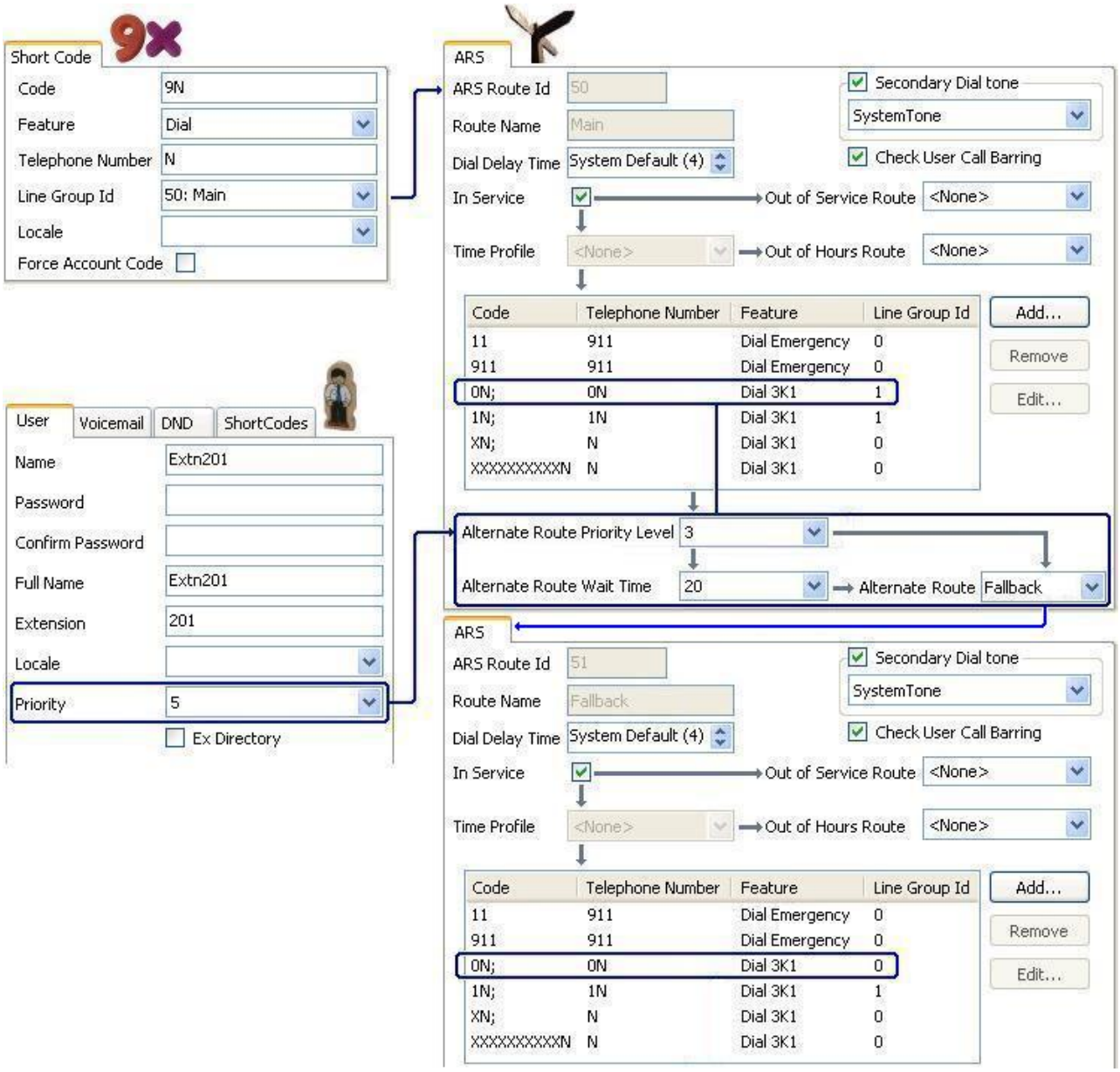
Configuring ARS on page 809

User Priority Escalation

User priority can be used to alter call routing when the required route is not available.

In this example, international calls are initially targeted to seize a line in outgoing line group 1. However an alternate route has been defined which will be used if no line in line group 1

is available. The fallback ARS form allows international calls to seize a line from line group 0. Whether this is done immediately or after a delay is set by whether the users priority is high enough.



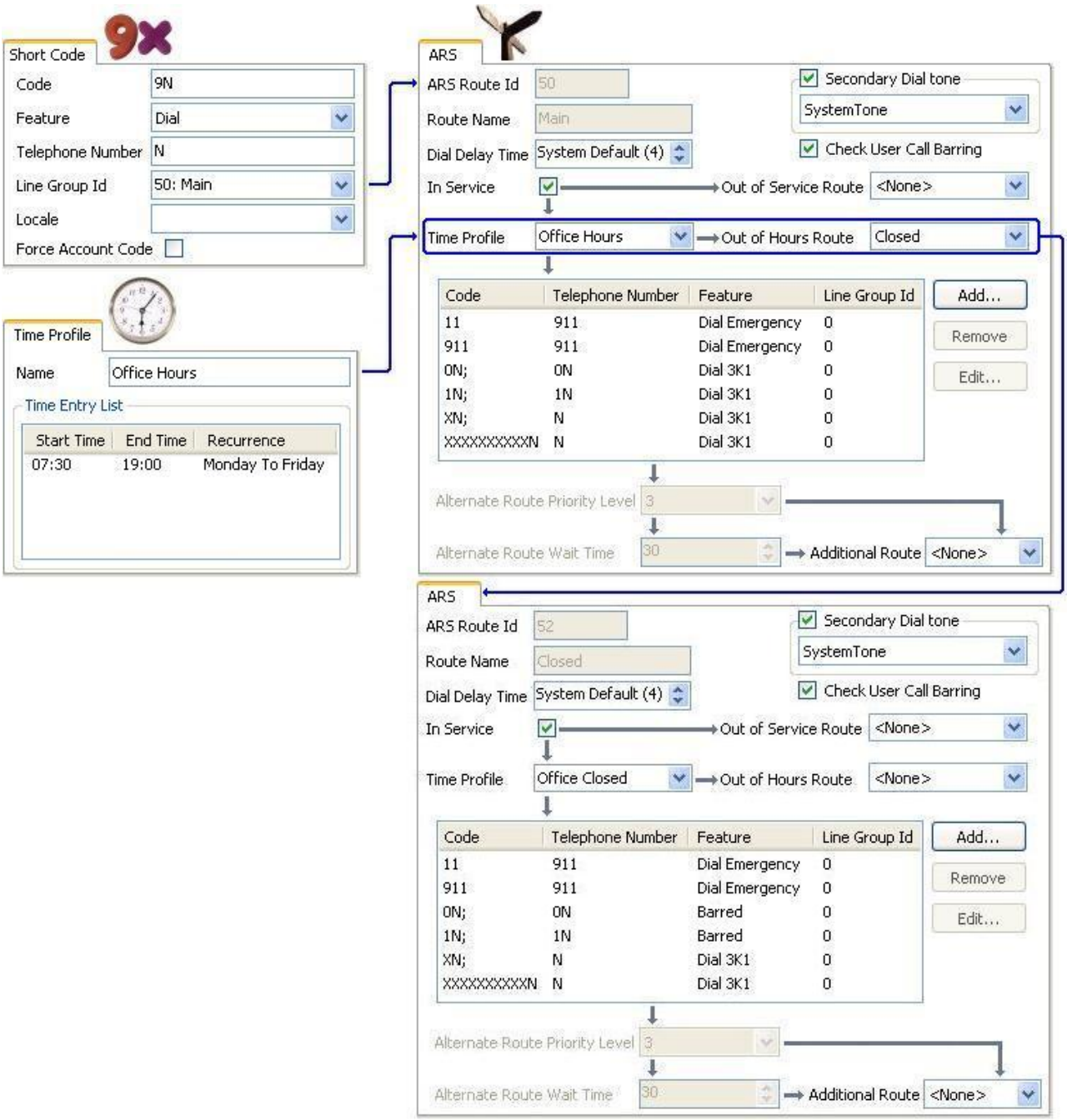
Related links

Configuring ARS on page 809

Time Based Routing

Time profiles can be used to switch call routing from one ARS form to another.

In the example below, a time profile has been define that sets the hours for normal operation. Outside the times set in the time profile, the other ARS form is used. This other ARS form only allows local and emergency calls.



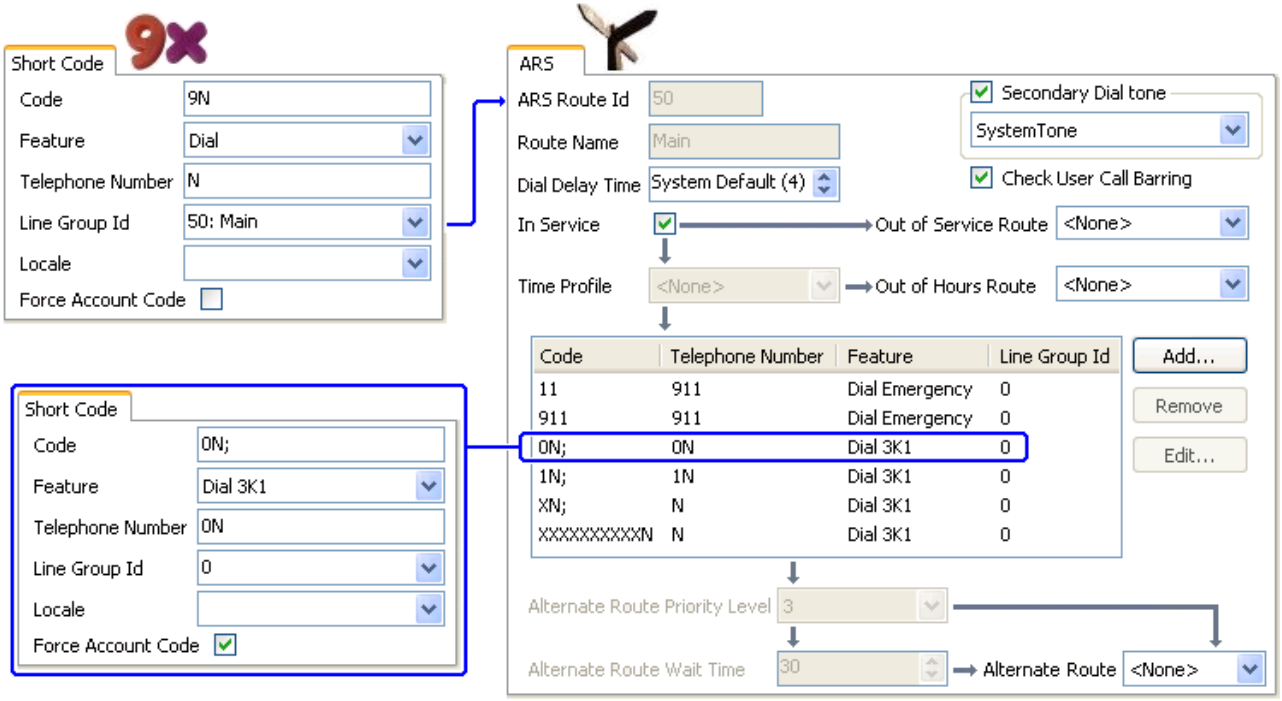
Related links

Configuring ARS on page 809

Account Code Restriction

The short codes within an ARS form can be individually set to require an account code before allowing any call that matches it to proceed.

In the example below, the short code for international calls has been set to require the user to enter an account code. A valid account code must be dialed to continue with the call.



If a user should always enter an account code to make any external call, the user option Force Account Code should be used.

Related links

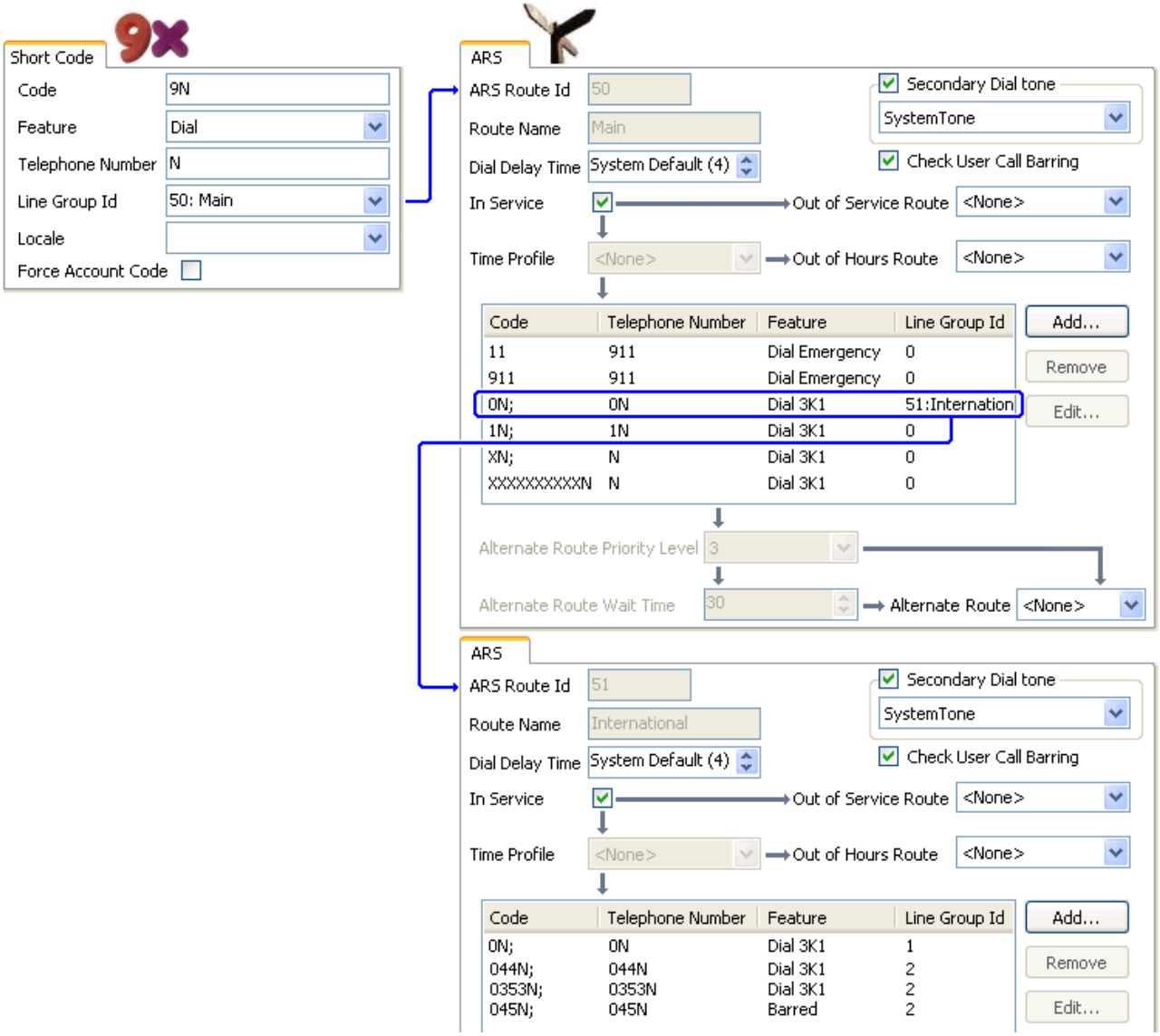
Configuring ARS on page 809

Tiered ARS Forms

It is possible for an ARS short code in one form to have another ARS form as its destination. Dialing that matches the short code is then subject to further matching against the short codes in the other ARS form.

In the example below, the user wants different routing applied to international calls based on the country code dialed. To do that in the default ARS form would introduce a large number of short codes in the one form, making maintenance difficult.

So the short code matching calls with the international dialing prefix 0 has been set to route matching calls to another ARS form. That form contains short codes for the different country dialing codes of interest plus a default for any others.



Related links

Configuring ARS on page 809

Planning ARS

Using the methods shown in the previous examples, it is possible to achieve ARS that meets most requirements. However the key to a good ARS implementation is planning.

A number of questions need to be assessed and answered to match the system's call routing to the customer's dialing.

What What numbers will be dialed and what needs to be output by the system. What are the different call tariffs and the dialing codes.

Where Where should calls be routed.

Who Which users should be allowed to use the call routes determined by the previous questions.

When When should outgoing external calls be allowed. Should barring be applied at any particular times? Does the routing of calls need to be adjusted for reasons such as time dependant call tariffs.

Related links

Configuring ARS on page 809

Chapter 81: Call Barring

Related links

Applying Call Barring on page 821
Overriding call barring on page 822

Applying Call Barring

Call barring can be applied in a number of ways.

Barring a User From Receiving Any External Calls:

For each user, the **Incoming Call Bar** setting (**User | Telephony | Supervisor Settings**) can be selected to stop that user from receiving any external calls.

Barring a User From Making Any External Calls:

For each user, the **Outgoing Call Bar** setting (**User | Telephony | Supervisor Settings**) can be selected to stop that user from making any external calls.

Barring Particular Numbers/Number Types:

System short codes are used to match user dialing and then perform a specified action. Typically the action would be to dial the number to an external line. However, short codes that match the dialing of particular numbers or types of numbers can be added and set to another function such as Busy. Those short codes can be added to a particular user, to a User Rights associated with several users or to the system short codes used by all users.

The system allows short codes to be set at user, user rights, system and least cost route. These have a hierarchy of operation which can be used to achieve various results. For example a system short code for a particular number can be set to busy to bar dialing of that number. For a specific user, a user short code match to the same number but set to Dial will allow that user to override the system short code barring.

Using Account Codes:

The system configuration can include a list of account codes. These can be used to restrict external dialing only to users who have entered a valid account code.

- **Forcing Account Code Entry for a User**: A user can be required to enter an account code before the system will return dialing tone. The account code that they enter must match a valid account code stored in the system configuration. The setting for this is **Force Account Code** (**User | Telephony | Supervisor Settings**)

- **Forcing Account Code Entry for Particular Numbers**: Each system short code has a Force Account Code option. Again the account code entered must match a valid account code stored in the system configuration. for the call to continue.

Barring External Transfers and Forwards:

A user cannot forward or transfer calls to a number which they cannot normally dial. In addition there are controls which restrict the forwarding or transferring of external calls back off-switch. See Off-Switch Transfer Restrictions on page 902.

Related links

Call Barring on page 821

Overriding call barring

When a system or user short code is configured to bar outgoing calls, you can override call barring. Typically, this configuration is used for a phone in a shared or public area. By default, the phone has outgoing calls barred. The administrator can override call barring for specific dialed numbers by entering numbers with a record in the external directory. When the dialed number exists in the external directory and the **Directory Overrides Call Barring** setting is enabled, call barring is overridden.

The System Directory entries must use the format (shortcode)number. For example, if the number to dial is 61234, where 6 is the shortcode used to dial externally and 1234 is the number, the System Directory entry must be (6)1234. If the dial shortcode contains a name string rather than digits, then **Directory Overrides Call Barring** will not work.

The **Directory Overrides Barring** setting is located on the **System | Telephony | Telephony** tab.

For information on the directory, see the description for the **System | Directory Services** tab.

Server Edition configuration

For Server Edition deployments, the **Directory Overrides Barring** must be enabled on each node. It is not a system wide setting.

For example, if the Primary Server uses an IP500 V2 expansion system as an ISDN gateway, **Directory Overrides Barring** must be enabled on the Primary Sever for Primary Server users dialing on external ISDN lines. For the IP500 V2 expansion users, **Directory Overrides Barring** must be enabled on the IP500 V2 expansion system.

It is recommend that the short code configured to dial externally on ISDN lines be the same on all nodes. For example, if Primary Server users and IP500 V2 expansion users want to reach PSTN number 123456789 on ISDN lines, configure the dial codes as follows.

- Primary Server: 6N/Dial/6N/XX (XX is the line group ID for the SCN line)
- IP500 V2 expansion: 6N/Dial/N/YY (YY is the line group ID for ISDN line)
- Directory Entry number defined on Primary Server: (6)123456789

Related links

Call Barring on page 821

Chapter 81: Configuring authorization codes

Note:

For Release 9.1 and higher, you can no longer associate **Authorization Code** entries with **User Rights**. **Authorization Code** configured in that way are removed during the upgrade.

Authorization codes are enabled by default.

A user dials a number that matches a short code set to **Force Authorization Code**. The user is prompted to enter an authorization code.

They dial their authorization code. If a matching entry is found in **Authorization Codes** records the system checks the corresponding user. Note that the user checked does not necessarily need to be connected with the user dialing or the user whose extension is being used to make the call.

The dial string is checked against the short codes with the matching user. If it matches a dial short code or no short code the call is allowed, otherwise it is blocked. Note that the short code is not processed, it is just checked for a match. If multi-tier authorization codes are required there must be blocking (busy) short codes (or a wild card '?')

Example:

A restaurant has a number of phones in publicly accessible areas and want to control what calls can be made by staff. Staff must not be able to dial long distance numbers. staff should be able to dial local and cell phone numbers.

ARS Table
In the Main (50) ARS table, add the following short codes: • 044XXXXXXXXX/Dial/044N/ • 01XXXXXXXXX/Dial/01N/Force Auth Code checked
Authorization Codes
Configure an authorization code for each staff member that is allowed to make long distance calls. For example, for staff members Alice and Bob: AuthCode: **2008 - Alice** AuthCode: **1983 - Bob**

It is recommended to use short codes that use X characters to match the full number of characters to be dialed. That ensures that authorization code entry is not triggered until the full number has been dialed rather than mid-dialing. For example 09 numbers are premium rate in the UK, so you

would create a **09XXXXXXXXX/Dial/N** short code set to Forced Authorization. In the associated user or user right short code it is recommended to use 09N type short codes.

System short codes that route to ARS will not have their **Force Authorization Code** setting used. However short codes within an ARS table will have their **Force Authorization** Code setting used.

Forcing Authorization Codes

There are two methods to force a user to enter an authorization code in order to complete dialing an external call.

- **To Force Authorization Codes on All External Calls** A user can be required to enter an authorization code for all external calls. This is done by selecting Force Authorization Code (**User | Telephony | Supervisor Settings**).
- **To Force Authorization Codes on Specific Calls** To require entry of an authorization code on a particular call or call type, the Force Authorization Code option should be selected in the short code settings. This can be used in user or system short codes in order to apply its effect to a user or all users respectively. You need to ensure that the user cannot dial the same number by any other method that would by pass the short code, for example with a different prefix.

Related links

Entering an Authorization Code on page 824

Entering an Authorization Code

Where possible, when an authorization code is required, the user can enter it through their phones display. However, this is not possible for all type of phone, for example it is not possible with analog phones and Avaya XX01 or XX02 phones. The users of these device must either enter the authorization code using a short code set to the Set Authorization Code feature immediately before making the call.

When entry of an authorization code is triggered, the user can enter any authorization code with which they are directly associated.

Note the following.

- If authorization code entry is setup for a particular number, calls forwarded or transferred to that number will also trigger authorization code entry.
- On systems using line appearances to BRI trunk channels to make outgoing calls, authorization code entry may not be triggered. This can be resolved by adding a short code such as [9]XN;/Dial/XN/0 (adjust the prefix and line group as necessary).

Related links

Configuring authorization codes on page 823

Chapter 81: Preventing Toll Bypass

Use this procedure to prevent toll bypass in Enterprise Branch and Small Community Network (SCN) deployments. Toll bypass is prevented by only allowing PSTN calls where the originating location and terminating location are the same.

The location of non-IP lines is the same as the system location. If an IP address is not resolved to any location, then that device is assumed to be in the system location. The location of public IP lines must be configured to same as PSTN termination location.

The **Location** field for extensions with simultaneous login must be automatic and the location tab must be properly configured for the IP range.

Enterprise Branch deployments: All the distributed users must be in the same location as system location. Users registering from a location different from the system location are not supported.

Procedure

1. In the navigation pane on the left, select **System**.
2. In the details pane, click the **Telephony** tab.
3. Under **Telephony**, click the **Telephony** tab.
4. On the **Telephony** tab:
   a. Click the check box to turn **Restrict Network Interconnect** on.
   b. Click the check box to turn **Include location specific information** on.

      Setting the two configuration setting on the **Telephony** tab adds a **Network Type** field to the configuration settings for each trunk.
5. For Enterprise Branch deployments, open the **SM Line | Session Manager** tab. For SCN deployments, open the **IP Office Line | Line** tab.
6. If the line is a PSTN trunk (includes SIP), set **Network Type** to **Public**. If the line is an enterprise trunk, set the **Network Type** to **Private**.
7. If the **Network Type** is **Private**, the **Include location specific information** field is available.

   If the line is connected to an Avaya Aura® system release 7.0 or higher, or an IP Office release 9.1 or higher, set **Include location specific information** to **On**.

Related links

Configuring unknown locations on page 826

Configuring unknown locations

Use this procedure to configure extensions where the location is unknown.

Procedure

1. In the navigation pane, select **Location**.
2. Enter a **Location Name**.
3. Set **Parent Location for CAC** to **Cloud**.
4. In the **Extension** > **Extn** tab, set the **Location** field to the location defined in step 2.

Related links

Preventing Toll Bypass on page 825

Chapter 81: Configuring Call Admission Control

Call Admission Control (CAC) is a method of controlling system resources using defined locations. Calls into and out of each location are allowed or disallowed based upon configured call constraints. In Manager, use the **Location** tab to define a location and configure the maximum calls allowed for the location.

Related links

Manager location tab on page 827
Assigning a network entity to a location on page 828
System actions at maximum call threshold on page 828
Example on page 829

Manager location tab

Configuring location settings

On the Manager **Location** tab, set the following parameters for a location:

- Location Name
- Subnet Address
- Subnet Mask

Configuring Call Admission Control settings

On the Manager Location tab, set the following CAC parameters:

- **Internal Maximum Calls**: Calls that pass from the location to another configured location.
- **External Maximum Calls**: Calls that pass from the location to an unmanaged location.
- **Total Maximum Calls**: The total internal and external calls permitted.

Related links

Configuring Call Admission Control on page 827

Assigning a network entity to a location

The **Location** field is a drop down list of locations defined on the **Location** tab. Network entities are assigned to a location using the **Location** field on the following Manager tabs.

- **System**
- **Extension**
- **SIP Line | VoIP**
- **H323 Line | VoIP**

The following default settings are applied.

- Each IP Office system can be configured with a defined location. For Server Edition deployments, the configuration of locations is done solution wide. All IP Office systems in the solution share the same location configuration.
- Digital phones default to the system location.
- The default setting for IP phones is **Automatic**. Phones registering from a subnet matching that of a location will be treated as within that location. Otherwise, the phone is assigned the same location as the system. Cloud can be used for phones whose Location is variable or unknown.
- IP Lines default to **Cloud**.

Related links

Configuring Call Admission Control on page 827

System actions at maximum call threshold

- A congestion alarm is raised.
- Calls that exceed the CAC maximum values are not allowed.
- Calls from extensions to public trunks through Alternate Route Selection (ARS) are queued and display **Waiting for Line**.
- Calls from extensions to public trunks which do not route through ARS receive a fast-busy tone and display **Congestion**.
- Idle phones display **Emergency/Local calls only**.
- Alternative routing to a local PSTN gateway follows ARS priority escalation rules.
- SIP calls that would exceed call limits and have no other targets are declined with **cause=486** or **cause = 503**.

Allowed calls

When CAC limits have been reached, the following calls are allowed.

- Emergency calls are always allowed.

- Established calls are never torn down to achieve limits.
- A phone on a remote site that parks a call is always allowed to retrieve it.
- Request Coaching Intrusion calls are allowed.

Related links

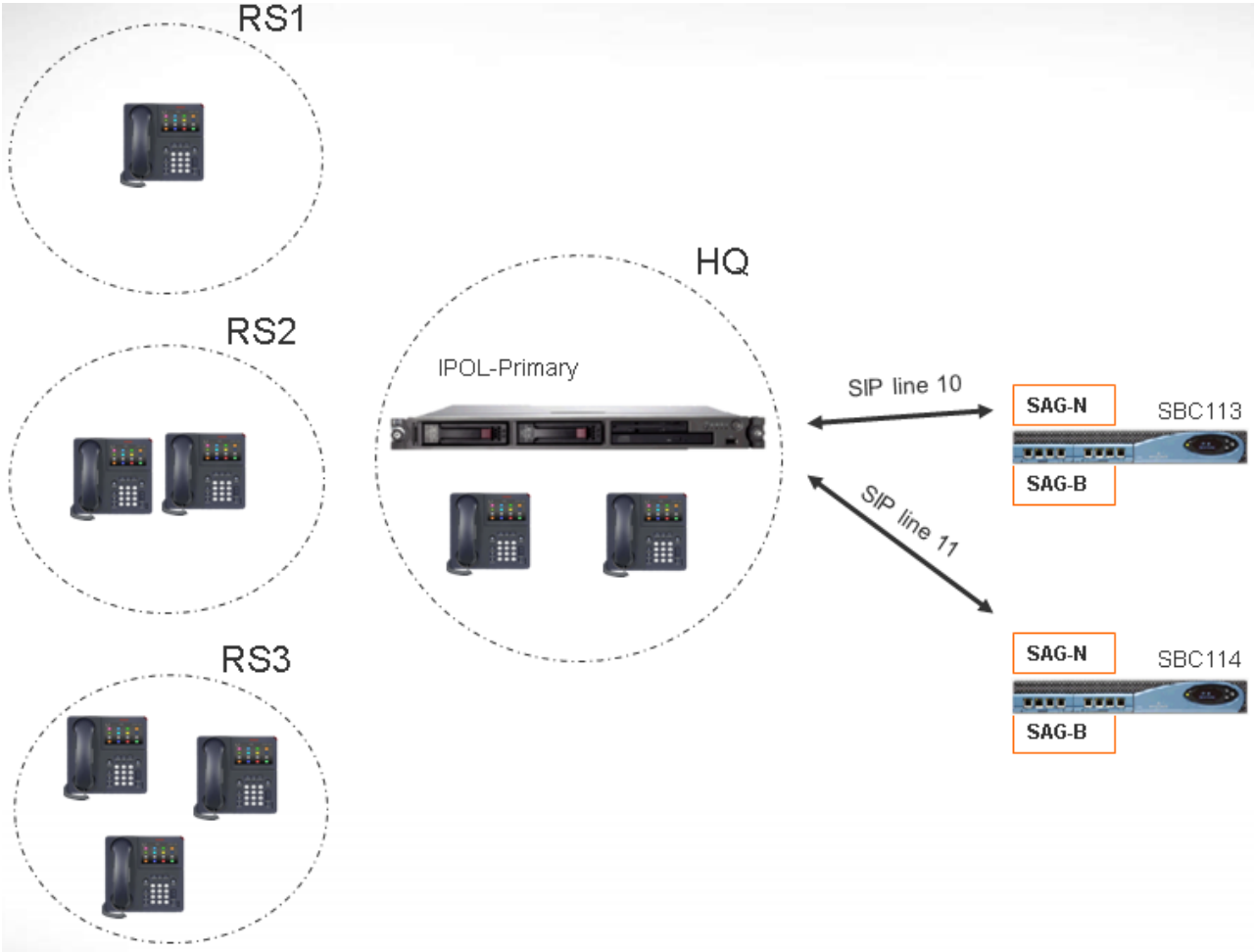
Configuring Call Admission Control on page 827

Example

The example configuration has four locations.

Location	Max Calls
HQ	20
RS1	5
RS2	10
RS3	15
+Cloud	unlimited

SIP Line 10 and SIP Line 11 are configured with 20 channels.



Notes

- Calls between locaton RS1 and SBC113 do not increment the call count for HQ.
- The HQ call count includes calls across the HQ boundary which anchor media inside HQ. SBC113 and SBC 114 are both included.
- The HQ maximum calls value is separate and complementary to the individual trunk call maximum.
- Incoming calls from SIP to RS1 (direct media) only need to verify that the RS1 location maximum call value is not exceeded.
- SIP calls that are not allowed to RS1 may go to HQ voicemail if the HQ call limit is not exceeded.

Related links

Configuring Call Admission Control on page 827

Chapter 82: Configure User Settings

Related links

User Management Overview on page 831
Configuring Gmail Integration on page 833
Call Intrusion on page 834
Call Tagging on page 837
Call Waiting on page 837
Call Barring on page 838
Centralized Call Log on page 839
Centralized Personal Directory on page 839
Account Code Configuration on page 840
Malicious Call Tracing (MCID) on page 842
Twinning on page 842
Private Calls on page 845
System Phone Features on page 846
The 'No User' User on page 847

User Management Overview

Users are the people who use the system. They do not necessary have to be an extension user, for example users are used for RAS dial in data access. In addition, more users can be created than there are extensions, with users logging in to an extension when they want to receive calls.

By default, a user is automatically created to match each extension. They are numbered from 201 upwards and the first 16 are placed in the hunt group Main (200), which is the default destination for incoming calls.

Terminology

Standard User: A standard user.

Centralized User: Centralized users can be provisioned for enterprise branch deployments.

No User: Used to apply settings for extensions which currently have no associated user. The **SourceNumbers** settings of the **NoUser** user is used to configure a number of special options. These are then applied to all users on the system.

Remote Manager: Used as the default settings for dial in user connections.

Hot Desking User: Users with a Login Code can move between extensions by logging in and off.

Deleting a User

When a user is deleted, any calls in progress continue until completed. The ownership of the call is shown as the NoUser user. Merging the deletion of a user causes all references to that deleted user to be removed from the system.

Changing a User's Extension

Changing a user's extension number automatically logs the user in on the matching base extension if available and the user doesn't have Forced Login enabled. If **Forced Login** is enabled, then the user remains on the current extension being used until they log out and log in at the new extension.

Note that changing a user's extension number affects the user's ability to collect Voicemail messages from their own extension. Each user's extension is set up as a "trusted location" under the Source Numbers tab of the User configuration form. This "trusted location" allows the user to dial *17 to collect Voicemail from his own extension. Therefore if the extension number is changed so must the "trusted location".

The following related configuration items are automatically updated when a user extension is changed:

- User, Coverage and Bridged Appearance buttons associated with the user.
- Hunt group membership (disabled membership state is maintained).
- Forwards and Follow Me's set to the user as the destination.
- Incoming call routes to this destination.
- Dial in source numbers for access to the user's own voicemail.
- Direct call pickup buttons are updated.
- The extension number of an associated extension is updated.

Server Edition User Management

In a Server Edition network, individual users are still added to the configuration of a particular server. Typically they are added to the configuration of the server that hosts the user's physical extension or supports their main place of work. That server is treated as the host system for the user. However, once a user is added to the configuration of a particular system, you can use Manager and Web Manager to manage all users in the Server Edition solution.

Centralized User Management

Centralized Users are provisioned for enterprise branch deployments. **Centralized Users** are registered with Session Manager and are able to utilize telephony features provided by Communication Manager. The **Centralized User** profile is applicable to both SIP and analogue extensions. For more information, see Administering Centralized Users for an IP Office™ Platform Enterprise Branch. The following requirements must be met when provisioning a centralized user:

- An SM line must be configured on the system.
- The user must be provisioned with an existing extension.
- The extension **Base Extension** value must match the centralized extension value.
- Centralized users must be configured with a password for SIP registration on Session Manager. The password is set in User | Telephony | Supervisor Settings | Login Code field.

Related links

Configure User Settings on page 831

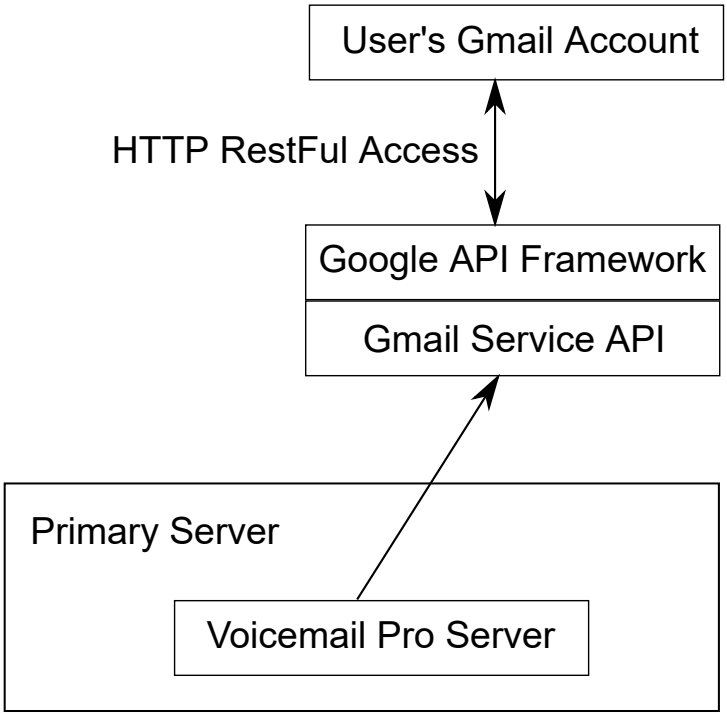
Configuring Gmail Integration

You can integrate the Google Gmail application into Voicemail Pro in order to use a Gmail account for voicemail to email functions. The supported functions are:

- **Forward**: Voicemail messages are sent as email to the Gmail account of a user. Users can use Gmail to retrieve and manage emails.
- **Copy**: Copies of voicemail messages are sent as email to the Gmail account of a user. The message is also stored locally on the Voicemail Pro server.
- **Alert**: An email is sent to the Gmail account of a user indicating the arrival of a new voicemail.

For the forwarding function:

- Up to 250 users are supported.
- The maximum message length is 7 minutes or 14 minutes when using companded.
- Messages can be accessed using Visual Voice but not one-X Communicator.



Related links

Configure User Settings on page 831

Call Intrusion

The IP Office system supports several different methods for call intrusion. The method used affects which parties can hear each other. Intrusion features are supported across a multi-site network.

- Intrusion features are controlled by the **Can Intrude** setting of the user intruding and the **Cannot Be Intruded** setting of user being intruded on. By default, no users can intrude and all users cannot be intruded.
- Intrusion features uses system conference resources during the call. If insufficient conference resource are available, the feature cannot be used.

⚠ Warning:

- Listening to a call without the other parties being aware is subject to local regulations. You must ensure that you have complied with the local regulations. Failure to do so can result in penalties.

In the examples below, A has called or is calling IP Office user B. A can be internal or external. User C invokes one of the call intrusion methods targeting user B.

Description	Privacy Settings Used		
	User	Target	
	Can Intrude	Cannot Be Intruded	Private Call
Call Listen Hear another user's call without being heard. • Monitoring can include a tone heard by all parties. This is controlled by the **Beep on Listen** setting (**System** > **Telephony** > **Tones & Music**). • **Call Listen** can only intrude on calls to users in a user's **Monitor Group** (**User** > **Telephony** > **Supervisor Settings**).	✓	✓	✓
Call Intrude Intrude on the existing connected call of the another user. All call parties are put into a conference and can talk to and hear each other. • A **Call Intrude** attempt to a user who is idle becomes a Priority Call.	✓	✓	✓
Call Steal Take a connected or alerting call from another user. • If the target has multiple alerting calls, the function steals the longest waiting call. • If the target has a connected call and no altering calls, the function steals the connected call. This is subject to the **Can Intrude** setting of the **Call Steal** user and the **Cannot Be Intruded** setting of the target. • If no target is specified, the function attempts to reclaim the user's last ringing or transferred call if it has not been answered or gone to voicemail. • Stealing a video call changes the call to an audio call. • R11.1 FP2 SP4 and higher: The shortcode for this feature can be used with the user's own extension number. That enables twinned and simultaneous device users to move a connected call from another one of their devices. This usage ignores the user's privacy and intrusion settings.	✓	✓	✓

Table continues…

Description	Privacy Settings Used		
	User	Target	
	Can Intrude	Cannot Be Intruded	Private Call
Dial Inclusion Temporarily interrupt another user's call to talk to them. Their current call is held whilst you talk. When you hang-up, the original calls is reconnected. • You and the user can talk but cannot be heard by the other party. • You can intrude on a user in a conference. The conference continues without the user. • During the intrusion, all parties hear a repeated intrusion tone. • Attempting to hold a dial inclusion call ends the intrusion. • You cannot park an inclusion call.	✓	✓	✓
Whisper Page Intrude on another user and be heard by them without interrupting or being able to hear their existing call. • You can use whisper page to talk to a user who has enabled private call.	✓	✓	×
Coaching Intrusion Intrude on another user's call and to talk to them without being heard by the other call parties to which they can still talk. • Example: When C intrudes on B, they can hear A and B, but only B can be hear C.	✓	✓	✓
Request Coaching Intrusion Request a coaching intrusion. • Example: B requests coaching from C. When C responds, they can hear A and B, but only B can hear C.	✓	✓	✓
Appearance Buttons Users can press appearance buttons indicating 'in use elsewhere' to join the call. • The **Can Intrude** setting of the user is not used. • This feature uses the **Cannot Be Intruded** setting of the call's longest present internal user.	×	✓	✓

Related links

Configure User Settings on page 831

Call Tagging

Call tagging associates a text string with a call. That string remains with the call during transfers and forwards. That includes calls across a multi-site network.

On Avaya display phones, the text is shown whilst a call is alerting and is then replace by the calling name and number when the call is connected. On analog phones with a caller ID display, the tag text replace the normal caller information.

Applications such as SoftConsole display any call tag associated with a call. If the call is parked, the tag is shown on the call park slot button used. A call tag can be added when making a call using SoftConsole or one-X Portal. A tag can be added to a call by an Incoming Call Route or by an Voicemail Pro Assisted Transfer action.

Related links

Configure User Settings on page 831

Call Waiting

Call waiting allows a user who is already on a call to be made aware of a second call waiting to be answered.

User Call Waiting

Call waiting is primarily a feature for analog extension users. The user hears a call waiting tone and depending on the phone type, information about the new caller may be displayed. The call waiting tone varies according to locale.

For Avaya feature phones with multiple call appearance buttons, call waiting settings are ignored as additional calls are indicated on a call appearance button if available.

To answer a call waiting, either end the current call or put the current call on hold, and then answer the new call. Hold can then be used to move between the calls.

Call waiting for a user can be enabled through the system configuration (User | Telephony | Call Settings | Call Waiting On) and through programmable phone buttons.

Call waiting can also be controlled using short codes. The following default short codes are available when using Call Waiting.

***15 - Call Waiting On** Enables call waiting for the user.

***16 - Call Waiting Off** Disables call waiting for the user.

***26 - Clear Call and Answer Call Waiting** Clear the current call and pick up the waiting call.

Hunt Group Call Waiting

Call waiting can also be provided for hunt group calls. The hunt group **Ring Mode** must be **Collective Call Waiting**.

On phones with call appearance buttons, the call waiting indication takes the form of an alert on the next available call appearance button. On other phones, call waiting indication is given by a tone in the speech path (the tone is locale specific).

The user's own **Call Waiting** setting is overridden when they are using a phone with call appearances. Otherwise the user's own **Call Waiting** setting is used in conjunction with the hunt group setting.

Related links

Configure User Settings on page 831

Call Barring

Call barring can be applied in a range of ways.

Barring a User From Receiving Any External Calls

For each user, **User** > **Telephony** > **Supervisor Settings** > **Incoming Call Bar** can be selected to stop that user from receiving any external calls.

Barring a User From Making Any External Calls

For each user, **User** > **Telephony** > **Supervisor Settings** > **Outgoing Call Bar** can be selected to stop that user from making any external calls.

Barring Particular Numbers/Number Types

The system allows short codes to be set at user, user rights, system and least cost route. These have a hierarchy of operation which can be used to achieve various results. For example a system short code for a particular number can be set to busy to bar dialing of that number. For a specific user, a user short code match to the same number but set to Dial will allow that user to override the system short code barring.

System short codes are used to match user dialing and then perform a specified action. Typically the action would be to dial the number to an external line. However, short codes that match the dialing of particular numbers or types of numbers can be added and set to another function such as Busy. Those short codes can be added to a particular user, to a User Rights associated with several users or to the system short codes used by all users.

Using Account Codes

The system configuration can include a list of account codes. These can be used to restrict external dialing only to users who have entered a valid account code.

- **Forcing Account Code Entry for a User** - A user can be required to enter an account code before the system will return dialing tone. The account code that they enter must

match a valid account code stored in the system configuration. The setting for this is **User** > **Telephony** > **Supervisor Settings** > **Forced Account Code**.

- **Forcing Account Code Entry for Particular Numbers** - Each system short code has a **Force Account Code** option. Again the account code entered must match a valid account code stored in the system configuration. for the call to continue.

Barring External Transfers and Forwards

A user cannot forward or transfer calls to a number which they cannot normally dial. In addition there are controls which restrict the forwarding or transferring of external calls back off-switch. See Off-Switch Transfer Restrictions on page 902.

Related links

Configure User Settings on page 831

Centralized Call Log

The IP Office stores a centralized call log for each user:

- The user's centralized call log is stored by the IP Office system on which the user is configured. If the user is logged in on another system, new call log records are sent to the user's home IP Office system, but using the time and date on the IP Office system where the user is logged in.
- Each user's centralized call log can contain 30 (IP500 V2) or 60 (Server Edition) call records. Each new call record replaces the oldest previous record when it reaches the limit.
- By default, the centralized call log is displayed on Avaya phones with a fixed **Call Log** or **History** button (1400, 1600, 9500, 9600, J100 Series) and in the one-X Portal, Avaya Workplace Client, and IP Office User Portal applications.
- The centralized call log moves with the user as they log onto different phones and IP Office applications.
- The missed call count is updated per unique caller, not per call.

Adjusting Call Log Operation

The operation of the centralized call log is control by the **System** > **Telephony** > **Call Log** and **User** > **Telephony** > **Call Log** settings.

Related links

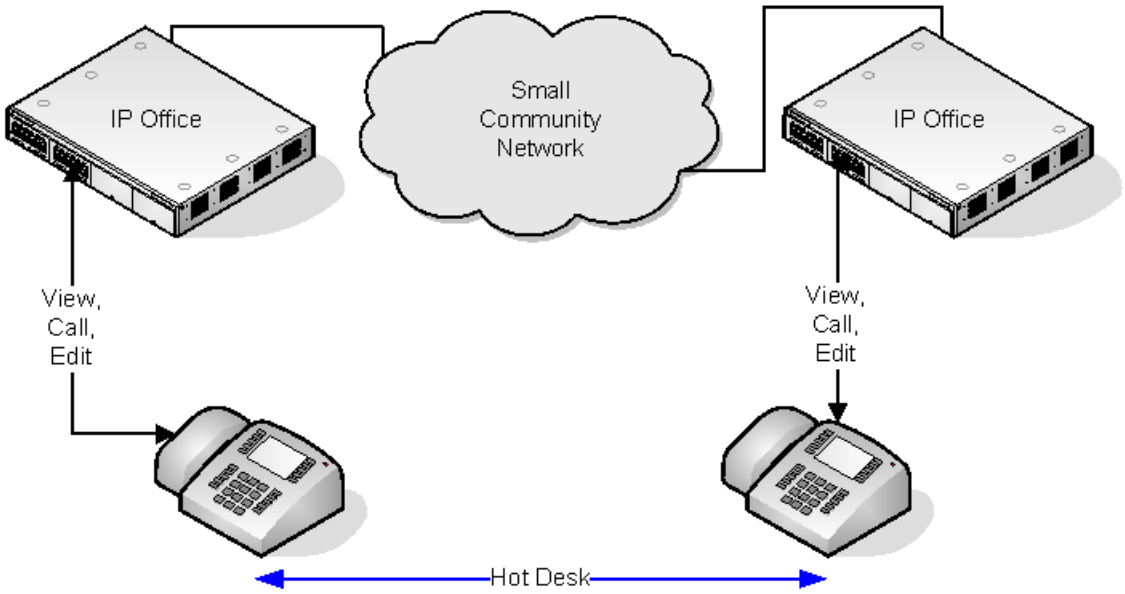
Configure User Settings on page 831

Centralized Personal Directory

Each system user is able to have up to 250 personal directory records stored by the system. A user's personal directory is also usable with 1400, 1600, 9500, 9600 and J100 Series (including

J129) phones with a **CONTACTS** button. The user can view these records and use them to make calls.

Phone users can edit their personal directory records through the phone. The user personal directory records can be edited by administrator through the **User** > **Personal Directory** menu in IP Office Manager and IP Office Web Manager. Users can edit their personal directory through their phone or using the user portal application.



When the user hot desks to another phone that supports the centralized personal directory, their personal directory records become accessible through that phone. That also includes hot desking to another system in the network.

Related links

Configure User Settings on page 831

Account Code Configuration

Forcing Account Code Entry for Specific Numbers

You can make entry of an account code a requirement for any dialing that matches a particular short code. This is done by ticking the **Force Account Code** option found in the short code settings.

Note that the account code request happens when the short code match occurs. Potentially this can be in the middle of dialing the external number, therefore the use of **X** wildcards in the short code to ensure full number dialing is recommended.

Entering Account Codes

The method for entering account codes depends on the type of phone being used. Refer to the relevant telephone User's Guide for details.

Account Code Button:

The Account Code Entry action (**User | Button Programming | Emulation | Account Code Entry**) and Set Account Code action (**User | Button Programming | Advanced | Set | Set Account Code**) can be assigned to a programmable button on some phones. They both operate the same. The button can be preset with a specific account code or left blank to request account code entry when pressed. The button can then be used to specify an account code before a call or during a call.

Setting an Account Code using Short Codes:

The **Set Account Code** feature allows short codes to be created that specify an account code before making a call.

Show Account Code Setting :

This setting on the **System | Telephony | Telephony** tab controls the display and listing of system account codes.

When on and entering account codes through a phone, the account code digits are shown while being dialed.

When off and entering account codes through a phone, the account code digits are replaced by **s** characters on the display.

Server Edition Account Code Management

Accounts codes configured on Server Edition are shared by all systems in the network.

Related links

Configure User Settings on page 831
Setting a User to Forced Account Code on page 841

Setting a User to Forced Account Code

Procedure

1. Receive the system configuration if one is not opened.
2. In the left-hand panel, click **User**. The list of existing user is shown in the right-hand panel.
3. Double-click the required user.
4. Select the **Telephony** tab.
5. Tick the Force Account Code option.
6. Click **OK**.
7. Merge the configuration.

Related links

Account Code Configuration on page 840

Malicious Call Tracing (MCID)

MCID (Malicious Caller ID) is an ISDN feature. It is supported on BRI and PRI trunks to ISDN service provider who provide MCID.

When used, it instructs the ISDN exchange to perform a call trace on the user's current call and to keep a record of the call trace at the exchange for the legal authorities. Trace information is not provided to or displayed by the system or system phones.

The use of MCID is subject to local and national legal requirements that will vary. The feature may also not be enabled until specifically requested from the service provider. You should consult with your ISDN service provider and with appropriate legal authorities before attempting to use MCID.

Note:

Currently, in Server Edition network, MCID is only supported for users using an MCID button and registered on the same IP500 V2 Expansion system as the MCID trunks.

Activating MCID

1. **Liaise with the ISDN Service Provider** MCID should not be used without first confirming its usage with the ISDN service provider.
2. **Enabling MCID Call Tracing on a Line** BRI and PRI lines include a **Support Call Tracing Option** which by default is off.
3. **Enabling MCID Call Tracing for a User** Each user has a **Can Trace Calls** (**User | Telephony | Supervisor Settings**) option. This option is off by default.
4. **Providing an Active MCID Control** The user needs to be provided with a mechanism to trigger the MCID call trace at the exchange. This can be done using either a short code or a programmable button.
   - **MCID Activate Button** The action **MCID Activate** (**Advanced | Miscellaneous | MCID Activate**) can be assigned to a programmable buttons. It allows a malicious call trace to be triggered during a call.
   - **MCID Activate Short Codes** The feature **MCID Activate** can be used to create a short code to triggering a malicious call trace.

Related links

Configure User Settings on page 831

Twinning

Twinning allows a user's calls to be presented to both their current extension and to another number. The system supports two modes of twinning:

	Internal	Mobile
Twinning Destination	Internal extensions only	External numbers only.
Supported in	All locales.	All locales.
License Required	No	No

User BLF indicators and application speed dials set to the primary user will indicate busy when they are connected to a twinned call including twinned calls answered at the mobile twinning destination.

Do Not Disturb and Twinning

Mobile Twinning

Selecting DND disables mobile twinning.

Internal Twinning

- Logging out or setting do not disturb at the primary stops twinned calls alerting at the secondary also.
- Logging out or setting do not disturb at the secondary only affects the secondary.

Do Not Disturb Exceptions List

For both types of twinning, when DND is selected, calls from numbers entered in the user's Do Not Disturb Exception List are presented to both the primary and secondary phones.

Internal Twinning

Internal twinning can be used to link two system extensions to act as a single extension. Typically this would be used to link a users desk phone with some form of wireless extension such as a DECT or WiFi handset.

Internal twinning is an exclusive arrangement, only one phone may be twinned with another. When twinned, one acts as the primary phone and the other as the secondary phone. With internal twinning in operation, calls to the user's primary phone are also presented to their twinned secondary phone. Other users cannot dial the secondary phone directly.

- If the primary or secondary phones have call appearance buttons, they are used for call alerting. If otherwise, call waiting tone is used, regardless of the users call waiting settings. In either case, the **Maximum Number of Calls** setting applies.
- Calls to and from the secondary phone are presented with the name and number settings of the primary.
- The twinning user can transfer calls between the primary and secondary phones.
- Logging out or setting do not disturb at the primary stops twinned calls alerting at the secondary also.
- Logging out or setting do not disturb at the secondary only affects the secondary.
- User buttons set to monitor the status of the primary also reflect the status of the secondary.
- Depending on the secondary phone type, calls alerting at the secondary but then answered at the primary may still be logged in the secondary's call log. This occurs if the call log is a function of the phone rather than the system.

- Call alerting at the secondary phone ignoring any **Ring Delay** settings applied to the appearance button being used at the primary phone. The only exception is buttons set to No Ring, in which case calls are not twinned.

The following applies to internal twinned extensions:

If using a 1400, 1600, 9500 or 9600 Series phone as the secondary extension:

- The secondary extension's directory/contacts functions access the primary user's Centralized Personal Directory records in addition to the Centralized System Directory.
- The secondary extension's call Log/call List functions access the primary user's Centralized Call Log.
- The secondary extension's redial function uses the primary users Centralized Call Log. Note that the list mode or single number mode setting is local to the phone.

It is also shown on 3700 Series phones on an Avaya Wireless DECT system installed using system provisioning .

For all phone types, changing the following settings from either the primary or secondary extension, will apply the setting to the primary user. This applies whether using a short code, programmable button or phone menu. The status of the function will be indicated on both extensions if supported by the extension type.

- Forwarding settings.
- Group membership status and group service status.
- Voicemail on/off.
- Do Not Disturb on/off and DND Exceptions Add/Delete.

Mobile Twinning

This method of twinning can be used with external numbers. Calls routed to the secondary remain under control of the system and can be pulled back to the primary if required. If either leg of an alerting twinned call is answered, the other leg is ended.

Mobile twinning is only applied to normal calls. It is not applied to:

- Intercom, dial direct and page calls.
- Calls alerting on line appearance, bridged appearance and call coverage buttons.
- Returning held, returning parked, returning transferred and automatic callback calls.
- Follow me calls.
- Forwarded calls except if the user's **Forwarded Calls Eligible for Mobile Twinning** setting is enabled.
- Hunt group calls except if the user's **Hunt Group Calls Eligible for Mobile Twinning** setting is enabled.
- Additional calls when the primary extension is active on a call or the twinning destination has a connected twinned call.

A number of controls are available in addition to those on this tab.

Button Programming Actions:

The **Emulation | Twinning** action can be used to control use of mobile twinning. Set on the primary extension, when that extension is idle the button can be used to set the twinning

destination and to switch twinning usage on/off. When a twinned call has been answered at the twinned destination, the button can be used to retrieve the call at the primary extension.

Mobile Twinning Handover:

When on a call on the primary extension, pressing the **Twinning** button will make an unassisted transfer to the twinning destination. This feature can be used even if the user's **Mobile Twinning** setting was not enabled.

- During the transfer process the button will wink.
- Pressing the twinning button again will halt the transfer attempt and reconnect the call at the primary extension.
- The transfer may return if it cannot connect to the twinning destination or is unanswered within the user's configured **Transfer Return Time** (if the user has no **Transfer Return Time** configured, a enforced time of 15 seconds is used).

Short Code Features:

The following short code actions are available for use with mobile twinning.

- **Set Mobile Twinning Number**.
- **Set Mobile Twinning On**.
- **Set Mobile Twinning Off**.
- **Mobile Twinned Call Pickup**.

Related links

Configure User Settings on page 831

Private Calls

This feature allows users to mark a call as being private.

When on, any subsequent calls cannot be intruded on until the user's private call status is switched off. The exception is Whisper Page which can be used to talk to a user on a private call.

Note that use of private calls is separate from the user's intrusion settings. If the user's **Cannot be Intruded** (User | Telephony | Supervisor Settings) setting is enabled, switching private calls off does not affect that status. To allow private calls to be used to fully control the user status, **Cannot be Intruded** (User | Telephony | Supervisor Settings) should be disabled for the user.

Use of private calls can be changed during a call. Enabling privacy during a call will stop any current recording, intrusion or monitoring. Privacy only applies to the speech part of the call. Call details are still recorded in the SMDR output and other system call status displays.

Button Programming The button programming action **Advanced | Call | Private Call** can be used to switch privacy on/off. Unlike the short code features it can be used during a call to apply or remove privacy from current calls rather than just subsequent calls. On suitable phones the button indicates the current status of the setting.

Short Codes A number of short code features are available for privacy.

- **Private Call** Short codes using this feature toggle private status on/off for the user's subsequent calls.
- **Private Call On** Short codes using this feature enable privacy for all the user's subsequent calls until privacy is turn off.
- **Private Call Off** Short codes using this feature switch off the user's privacy if on.

Related links

Configure User Settings on page 831

System Phone Features

The user option **System Phone Rights** (User | User) can be used to designate a user as being a system phone user. System phone users can access a number of additional function not available to other phone users. Note that if the user has a login code set, they are prompted to enter that code in order to access these features.

Setting	Description
None	The user cannot access any system phone options.
Level 1	The user can access all system phone options supported on the type of phone they are using except system management and memory card commands.
Level 2	The user can access all system phone options supported on the type of phone they are using including system management and memory card commands. Because of the nature of the additional commands, you should set a user login code for the user to restrict access.

System Phone Functions

The following functions are supported:

Feature	Description
MENU to set date/ time	Restricted to 4412, 4424, 6408, 6416 and 6424 phones where supported by the system. On these phones, a system phone user can manually set the system date and time by pressing **Menu | Menu | Func | Setup**.
Change Login Code of Other Users	Using a short code with the Change Login Code feature, system phone users can change the login code of other users on the system.
Outgoing Call Bar Off	Using a short code with the Outgoing Call Bar Off feature, system phone users can switch off the outgoing call bar status of other users on the system.

The following commands are only supported using 1400, 1600, 9500, 9600 and J100 Series phones. Due to the nature of the commands a login code should be set for the user to restrict access. The commands are accessed through the **Features | Phone User | System Administration** menu. For full details refer to the appropriate phone user guide.

Feature	Description
Edit System Directory Records	Using a 1400, 1600, 9500 or 9600 Series phone, a system phone user can edit system directory records stored in the configuration of the system on which they are hosted. They cannot edit LDAP and/or HTTP imported records.
Date/Time Programmable Button	Allows system phone users to manually set the system date and time through a programmable button (see System Date and Time on page 783).
The following options are only supported on IP500 V2 systems.	
System Management	Allows the user to invoke a system shutdown command.
Memory Card Management	Allows the user to shutdown, startup memory cards and to perform actions to move files on and between memory cards.
System Alarms	For certain events the system can display an **S** on the user's phone to indicate that there is a system alarm. The user can then view the full alarm text in the phone's Status menu. The possible alarms in order of priority from the highest first are: 1. Memory Card Failure. 2. Expansion Failure. 3. Voicemail Failure. 4. Voicemail Full. 5. Voicemail Almost Full. 6. License Key Failure. 7. System Boot Error. 8. Corrupt Date/Time.

Related links

Configure User Settings on page 831

The 'No User' User

It is possible to have an extension which has no default associated user. This can occur for a number of reasons:

- The extension has no **Base Extension** setting associating it with a user who has the same setting as their **Extension** to indicate that they are the extension's default associated user.
- The extension's default associated user has logged in at another extension. Typically they will be automatically logged back in at their normal extension when they log out the other phone.
- The extension's default associated user cannot be automatically logged in as they are set to **Forced Login**.

Phones with no current user logged in are associated with the setting of the **NoUser** user in the system configuration. This user cannot be deleted and their Name and Extension setting cannot be edited. However their other settings can be edited to configure what functions are available at extensions with no currently associated user.

By default the **NoUser** user has **Outgoing Call Bar** enabled so that the extension cannot be used for external calls. The users first programmable button is set to the **Login** action.

Avaya 1100 Series, 1200 Series, M-Series and T-Series phones, when logged out as **No User**, the phones are restricted to logging in and dial emergency calls only.

NoUser Source Numbers

The **SourceNumbers** tab of the **NoUser** user is used to configure a number of special options. These are then applied to all users on the system. For details refer to the **User | Source Numbers** section.

Related links

Configure User Settings on page 831
Suppressing the NoCallerId alarm on page 848

Suppressing the NoCallerId alarm

Use this procedure to suppress the NoCallerId alarm for all users on the system. Once the task is completed, the NoCallerID alarm is not raised in SysMonitor, SNMP traps, email notifications, SysLog or System Status.

Procedure

1. In Manager, in the navigation pane on the left, select **User**.
2. In the list of users, select **NoUser**.
3. In the details pane, select the **Source Numbers** tab.
4. Click **Add**.
5. In the **Source Number** field, enter **SUPPRESS_ALARM=1**.
6. Click **OK**.

Related links

The 'No User' User on page 847

Chapter 83: Avaya cloud authorization

Using Avaya cloud authorization, you can configure the Avaya Workplace Client connection using your Google, Office 365, Salesforce account, Avaya native spaces email account, or Enterprise Account (SSO).

You can configure the Avaya Workplace Client settings automatically using your email address or the automatic configuration web address.

Enabling Avaya cloud authorization automatically uses your network login and password to access different enterprise systems with a single sign-on. Using Avaya cloud authorization, you do not need to separately login to each system or service in your organization.

For full details, refer to the IP Office SIP Telephone Installation Notes manual.

Note:

Avaya Cloud Account Authorization works only on TLS transport type.

Related links

Apple push notification services on page 849

Apple push notification services

Apple Push Notification service (APNs) is a platform notification service created by Apple Inc. This service allows iOS users of Avaya Workplace Client for iOS to receive notification of new calls, voicemail messages, and other events. They receive these notifications regardless when the Avaya Workplace Client for iOS is idle in the background or is in quit state. However, if Avaya Workplace Client for iOS is on suspension, then Avaya Workplace Client for iOS automatically starts when a new call or instant message notification arrives.

- Apple Push Notification service (APNs) works only on TLS transport type.
- The iOS device sends notifications via an intermediate push notifications server provided by Avaya.
- IP Office supports push notification with Avaya Workplace Client for iOS R3.8 and later.
- On receiving a new call notification, and while Avaya Workplace Client for iOS is on suspension, it takes up to six seconds before the Avaya Workplace Client for iOS becomes active, and you can answer the call. The exact delay depends on the version of iOS and the device used. Therefore, the **No Answer Time** setting time is increased to more than

20 seconds to allow the calls to ring before going to voicemail or following the divert on no answer settings.

- APNs service supports only a single iOS device per user. If the you use Avaya Workplace Client for iOS on two devices, for example, an iPad and an iPhone, only the last client to register will receive notifications.
- While using iOS push notifications, always configure and enable voicemail or an alternate call destination number. When Avaya Workplace Client for iOS is not reachable, the **No Answer Time** setting triggers and the push notifications to a voicemail or a forward on no answer number.
- Setting your iOS device with a GSM telephone number as your mobile twinning, and setting the **Mobile Dial Delay** (sec) to more than 10 seconds, allows the time for the call notification to be answered on a previously suspended client before it alerts the GSM call.

Note:

In IP Office,while using iOS push notifications, if you were using a secured port in the primary server, use the same secured port as a preferred port in secondary server. Any mismatch in the secured port configuration is not valid.

Related links

Avaya cloud authorization on page 849
Enabling Apple push notifications on page 850

Enabling Apple push notifications

About this task

Apple Push notifications for Avaya Workplace Client on iOS devices.

Use this procedure to enable the push notifications to allow the clients to receive call and voicemail message notifications.

Note:

When Avaya Workplace Client in your iOS device, such as iPad or iPhone, is in suspended state or quit state and you log in to another Android or Windows based mobility or desktop device using the same user, IP Office deletes the associated application device token and unregisters your iOS device if registered. When you log in using the same user, you must manually logout and login to the the iOS device to reactivate the token so that you can receive push notification calls.

Before you begin

- All IP Office's in Small Community Networking (SCN) should have egress public access to connect to Apple Push Notification Provider (APNP) to support push notification to Avaya Workplace Client.
- In the case of SCN deployments,IP Office primary server should synchronize the configured System ID, Private/Public key with all IP Office in SCN deployments.
- Configuration synchronize is supported only in IP Office Server Edition with a centralized primary server (only Star topologies) and Managed/Hybrid Customer Premises Equipment

(CPE). It is does not in case of Traditional SCN Deployments with 500v2 (includes serial, mesh and star topologies).

- In the case of Server Edition with centralized primary or Managed/Hybrid CPE, synchronizing Push details should be done through an explicit button that is available in Web-Manager at the solution level.
- Synchronizing Push details is dependent on the generation of System-ID (dependent on the configuration of Zang domain and APNS) and Public Key/Private Key. Enabling APNS at the solution level, synchronizes the push button.
- Web-Manager needs to synchronize the System-ID and Public/Private key pair in **System Security** settings generated in primary server of SCN nodes.
- To sync security settings, the administrator should have access to security settings of IP Office
- Adding a new expansion to the existing solution synchronizes the configuration to the expansion. But synchronization of the push details(security settings) should be done manually using the synchronization button in Web-Manager by Administrator.
- In the case of IP Office 500v2 systems in SCN or Server Edition without a centralized primary, ensure the company domain is configured and verified.

Procedure

1. Select **System Settings** > **System** > **Avaya Push Notification Services**.
2. Select **Enable Apple Push Notification Services**.
3. Click **OK**.

Note:

Increase the **No Answer Time** settings while using Avaya Workplace Client on iOS devices to at least 20 seconds. This can be done either by:

- Go to **System Settings** > **System** > **Telephony** > **Telephony** and increase the **Default No Answer Time** settings
- Select **Call Management** > **Users** > **Add** > **Telephony** > **Call Settings** and increase the **No Answer Time** setting of the individuals.

Related links

Apple push notification services on page 849

Chapter 84: Managing Users with LDAP

Lightweight Directory Access Protocol (LDAP) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the internet or on a corporate intranet. IP Office supports LDAP version 2 and 3 compliant directory services servers.

LDAP synchronization allows an administrator to quickly configure the IP Office system with users and extensions for the users based on an organization's LDAP directory. An LDAP directory is organized in a simple tree consisting of the following hierarchy of levels:

1. The root directory (the starting place or the source of the tree)
2. Countries
3. Organizations
4. Organizational units (divisions, departments, etc.)
5. Individuals (which includes people, files, and shared resources, for example printers)

An LDAP directory can be distributed among many servers. Each server can have a replicated version of the total directory that is synchronized periodically. An LDAP server is called a Directory System Agent (DSA). An LDAP server that receives a request from a user takes responsibility for the request, passing it to other DSA's as necessary, but ensuring a single coordinated response for the user.

Related links

Performing LDAP Synchronization on page 852
Creating a User Provisioning Rule for LDAP Synchronization on page 853

Performing LDAP Synchronization

Procedure

1. In Web Manager, navigate to the page **Solution** > **Solution Settings** > **User Synchronization Using LDAP** > **Connect to Directory Service**.
2. Define the connection to the LDAP server and to define the parameters for searching the LDAP directory. All fields are mandatory.
3. Click **Test Connection**.

   Web Manager attempts to connect to the LDAP server with the specified credentials.

4. Click **Synchronize User Fields**.
5. Map the IP Office user fields to the LDAP fields. Not all fields are mandatory.

   Note:

   You must click **Test Connection** on the **Connect to Directory Service** page to populate the LDAP fields on the **Synchronize User Fields** page.
6. Click **Preview Results** and review the list in the Preview Results window.
7. Click **Synchronize**.

   The User Synchronization window opens. Click the information icon to open a detailed report.

Related links

Managing Users with LDAP on page 852

Creating a User Provisioning Rule for LDAP Synchronization

A user provisioning rule (UPR) provides a way to manage the users to be imported. A UPR can provide the following properties for importing users.

- the IP Office system where the users are created
- starting extension
- extension template
- extension type
- user template

Procedure

1. In Web Manager, navigate to the page **Solution** > **Solution Settings** > **User Synchronization Using LDAP** > **Manage User Provisioning Rules**.
2. In the **User Provisioning Rule Name** field, enter a name for the rule.
3. Optional. Select an **IP Office Name** from the list.

   If an IP Office system is selected, the users are created on this system.
4. Optional. Enter a **Start Extension**.

   If a start extension is provided, users are assigned starting from this extension. If an extension number is in use, the extension number is skipped and the next available number is assigned.

Note:

Start Extension is a mandatory field if a value is provided for **Extension Template** or **Extension Type**.

5. Optional. Select an **Extension Template** from the **Select Extension Template** list.

   The extension template is applied to all users imported with this UPR.

6. Optional. Select an **Extension Type** to define the extension type created for each user.

   If both **Select Extension Template** and **Extension Type** are selected, the **Extension Template** is used.

7. Optional. Select a **User Template** from the **Select User Template** list.

   The user template is applied to all users imported with this UPR.

8. In the LDAP directory, enter the name of the UPR created in IP Office in the User column.
9. In IP Office, navigate to the page **Solution** > **Solution Settings** > **User Synchronization Using LDAP** > **Synchronize User Fields**.
10. Map the IP Office fields defined in the user provisioning rule to **User Provisioning Rule**.

Related links

Managing Users with LDAP on page 852

Chapter 85: Message Waiting Indication

Message waiting indication (MWI) or a message lamp is supported for a wide variety of phones. It is used to provide the user with indication of when their voicemail mailbox contains new messages. It can also be configured to provide them with indication when selected hunt group mailboxes contain new messages.

Avaya digital and IP phones all have in-built message waiting lamps. Also for all phone users, the one-X Portal for IP Office application provides message waiting indication.

Related links

Message Waiting Indication for Analog Phones on page 855
Message Waiting Indication for Analog Trunks on page 856

Message Waiting Indication for Analog Phones

For analog phones, the system supports a variety of analog message waiting indication (MWI) methods. The method used for an individual analog extension is set for the **Extn | Analog | Message Waiting Lamp Indication Type** field. Those methods are

- **101V**
- **51V Stepped**
- **81V**
- **Bellcore FSK**
- **Line Reversal A**
- **Line Reversal B**
- **None**
- **On**

The 101V method is only supported when using a Phone V2 expansion module.

81V is typically used in European countries. 51V Stepped is used in most other countries. However the actual method used for a particular model of analog phone should be confirmed with the phone manufacturer's documentation.

The **Message Waiting Lamp Indication Type** field also provides options for **None** (no MWI operation) and **On**. **On** selects a default message waiting indication method based on the system locale.

'On' Method	Locale
81V	Belgium, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Netherlands, Norway, Poland, Portugal, Russia, Saudi Arabia, Sweden, Switzerland, United Kingdom.
51V Stepped	Argentina, Australia, Brazil, Canada, Chile, China, Colombia, Japan, Korea, Mexico, New Zealand, Peru, South Africa, Spain, United States.

For the United Kingdom system locale (eng), the default Caller Display Type (UK) allows updates of an analog phone's ICLID display whilst the phone is idle. The system uses this facilities to display the number of new messages and total number of messages in the users own mailbox. This feature is not supported with other Caller Display Types.

Hunt Group Message Waiting Indication

By default no message waiting indication is provided for hunt group voicemail mailboxes. Message waiting indication can be configured by adding an **H** entry followed by the hunt groups name to the Source Numbers tab of the user requiring message waiting indication for that hunt group. For example, for the hunt group Sales, add **HSales**. Hunt group message waiting indication does not require the user to be a member of the hunt group.

Related links

Message Waiting Indication on page 855

Message Waiting Indication for Analog Trunks

IP Office can provide a MWI for analog trunks from the PSTN network that terminate on an ATM4U-V2 card. Multiple users can be configured to receive a MWI from a single analog line. Users can receive an MWI from multiple lines. Configuring a user for MWI includes configuraton of a button for automatically dialing the message center.

Note the following conditions.

- Only supported for analog trunks terminating on the ATM4U-V2 card.
- When Analog Trunk MWI is selected as the Voicemail Type, no other voicemail system is active. As a result, hunt group queue announcements are not supported, since they require Embedded Voice Mail or Voicemail Pro.
- All analog trunks configured for MWI must use the same message center number. Multiple message centers are not supported.
- Not supported in One-X Portal.
- No TAPI is provided for analog trunk MWI status.
- Not supported across multiple IP Office systems. If the analog line is on a different node than the user’s phone, that phone cannot receive an MWI for the line.
- Mobile twinning is not supported. Analog trunk MWI is displayed only on the master set.
- Internal twinning is not supported automatically. However, the twinned set can be configured to receive the same analog trunk MWI as the master set.

Configuring MWI for an Analog Trunk

1. Go to **System | Voicemail**. In the **Voicemail** field, select **Analog Trunk MWI**.
2. In the **Destination** field, enter the message center telephone number.
3. Select the **Line** you want to configure for Analog MWI, and then select the **Analog Options** tab.
4. In the **MWI Standard field**, select **Bellcore FSK**.
5. Select the **User** you want to configure for MWI and then select the **Button Programming** tab.
6. Select the button you want to configure and then click **Edit**.
7. In the **Action** field click the browse (...) button and select **Advanced > Voicemail > Monitor Analog Trunk MWI**.
8. In the **Action Data** field, enter the line appearance ID of the analog line.

Related links

Message Waiting Indication on page 855

Chapter 86: Configuring User Rights

For most settings in a user rights template, the adjacent drop down list is used to indicate whether the setting is part of the template or not. The drop down options are:

- **Apply User Rights Value** Apply the value set in the user rights template to all users associated with the template.
  - The matching user setting is grayed out and displays a lock symbol.
  - Users attempting to change the settings using short codes receive inaccessible tone.
- **Not Part of User Rights** Ignore the user rights template setting.

Default User Rights

For defaulted systems, the following user rights are created as a part of the default configuration. Fields not listed are not part of the user rights.

Note:

When a user logs in as a Outbound Contact Express agent, the Outdialer user rights are automatically applied. When the agent logs out, the previous user rights are applied.

✓ = Set to On. ✗ = Set to Off. – = Not part of the user rights.

User Rights	IP Hard Phone	Mailbox	Paging	Outdialer
Priority	✓ 5	✓ 5	✓ 5	✓ 5
Voicemail	–	✓	–	✗
Voicemail Ringback	✗	✗	–	✗
Outgoing Call Bar	✗	✗	✗	✓
No Answer Time	✓ 0	✓ 0	✓ 0	0
Transfer Return Time	✓ 0	✓ 0	✓ 0	0
Individual Coverage Time	✓ 10	✓ 10	✓ 10	10
Busy on Held	✗	–	–	✓
Call Waiting	✗	✗	✗	✗
Can Intrude	✗	✗	✗	✗
Cannot be Intruded	✓	✗	✗	✗

Table continues…

User Rights	IP Hard Phone	Mailbox	Paging	Outdialer
Deny Auto Intercom Calls	–	–	–	✗
Enable Inhibit Off-Switch Forward/ Transfer	–	–	–	✓
Enable Outgoing Call Bar	–	–	–	✓
Centralized Logging	–	–	–	✗
Force Login	–	–	–	✗
Force Account Code	✗	✗	✗	✗
Button Programming	1: a= 2: b= 3: c= 6: Dial *17	✓	–	1: a= 2: b= 3: Supervisor 4: Extn Logout

User Rights	Call Center Agent	Boss	Application	Default
Priority	✓ 5	✓ 5	✓ 5	✓ 5
Voicemail	–	–	–	–
Voicemail Ringback	✗	✗	✗	✗
Outgoing Call Bar	✗	✗	✗	✗
No Answer Time	✓ 0	✓ 0	✓ 0	✓ 0
Transfer Return Time	✓ 0	✓ 0	✓ 0	✓ 0
Individual Coverage Time	✓ 10	✓ 10	✓ 10	✓ 10
Busy on Held	✗	✗	✗	✗
Call Waiting	✗	✗	✓	✗
Can Intrude	✗	✗	✗	✗
Cannot be Intruded	✗	✗	✓	✓
Deny Auto Intercom Calls	–	–	–	–
Enable Inhibit Off-Switch Forward/ Transfer	–	–	–	–
Enable Outgoing Call Bar	–	–	–	–
Centralized Logging	–	–	–	–
Force Login	✓	–	–	–

Table continues…

User Rights	Call Center Agent	Boss	Application	Default
Force Account Code	✗	✗	✗	✗
Button Programming	1: a= 2: b= 4: HGEna 5: DNDOn 6: Busy	1: a= 2: b= 3: c= 6: DNDOn 7: Dial *17	✓	1: a= 2: b= 3: c=

Related links

Adding User Rights on page 860
Creating a User Right Based on an Existing User on page 860
Associating User Rights to a User on page 861
Copy User Rights Settings over a User's Settings on page 861

Adding User Rights

Procedure

1. Select **User Rights**.
2. Click and select **User Rights**.
3. Enter a name.
4. Configure the user rights as required.
5. Click **OK**.

Related links

Configuring User Rights on page 858

Creating a User Right Based on an Existing User

About this task

Procedure

1. Select **User Rights**.
2. In the group pane, right-click and select **New User Rights from a User**.
3. Select the user and click **OK**.

Related links

Configuring User Rights on page 858

Associating User Rights to a User

Procedure

1. Select **User Rights** or **User**.
2. In the group pane, right-click and select **Apply User Rights to Users**.
3. Select the user rights to be applied.
4. On the **Members of this User Rights** sub tab select the users to which the user rights should be applied as their Working Hours User Rights.
5. On the **Members when out of hours** sub tab select which users should use the selected user rights as their out of hours user rights.
6. Click **OK**.

Related links

Configuring User Rights on page 858

Copy User Rights Settings over a User's Settings

About this task

This process replaces a user's current settings with those that are part of the selected user rights. It does not associate the user with the user rights.

Procedure

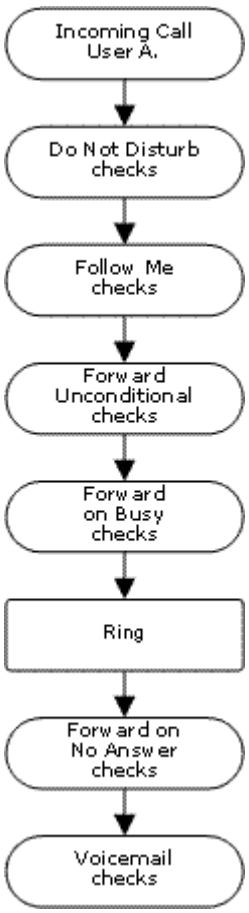
1. Select **User Rights**.
2. In the group pane, right-click and select **Copy user rights values to users**.
3. Select the user rights to be applied.
4. Click **OK**.

Related links

Configuring User Rights on page 858

Chapter 87: DND, Follow Me and Forwarding

This section contains topics looking at how users can have their calls automatically redirected. As illustrated, there is an order of priority in which the redirect methods are used.



1. **Do Not Disturb (DND)**

   Redirect all calls to voicemail if available, otherwise return busy tone. DND overrides all the redirect method below unless the calling number is in the user's DND Exception Numbers List.

2. **Follow Me**

   Redirect all calls to another extension that the users is temporarily sharing. Follow Me overrides Forward Unconditional. The Follow Me destination is busy or does not answer, the user's Forward on Busy or Forward on No Answer options can be used if set.

3. **Forward Unconditional**

   Redirect the user's external calls to another number. That number can be any number the user can normally dial including external numbers. Forwarding of hunt group and internal calls is optional. Forward Unconditional overrides Forward on Busy and Forward on No Answer.

   If the destination is an internal user on the same system, they are able to transfer calls back to the user, overriding the Forward Unconditional.

4. **Forward on Busy**

   Redirects the user's external calls when the system sees the user as being busy. Uses the same number as Forward Unconditional unless a separate Forward on Busy Number is set. Forwarding internal calls is optional. Forward on Busy overrides Forward on No Answer.

5. **Forward on No Answer**

   Redirects the user's external calls when they ring for longer than the user's No Answer Time. Uses the same number as Forward Unconditional unless a separate Forward on Busy Number is set. Forwarding internal calls is optional.

Retrieving Externally Forwarded Calls:

Where a call is forwarded to an external destination and receives busy or is not answered within the forwarding user's **No Answer Time**, the system will attempt to retrieve the call. If forwarded on a trunk that does not indicate its state the call is assumed to have been answered, for example analog loop start trunks.

Off-Switch Forwarding Restrictions:

User forwarding is subject to the same restrictions as transferring calls. To bar a user from forwarding calls to an external number, the **Inhibit Off-Switch Forward/Transfers (User | Telephony | Supervisor Settings)** option. To bar all users from forwarding calls to external numbers the Inhibit **Off-Switch Forward/Transfers** option can be used.

When transferring a call to another extension that has forwarding enabled, the type of call being transferred is used. For example, if transferring an external call, if the transfer target has forwarding of external calls enabled then the forward is used.

Block Forwarding:

The Block Forwarding setting is used for enforcing predictable call routing, where the call should always go to the same destination. This setting was implemented for contact center applications.

Block Forwarding can be set for a user on the **User | Forwarding** page or as a user rights setting on the **User Rights | Forwarding** page.

Related links

Do Not Disturb (DND) on page 863
Follow Me on page 865
Forward Unconditional on page 867
Forward on Busy on page 869
Forward on No Answer on page 871
Determining a User's Busy Status on page 873
Chaining on page 874

Do Not Disturb (DND)

Summary: Redirect all calls to busy tone or to voicemail if available except those in your DND exceptions list.

Do Not Disturb (DND) is intended for use when the user is present but for some reason does not want to be interrupted. Instead calls are sent to voicemail if available, otherwise they receive busy tone.

- **Exceptions** Specific numbers can be added to the user's Do Not Disturb Exception List. Calls from those numbers override DND. N and X wildcards can be used at the end of exception numbers to match a range of numbers. For external numbers, this uses the incoming caller line ID (ICLID) received with the call.
- **Priority** Enabling DND overrides any Follow Me or forwarding set for the user, except for calls in the user's Do Not Disturb Exception List.
- **Phone** When enabled, the phone can still be used to make calls. An **N** is displayed on many Avaya phones. When a user has do not disturb in use, their normal extension will give alternate dialtone when off hook.

Applied to

Call Types Blocked		Call Treatment
Internal	✓	Voicemail if available, otherwise busy tone.
External	✓	Voicemail if available, otherwise busy tone.
Hunt Group	✓	Call not presented (DND exceptions are not used).
Page	✓	Call not presented.
Follow Me	✗	Rings.
Forwarded	✓	Busy.
VM Ringback	✗	Rings
Automatic Callback	✗	Rings
Transfer Return	✗	Rings.
Hold Return	✗	Rings.
Park Return	✗	Rings.
Twinning	✓	Voicemail if available, otherwise busy tone.

Do Not Disturb and Twinning

- **Mobile Twinning** Selecting DND disables mobile twinning.
- **Internal Twinning**
  - Logging out or setting do not disturb at the primary stops twinned calls alerting at the secondary also.
  - Logging out or setting do not disturb at the secondary only affects the secondary.
- **Do Not Disturb Exceptions List** For both types of twinning, when DND is selected, calls from numbers entered in the user's Do Not Disturb Exception List are presented to both the primary and secondary phones.

Do Not Disturb Controls

Do Not Disturb	
Manager	A user's DND settings can be viewed and changed through the User | DND tab within the system configuration settings.
Controls	The following short code features/button programming actions can be used:
Voicemail	If voicemail is available, it is used instead of busy tone for callers not in the users exceptions list. For Voicemail Pro, the Play Configuration Menu action can be used to let callers switch DND on or off.
SoftConsole	A SoftConsole user can view and edit a user's DND settings except exception numbers. Through the directory, select the required user. Their current status including DND is shown. Double-click on the details to adjust DND on or off.

Feature/Action	Short Code	Default	Button
Do Not Disturb On	✓	*08	✓ - Toggles.
Do Not Disturb Off	✓	*09	✓
Do Not Disturb Exception Add	✓	*10*N#	✓
Do Not Disturb Exception Delete	✓	*11*N#	✓
Cancel All Forwarding	✓	*00	✓

Related links

DND, Follow Me and Forwarding on page 862

Follow Me

Summary: Have your calls redirected to another user's extension, but use your coverage, forwarding and voicemail settings if the call receives busy tone or is not answered.

Follow Me is intended for use when a user is present to answer calls but for some reason is working at another extension such as temporarily sitting at a colleague's desk or in another office or meeting room. Typically you would use Follow Me if you don't have a Hot Desking log in code or if you don't want to interrupt your colleague from also receiving their own calls, ie. multiple users at one phone.

- **Priority**

  Follow Me is overridden by DND except for callers in the user's DND Exception Numbers List. Follow Me overrides Forward Unconditional but can be followed by the user's Forward on Busy or Forward on No Answer based on the status of the Follow Me destination.

- **Destination**

  The destination must be an internal user extension number. It cannot be a hunt group extension number or an external number.

- **Duration**

  The Follow Me user's no answer timeout is used. If this expires, the call either follows their Forward on No Answer setting if applicable, or goes to voicemail is available. Otherwise the call continues to ring at the destination.

- **Phone**

  When enabled, the phone can still be used to make calls. When a user has follow me in use, their normal extension will give alternate dial tone when off hook.

- **Exceptions**

  - The Follow Me destination extension can make and transfer calls to the follow me source.

- The call coverage settings of the user are applied to their Follow Me calls. The call coverage settings of the destination are not applied to Follow Me calls it receives.

Call Types Redirected		
Internal	✓	Redirected.
External	✓	Redirected.
Hunt Group	✓	Redirected*.
Page	✓	Redirected.
Follow Me	✗	Not redirected.
Forwarded	✓	Redirected.
VM Ringback	✗	Not redirected.
Automatic Callback	✗	Not redirected.
Transfer Return	✗	Not redirected.
Hold Return	✗	Not redirected.
Park Return	✗	Not redirected.

*Except calls for "Longest Waiting" type hunt groups.

Follow Me Controls	
Manager	A user's Follow Me settings can be viewed and changed through the User | Forwarding tab within the system configuration settings. Note that on this tab, entering a Follow Me Number also enables Follow Me.
Controls	The following short code features/button programming actions can be used:
Voicemail	For calls initially targeted to the user but then redirected, when voicemail is invoked the mailbox of the user is used and not the mailbox of the destination. For Voicemail Pro, the Play Configuration Menu action can be used to let callers alter or set their current Follow Me destination.
SoftConsole	A SoftConsole user can view and edit a user's Follow Me settings. Through the directory, select the required user. Their current status including Follow Me is shown. Double-click on the details and select Forwarding to alter their forwarding settings including Follow Me.

Feature/Action	Short Code	Default	Button
Follow Me Here	✓	*12*N#	✓
Follow Me Here Cancel	✓	*13*N#	✓
Follow Me To	✓	*14*N#	✓
Cancel All Forwarding	✓	*00	✓

Related links

DND, Follow Me and Forwarding on page 862

Forward Unconditional

Summary: Have your calls redirected immediately to another number including any external number that you can dial.

- **Priority**

  This function is overridden by DND and or Follow Me if applied. **Forward Unconditional** overrides **Forward on Busy**.

- **Destination**

  The destination can be any number that the user can dial. If external and Inhibit Off-Switch Transfers is applied, the caller is directed to voicemail if available, otherwise they receive busy tone. If the destination is an internal user on the same system, they are able to transfer calls back to the user, overriding the Forward Unconditional.

- **Duration**

  After being forwarded for the user's no answer time, if still unanswered, the system can apply additional options. It does this if the user has forward on no answer set for the call type or if the user has voicemail enabled.

  - If the user has forward on no answer set for the call type, the call is recalled and then forwarded to the forward on no answer destination.
  - If the user has voicemail enabled, the call is redirected to voicemail.
  - If the user has both options set, the call is recalled and then forwarded to the forward on no answer destination for their no answer time and then if still unanswered, redirected to voicemail.
  - If the user has neither option set, the call remains redirected by the forward unconditional settings.

Note that for calls redirected via external trunks, detecting if the call is still unanswered requires call progress indication. For example, analog lines do not provide call progress signalling and therefore calls forwarded via an analog lines are treated as answered and not recalled.

- **Phone**

  When enabled, the phone can still be used to make calls. An **D** is displayed on DS phones. When a user has forward unconditional in use, their normal extension will give alternate dialtone when off hook.

- **Calls Forwarded**

  Once a call has been forwarded to an internal destination, it will ignore any further **Forward No Answer** or **Forward on Busy** settings of the destination but may follow additional **Forward Unconditional** settings unless that creates a loop.

Call Types Forwarded		
Internal	✓	Optional.

Table continues…

Call Types Forwarded		
External	✓	Forwarded.
Hunt Group	✓	Optional.*
Page	✗	Not presented.
Follow Me	✗	Rings.
Forwarded	✓	Forwarded.
VM Ringback	✗	Rings.
Automatic Callback	✗	Rings.
Transfer Return	✗	Rings.
Hold Return	✗	Ring/hold cycle.
Park Return	✗	Rings.

*Optional only for calls targeting sequential and rotary type groups. Includes internal call to a hunt group regardless of the forward internal setting.

- **To Voicemail**: Default = Off.

  If selected and forward unconditional is enabled, calls are forwarded to the user's voicemail mailbox. The **Forward Number** and **Forward Hunt Group Calls** settings are not used. This option is not available if the system's **Voicemail Type** is set to **None**. 1400, 1600, 9500 and 9600 Series phone users can select this setting through the phone menu. Note that if the user disables forward unconditional the **To Voicemail** setting is cleared.

Forward Unconditional Controls

Forward Unconditional Controls	
Manager	A user's forwarding settings can be viewed and changed through the User | Forwarding tab within the system configuration settings.
Controls	The following short code features/button programming actions can be used:
Voicemail	For calls initially targeted to the user but then redirected, when voicemail is invoked the mailbox of the user is used and not the mailbox of the destination. For Voicemail Pro, the Play Configuration Menu action can be used to let callers set their current forwarding destination and switch Forwarding Unconditional on/off.
SoftConsole	A SoftConsole user can view and edit a user's forwarding settings. Through the directory, select the required user. Their current forwarding status is shown. Double-click on the details and select Forwarding to alter their forwarding settings.

Feature/Action	Short Code	Default	Button
Forward Number	✓	*07*N#	✓
Forward Unconditional On	✓	*01	✓ - Toggles.
Forward Unconditional Off	✓	*02	✓

Table continues…

Feature/Action	Short Code	Default	Button
Forward Hunt Group Calls On	✓	✗	✓ - Toggles.
Forward Hunt Group Calls Off	✓	✗	✓
Disable Internal Forwards	✓	✗	✗
Enable Internal Forwards	✓	✗	✗
Disable Internal Forwards Unconditional	✓	✗	✗
Enable Internal Forwards Unconditional	✓	✗	✗
Set No Answer Time	✓	✗	✓
Cancel All Forwarding	✓	*00	✓

Related links

DND, Follow Me and Forwarding on page 862

Forward on Busy

Summary: Have your calls redirected when you are busy to another number including any external number that you can dial.

The method by which the system determines if a user is 'busy' to calls depends on factors such as whether they have multiple calls appearance buttons or Call Waiting and or Busy on Held set. See Busy.

- **Priority**

  This function is overridden by DND and or Forward Unconditional if applied. It can be applied after a Follow Me attempt. It overrides Forward on No Answer.

- **Destination**

  The destination can be any number that the user can dial. The Forward Unconditional destination number is used unless a separate number Forward on Busy Number is set. If Inhibit Off-Switch Transfers is applied, the caller is directed to voicemail if available, otherwise they receive busy tone.

- **Duration**

  The destination is rung using the forwarding user's No Answer Time. If this expires, the call goes to voicemail is available. Calls to an external destination sent on trunks that do not signal their state are assumed to have been answered, for example analog loop start trunks.

- **Phone**

  Forward on Busy is not indicated and normal dial tone is used.

- **Calls Forwarded**

  Once a call has been forwarded to an internal destination, it will ignore any further **Forward No Answer** or **Forward on Busy** settings but may follow additional **Forward Unconditional** settings.

Call Types Forwarded		
Internal	✓	Optional.
External	✓	Forwarded.
Hunt Group	✗	Not presented.
Page	✗	Not presented.
Follow Me	✗	Rings.
Forwarded	✓	Forwarded.
VM Ringback	✗	Rings.
Automatic Callback	✗	Rings.
Transfer Return	✗	Rings.
Hold Return	✗	Ring/hold cycle.
Park Return	✗	Rings.

Forward on Busy Controls	
Software Level	A user's forwarding settings can be viewed and changed through the User | Forwarding tab within the system configuration settings.
Controls	The following short code features/button programming actions can be used:
Voicemail	For calls initially targeted to the user but then redirected, when voicemail is invoked the mailbox of the user is used and not the mailbox of the destination. For Voicemail Pro, the Play Configuration Menu action can be used to let callers set the forward destination.
SoftConsole	A SoftConsole user can view and edit a user's forwarding settings. Through the directory, select the required user. Their current forwarding status is shown. Double-click on the details and select Forwarding to alter their forwarding settings.

Feature/Action	Short Code	Default	Button
Forward Number	✓	*07*N#	✓
Forward on Busy Number	✓	*57*N#	✓
Forward on Busy On	✓	*03	✓ - Toggles.
Forward on Busy Off	✓	*04	✓
Disable Internal Forwards	✓	✗	✗
Enable Internal Forwards	✓	✗	✗
Disable Internal Forwards Busy or No Answer	✓	✗	✗

Table continues…

Feature/Action	Short Code	Default	Button
Enable Internal Forwards Busy or No Answer	✓	✗	✗
Set No Answer Time	✓	✗	✓
Cancel All Forwarding	✓	*00	✓

Related links

DND, Follow Me and Forwarding on page 862

Forward on No Answer

Summary: Have your calls redirected another number if it rings without being answered.

- **Priority**

  This function is overridden by DND and Forward on Busy if applied. It can be applied after a Follow Me attempt. Forward Unconditional overrides Forward on Busy and Forward on No Answer.

- **Destination**

  The destination can be any number that the user can dial. The Forward Unconditional destination number is used unless a separate number Forward on Busy Number is set. If Inhibit Off-Switch Transfers is applied, the caller is directed to voicemail if available, otherwise they receive busy tone.

- **Duration**

  The destination is rung using the forwarding user's No Answer Time. If this expires, the call goes to voicemail is available. Otherwise the call continues to ring at the destination. Calls to an external destination sent on trunks that do not signal their state are assumed to have been answered, for example analog loop start trunks.

- **Phone**

  Forward on No Answer is not indicated and normal dial tone is used.

- **Calls Forwarded**

  Once a call has been forwarded to an internal destination, it will ignore any further **Forward No Answer** or **Forward on Busy** settings but may follow additional **Forward Unconditional** settings.

Call Types Forwarded		
Internal	✓	Optional.
External	✓	Forwarded.
Hunt Group	✗	Not applicable.

Table continues…

Call Types Forwarded		
Page	✗	Not applicable.
Follow Me	✗	Rings.
Forwarded	✓	Forwarded.
VM Ringback	✗	Rings.
Automatic Callback	✗	Rings.
Transfer Return	✗	Rings.
Hold Return	✗	Ring/hold cycle.
Park Return	✗	Rings.

Forward on No Answer Controls	
Manager	A user's forwarding settings can be viewed and changed through the User | Forwarding tab within the system configuration settings.
Controls	The following short code features/button programming actions can be used:
Voicemail	For calls initially targeted to the user but then redirected, when voicemail is invoked the mailbox of the user is used and not the mailbox of the destination. For Voicemail Pro, the Play Configuration Menu action can be used to let callers set the forward destination. It cannot however be used to enable Forward on Busy or set a separate Forward on Busy number.
SoftConsole	A SoftConsole user can view and edit a user's forwarding settings. Through the directory, select the required user. Their current forwarding status is shown. Double-click on the details and select Forwarding to alter their forwarding settings.

Feature/Action	Short Code	Default	Button
Forward Number	✓	*07*N#	✓
Forward on Busy Number	✓	*57*N#	✓
Forward on No Answer On	✓	*05	✓ - Toggles.
Forward on No Answer Off	✓	*06	✓
Enable Internal Forwards	✓	✗	✗
Disable Internal Forwards	✓	✗	✗
Enable Internal Forwards Busy or No Answer	✓	✗	✗
Disable Internal Forwards Busy or No Answer	✓	✗	✗
Set No Answer Time	✓	✗	✓
Cancel All Forwarding	✓	*00	✓

Related links

DND, Follow Me and Forwarding on page 862

Determining a User's Busy Status

Various system features allow users to handle more than one call at a time. Therefore the term "busy" has different meanings. To other users it means whether the user is indicated as being busy. To the system it means whether the user is not able to receive any further calls. The latter is used to trigger 'busy treatment', either using a user's **Forward on Busy** settings or redirecting calls to voicemail or just returning busy tone.

- **Busy Indication - In Use**

  The user busy indication provided to programmable buttons and to user applications, is based on the monitored user's hook switch status. Whenever the user is off-hook, they will be indicated as being busy regardless of call waiting or call appearance settings.

- **Busy to Further Calls**

  Whether a user can receive further calls is based on a number of factors as described below.

  - **Logged In and Present**

    Is the user logged into an extension and is that extension physically connected to the system.

  - **Busy on Held**

    If a user enables their Busy on Held setting, whenever they have a call on hold, they are no longer available to any further incoming calls.

  - **Appearance Buttons**

    A user's call appearance button are used to receive incoming calls. Normally, whilst the user has any free call appearance buttons, they are available to receive further calls. Exceptions are:

    - **Reserve Last Appearance**

      Users with appearance buttons require a free call appearance button to initiate transfers or conferences. Therefore it is possible through the user's configuration settings to reserve their last call appearance button for outgoing calls only.

    - **Other Appearance Buttons**

      Calls may also be indicated on line, call coverage and bridged appearance buttons.

- **Call Waiting**

  Users of phones without appearance buttons can use call waiting. This adds an audio tone, based on the system locale, when an additional call is waiting to be answered. Only one waiting call is supported, any further calls receive busy treatment.

- **Hunt Group Calls**

  A user's availability to receive hunt group calls is subject to a range of other factors. See Member Availability.

Related links

DND, Follow Me and Forwarding on page 862

Chaining

Chaining is the process where a call forward to an internal user destination is further forwarded by that user's own forwarding settings.

- **Follow Me Calls**

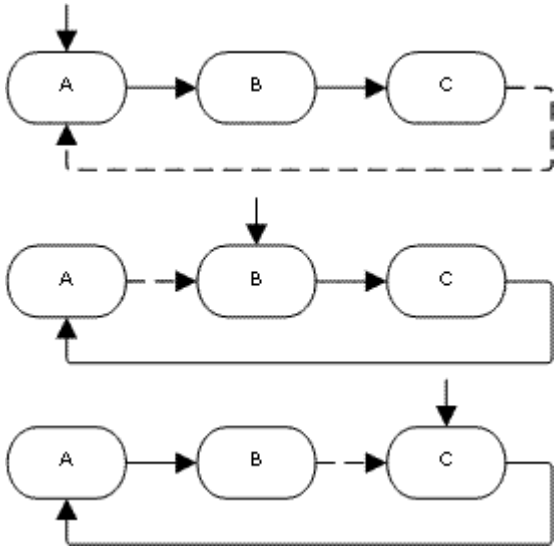
  Follow Me calls are not chained. They ignore the forwarding, Follow Me and Do Not Disturb settings of the Follow Me destination.

- **Voicemail**

  If the call goes to voicemail, the mailbox of the initial call destination before forwarding is used.

- **Looping**

  When a loop would be created by a forwarding chain, the last forward is not applied. For example the following are scenarios where A forwards to B, B forwards to C and C forwards to A. In each case the final forward is not used as the destination is already in the forwarding chain.



- **Hunt Group Loop**

  If a user forwards a call to a hunt group of which they are a member, the group call is not presented to them but is presented to other members of the hunt group.

- **Maximum Number of Forwards**

  A maximum of 10 forwarding hops are supported for any call.

- **Calls Forwarded**

  Once a call has been forwarded to an internal destination, it will ignore any further **Forward No Answer** or **Forward on Busy** settings but may follow additional **Forward Unconditional** settings.

Related links

DND, Follow Me and Forwarding on page 862

Chapter 88: Hot Desking

Hot desking allows users to log in at another phone. Their incoming calls are rerouted to that phone and their user settings are applied to that phone. There are a number of setting and features which affect logging in and out of system phones.

To hot desk, a user must be assigned a **Login Code** (**User** > **Telephony** > **Supervisor Settings**) in the system configuration.

By default, each system extension has an **Base Extension** setting. This associates the extension with the user who has the matching **Extension** settings as being that extension's default associated user.

- By leaving the **Base Extension** setting for an extension blank, it is possible to have an extension with no default associated user. This is only supported for non-IP/CTI extensions. Extensions in this state use the settings of a special user named **NoUser**. On suitable phones the display may show **NoUser**.
- You can create users whose Extension directory number is not associated with any physical extension. These users must have a log in code in order to log in at a phone when they need to make or receive calls. In this way the system can support more users than it has physical extensions.
- Remote extensions must have an associated default user who is logged in. That user's user profile establishes the extension's right to operate as a remote extension. Any other user logging in over the default user must also have a user profile that allows remote extension usage.

Related links

Hot Desking Operation on page 877
Logging Out on page 877
Hot Desking Controls on page 878
Hot Desking in an IP Office Network on page 878
Call Center Agents on page 879
Hot Desking Examples on page 879
Automatic Log Out on page 881

Hot Desking Operation

When another user logs in at an extension, they control that phone. Any existing user, including the default associated user, is logged out of that phone.

- Any user settings not applicable to the type of phone on which the user has logged in become inaccessible. For example some programmable button features will become inaccessible if the phone at which a user logs in does not have a sufficient programmable buttons.
- 1400 Series, 1600 Series, 9500 Series, 9600 Series and J100 Series telephones all use the centralized call log and centralized personal directory features that move those settings with the user as they hot desk.
- Other Avaya H.323 IP telephones can be configured to backup and restore user settings to a file server when a user hot desks between phones. The range of settings supported depends on the particular phone model. Refer to the Avaya IP Office™ Platform H.323 Telephone Installation manual.
- For all other features and phone types, it must be assumed that any settings and data shown by the phone is stored by the phone and are still accessible after logging off.
- By default the IP Office system blocks J129 and H175 phones from being used for hot-desking. If required, the NoUser source number `SIP_ENABLE_HOT_DESK` enables hot-desking support for those phones.
- Hot-desking is not supported for SIP softphone applications. That includes clients running on Avaya Vantage™ telephones.

Related links

Hot Desking on page 876

Logging Out

When a user logs out or is logged out by someone else logging in, they are automatically logged back in at the extension for which they are the default associated user if no one else is logged in at that extension. However this does not happen for users set to **Forced Login** (**User** > **Telephony** > **Supervisor Settings**).

- For each user, you can configure how long the extension at which they are logged in can remain idle before they are automatically logged out. This is done using the Login Idle Period option. This option should only be used in conjunction with Force Login.
- Logged in users who are members of a hunt group can be automatically logged out if they do not answer hunt group calls presented to them. This is done by selecting **Logged Off** as the user's **Status on No Answer** (**User** > **Telephony** > **Supervisor Settings**) setting.
- Calls to a logged out user are treated as if the user is busy until the user logs in.

Related links

Hot Desking on page 876

Hot Desking Controls

Logging in and out at a phone can be done either using system short codes or programmable buttons.

- The default system short code for logging in, is ***35*N#** where the user replaces N with their extension number and log in code separated by a *. This uses the short code feature **ExtnLogin**. If the user dials just a log in code as N, it is checked against the user with the same extension number as the extension's base extension number.
- The default system short code for logging out is ***36**. This uses the short code feature **ExtLogout**.
- The **ExtnLogin** and **ExtnLogout** features can be assigned to programmable buttons on suitable Avaya phones. The **ExtnLogin** button prompts the user to enter their details.

Related links

Hot Desking on page 876

Hot Desking in an IP Office Network

Hot desking can be used in a network of IP Office systems.

- The IP Office system on which the user is configured is termed their 'home' system
- All other IP Office systems are 'remote' systems.

The following additional features are supported for hot-desking with a network of IP Office systems.

Hot Desking onto another IP Office System

The system supports hot desking between systems within a network of IP Office systems. In the descriptions below:

When a user logs in to a remote system:

- The user's incoming calls are automatically rerouted to the remote IP Office system.
- The user's outgoing calls uses the settings of the remote IP Office system.
- The user's license privileges move with them. For example, their user profile setting is retained with the remote IP Office needing licenses for that profile type.

- The user's own settings are transferred. However, some settings may become unusable or may operate differently:
  - User rights are not transferred to the remote system but the name of any user rights associated with the user are transferred. If user rights with the same name exist on the remote system, then they are used. The same applies for user rights applied by time profiles, if time profiles with the same name exist on the remote system .
  - Appearance buttons configured for users on the home system will no longer operate.
  - Various other settings may either no longer work or may work differently depending on the configuration of the remote system at which the user has logged in.

If the user's home system is disconnected from the network while the user is remotely hot desked, the user remains remotely hot desked. They can remain in that state unless the remote system is restarted. Note however, when the user's home system is reconnected, the user may be automatically logged back onto that system.

Dialing from another IP Office System (Break Out)

In some scenarios a hot desking user logged in at a remote system will want to dial a number using the system short codes of another system, typically their home system. This can be done using either short codes with the **Break Out** feature or a programmable button set to **Break Out**. This feature can be used by any user within the multi-site network but is of most use to remote hot desked users.

Related links

Hot Desking on page 876

Call Center Agents

On systems with a call center application such as Compact Contact Center (CCC) or Compact Business Center (CBC), logging in and logging out is a key part of tracking and reporting on call center agents. It also controls call distribution as, until the agent logs in, their hunt group membership is seen as disabled.

For CCC, CBC and Delta Server, an agent is defined as being a user with a Login Code and set to Forced Login. Those users consume a CCC agent license.

Related links

Hot Desking on page 876

Hot Desking Examples

The following are example of different ways that the hot desking settings can be used.

Related links

Hot Desking on page 876

Scenario 1: Occasional Hot Desking

About this task

In this scenario, a particular user, for this example extension 204, needs to occasionally work at other locations within the building.

Procedure

1. A **Login Code** is added to the user's configuration settings, for this example **1234**.
2. The user can now log in when needed at any other phone by dialing ***35*204*1234#**.

   The phone's default associated user is logged out by this and their calls get busy treatment. User 204 is also logged out their normal phone and their calls now rerouted to the phone at which they have logged in.
3. When finished, the user can dial ***36** to log out.
4. This logs the phone's normal default user back on.

   Its also logs the hot desking user back on at their normal extension.

Scenario 2: Regular Hot Desking

About this task

This scenario is very similar to the one above. However, the user doesn't want to be automatically logged back in on their normal phone until they return to its location.

Procedure

1. A **Login Code** is added to the user's configuration settings, for this example **1234**.
2. The Forced Login option is selected.
3. When the user logs out of the phone that they are currently using, they are no longer automatically logged in on their normal extension.

   When they return to it they must dial ***35*204*1234#** to log in.
4. Whilst not logged in anywhere, calls to the user receive busy treatment.

Scenario 3: Full Hot Desking

About this task

Similar to the scenarios above but this time the user doesn't have a regular phone extension that they use. In order to make and receive calls they must find a phone at which they can log in.

Procedure

1. The user is given an Extension directory number that is not matched by the extension directory number setting of any existing extension.

2. They are also given a **Login Code** and a **Login Idle Period** is set, for this example 3600 seconds (an hour). **Forced Login** isn't required as the user has no default extension at which they might be automatically logged in by the system.
3. The user can now log in at any available phone when needed.
4. If at the end of the business day they forget to log out, the Login Idle Period will eventually log them off automatically.

Scenario 4: Call Center Hot Desking

About this task

In this scenario, the phone extensions have no default extension number. Several phones set like this might be used in a call center where the agents use whichever desk is available at the start of their shift. Alternatively a set of desks with such phones might be provided for staff that are normally on the road but occasionally return to the office and need a temporary desk area to complete paper work.

Procedure

1. For the extensions, the Extension setting is left blank.

   This means that those phones will be associated with the NoUser user's settings and display **NOT LOGGED ON**.
2. The call center agents or road-warrior users are configured with Extension directory numbers that also don't match any existing physical extensions.

   They are all given Login Code numbers.
3. The users can log in at any of the extensions when required.

   When they log out or log in elsewhere, the extensions return to the NoUser setting.

Automatic Log Out

Normally a user can either log themselves out or be logged out by another user logging in. The following methods can be used by the system to automatically log out a user, so long as that user has a **Login Code** and is set to **Forced Login**.

Note: A remote hot desking user whose home system can no longer be seen by the remote system at which they are logged in is automatically logged out after 24 hours.

Idle Timeout:

The user **Login Idle Period** (**User | Telephony | Supervisor Settings**) can be used to automatically log out the user after a set period of phone inactivity. The period can be set between 1 to 99999 seconds and is based on call inactivity other than ringing calls.

Unanswered Calls:

Users who are members of hunt groups are presented with hunt group calls when they are logged in and not already on a call. If the user is logged in but not actually present they will continue to be presented with hunt group calls. In this scenario it can be useful to log the user off.

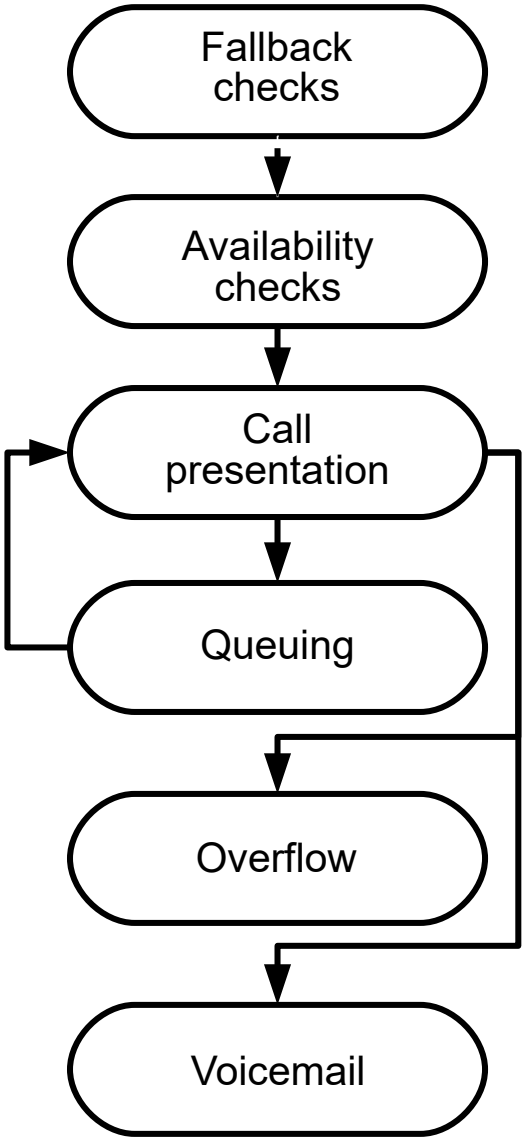
- **For the hunt group** On the **Hunt Group | Hunt Group** tab, use the **Agent's Status on No Answer Applies to** setting to select which types of unanswered hunt group calls should change the user's status. The options are:
  - **None**
  - **Any Calls**
  - **External Inbound Calls Only**
- **For the user** The **Status on No Answer** setting (**User | Telephony | Supervisor Settings**) can be used. This sets what the user's status should be changed to if they do not answer a hunt group call. The options are:
  - **Logged In** If this option is selected, the user's status is not changed.
  - **Busy Wrap-Up** If this option is selected, the user's membership status of the hunt group triggering the action is changed to disabled. The user can still make and receive calls and will still continue to receive calls from other hunt groups to which they belong.
  - **Busy Not Available** If this option is selected, the user's status is changed to do not disturb. This is the equivalent of DND and will affect all calls to the user.
  - **Logged Off** If this option is selected, the user’s status is changed to logged out. In that state the cannot make calls and cannot receive calls. Hunt group calls go to the next available agent and personal calls treat the user as being busy.

Related links

Hot Desking on page 876

Chapter 89: Group Operation

A group is a collection of users accessible through a single directory number. Calls to that group can be answered by any available member of the group. The order in which calls are presented can be adjusted by selecting different group types and adjusting the order in which group members are listed.



- **Call Presentation**: The order in which the available members of the group are used for call

presentation is selectable.

- **Availability**: There are a range of factors which control whether group calls are presented to a user in addition to that user being a member of the group.
- **Queuing**: This optional feature allows calls to be queued when the number of calls to be presented exceeds the number of available group members to which call can be presented.
- **Announcements**: On systems with a voicemail server (Voicemail Pro or Embedded Voicemail), announcements can be played to callers waiting to be answered. That includes calls that are ringing and calls that are queued.
- **Overflow**: This optional feature can be used to include additional agents from an overflow group or groups when a call is not answered.
- **Fallback**: A group can be taken out of operation manually or using a time profile. During fallback, calls can be redirected to a fallback group or sent to voicemail or just receive busy tone. Two types of fallback are supported; night service and out of service.
- **Voicemail**: Calls can be redirected to voicemail. The system allows selection of whether group calls remain in the group mailbox or are copied (broadcast) to the individual mailboxes of the group members. When messages are stored in the group's own mailbox, selection of who receives message waiting indication is possible.

Group Editing

Changing the name of a group has the following effects:

- A new empty mailbox is created on voicemail with the new group name.
- Records in other groups' Overflow lists will be updated.
- Out-of-Service and Night-Service fallback references are updated.

Modifying the extension number of a group updates the following:

- Group buttons.
- Overflow, Out of Service Fallback and Night Service Fallback group records.
- Incoming call route records.

When a group is deleted, all references to the deleted group will be removed including:

- Records in Incoming call routing tables.
- Transfer target in internal auto-attendant.
- Overflow, Night-Service or Fallback-Service on other groups.
- DSS keys monitoring group status.

Server Edition Group Management

Groups can be stored in the configuration of any system in the network. Groups created at the solution level on Manager and Web Manager are stored on the Primary Server. All groups can include users from anywhere in the network and are automatically advertised to and diallable on any of the systems in the network.

Groups configured on the Server Edition Primary by default fail over to the Server Edition Secondary. Groups configured on a Server Edition Expansion System can be configured to fail over to the Server Edition Primary, the Server Edition Secondary, or another Server Edition Expansion System.

Groups in a Multi-Site Network

In a multi-site network, the extension numbers of users are automatically shared between systems and become diallable from other systems without any further programming.

The following features are available for groups.

Advertised Groups:

Each group can be set as being 'advertised'. The group can then be dialed from other systems within the multi-site network. The groups extension number and name must be unique within the network. Non-advertised group numbers remain local only to system hosting the group.

Distributed Groups:

Groups on a system can include users located on other systems within the network. Distributed groups are automatically advertised to other systems within the network. Note that distributed groups can only be edited on the system on which they were created.

Related links

Group Types on page 886
Call Presentation on page 887
Group Member Availability on page 889
Example Hunt Group on page 891
CBC/CCC Agents and Hunt Groups on page 892
Coverage Groups on page 893

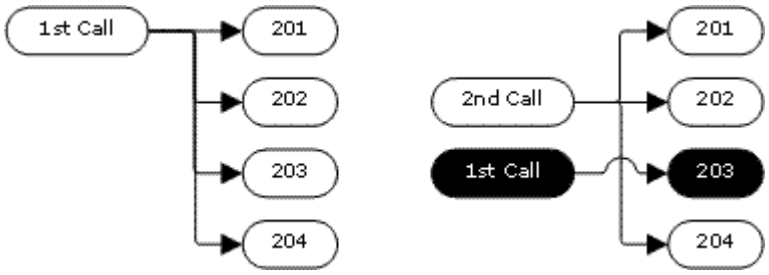
Group Types

At its most basic, a group's settings consist of a group name, an extension number, a list of group members and a hunt type selection. It is the last two settings which determine the order in which incoming calls are presented to hunt group members.

The available group types are; Collective, Sequential, Rotary and Longest Waiting. These work are follows:

Collective Group

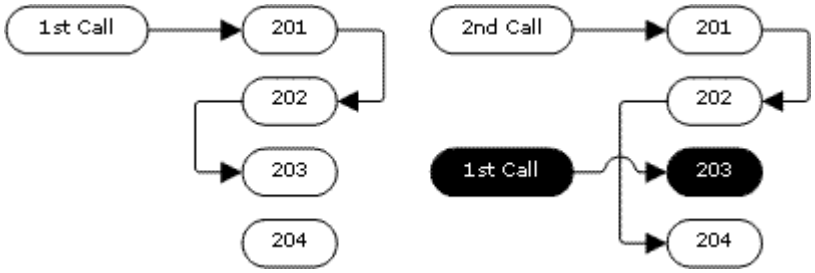
An incoming call is presented simultaneously to all the available group members.



Sequential Group

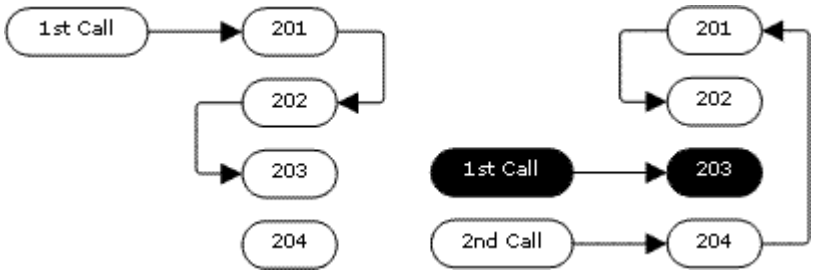
An incoming call is presented to the first available member in the list. If unanswered, it is presented to the next available member in the list.

The next incoming call uses the same order. It is presented to the available members starting again from the top of the list.



Rotary Hunt Type

This hunt type operates similarly to Sequential. However the starting point for call presentation is the first available member after the last member to answer a call.



Longest Waiting Hunt Type

Where hunt group calls are being presented to a twinned extension, the longest waiting status of the user can be reset by calls answered at either their master or twinned extension.

An incoming call is first presented to the available member who has been idle the longest. If unanswered it is presented to the next longest idle member.

This hunt type does not present calls to hunt group members in the order that they are listed. It presents calls using the order of how long the available hunt group members have been idle.

Related links

Group Operation on page 883

Call Presentation

Summary: Calls are presented to each available hunt group member in turn. If having been presented to all the available members, none answers, the call is redirected to voicemail if available, otherwise it continues to be presented to the next available member.

In addition to the summary, options exist to have calls queued or to have calls also presented to agents in an overflow group or groups.

- **First and Next Available Members**

  The first available member to which a call is presented and the order of the next available members to which a call is presented are determined by the hunt group's Hunt Type setting.

- **Additional Calls**

  When additional calls are waiting to be presented, additional available hunt group members are alerted using the hunt group type. When any member answers a call it will be the first waiting call that is answered.

- **No Available Members**

  If the number of incoming calls exceeds the number of available members to which calls can be presented, the following actions are usable in order of precedence.

- **Queuing**

  If queuing has been enabled for the hunt, it is applied to the excess calls up to the limits specified for the number of queued calls or length of time queued.

- **Voicemail**

  If voicemail has been enabled for the hunt group, excess calls are directed to voicemail.

- **Busy Tone**

  Busy tone is returned to the excess calls (except analog and T1 CAS calls which remain queued).

- **No Answer Time**

  This value is used to determine how long a call should ring at a hunt group member before being presented to the next available hunt group member. The **System | Telephony | Telephony | No Answer Time** setting is used unless a specific **Hunt | Hunt Group | No Answer Time** is set.

- **Voicemail**

  If voicemail is being used, if having been presented to all the available group members the call is still not answered then it goes to voicemail.

  - The call will also go to voicemail when the hunt group's **Voicemail Answer Time** is exceeded. the mailbox of the originally targeted hunt group is used even if the call has overflowed or gone to a night server hunt group.

- **Calls Not Being Answered Quick Enough - Overflow**

  In addition to ringing at each available member for the No Answer Time, a separate **Overflow Time** can be set. When a calls total ring time against the group exceeds this, the call can be redirected to an overflow group or groups.

- **No Available Member Answers**

  If a call has been presented unanswered to all the available members, either of two actions can be applied. If voicemail is available, the call is redirected to voicemail. If otherwise, the

call will continue being presented to hunt group members until answered or, if set, overflow is used.

- **Call Waiting**

  For hunt groups using the Group hunt type, call waiting can be used.

Related links

Group Operation on page 883

Group Member Availability

Summary: Details when a hunt group member is seen as being available to be presented a hunt group call.

The Hunt Group settings within Manager list those users who are members of the hunt group and therefore may receive calls directed to that hunt group. However there are a range of factors that can affect whether a particular hunt group member is available to take hunt group calls at any time.

- **Existing Connected Call**

  Users with an existing connected call are not available to further hunt group calls. This is regardless of the type of connected call, whether the user has available call appearance buttons or is using call waiting.

- **Hunt Group Call Waiting**

  For Collective hunt groups call waiting can be enabled using the **Ring Type** of **Collective Call Waiting**.

- **Logged In/Logged Out**

  The system allows user's to log in and out extensions, a process known as 'hot desking'. Whilst a user is logged out they are not available to receive hunt group calls.

  - Mobile Twinning users with both **Hunt group calls eligible for mobile twinning** and **Twin when logged out** selected will still receive hunt group calls unless they switch off twinning.

- **Membership Enabled/Disabled**

  The system provides controls to temporarily disable a users' membership of a hunt group. Whilst disabled, the user is not available to receive calls directed to that hunt group.

- **Do Not Disturb**

  This function is used by users to indicate that they do not want to receive any calls. This includes hunt group calls. In call center environments this state is also known as 'Busy Not Available'. See Do Not Disturb.

- **Busy on Held**

When a user has a held call, they can receive other calls including hunt group calls. The Busy on Held settings can be used to indicate that the user is not available to further calls when they have a held call.

- **Forward Unconditional**

  Users set to Forward Unconditional are by default not available to hunt group calls. The system allows the forwarding of hunt group calls to be selected as an option.

- **Idle /Off Hook**

  The hunt group member must be idle in order to receive hunt group call ringing.

- **No Available Members**

  If queuing has been enabled, calls will be queued. If queuing has not been enabled, calls will go to the overflow group if set, even if the overflow time is not set or is set to 0. If queuing is not enabled and no overflow is set, calls will go to voicemail. If voicemail is not available, external calls go to the incoming call routes fallback destination while internal calls receive busy indication.

Hunt Group Member Availability Settings	
Manager	Forwarding and do not disturb controls for a user are found on the User | Forwarding and User | DND tabs. Enabling and disabling a users hunt group membership is done by ticking or unticking the user entry in the hunt group's extensions list on the Hunt Group | Hunt Group tab.
Controls	The following short code features/button programming actions can be used:
SoftConsole	A SoftConsole user can view and edit a user's settings. Through the directory, select the required user. Their current status including DND, Logged In and hunt group membership states are shown and can be changed. Forwarding settings can be accessed by then selecting Forwarding.

Feature/Action	**Short Code**	**Default**	**Button**
Hunt Group Enable	✓	✗	✓HGEna - Toggles.
Hunt Group Disable	✓	✗	✓HGDis
Forward Hunt Group On	✓	✓-*50	✓FwDH+ - Toggles
Forward Hunt Group Off	✓	✓-*51	✓FwDH-
Busy on Held	✓	✗	✓BusyH
Do Not Disturb On	✓	✓-*08	✓DNDOn - Toggles
Do Not Disturb Off	✓	✓-*09	✓DNDOf
Extn Login	✓	✓-*35*N#	✓Login
Extn Logout	✓	✓-*36	✓Logof

Related links

Group Operation on page 883

Example Hunt Group

The follow are simple examples of how a department might use the facilities of a hunt group.

1. Basic Hunt Group

The Sales department want all sales related calls to be presented first to Jane, then Peter and finally Anne.

Actions	1. Create a hunt group named Sales and assign it an extension number. 2. Set the **Hunt Type** to **Sequential**. 3. Add Jane, Peter and Ann to the **User L** ist in that order. 4. Turn off queuing on the Queuing tab and voicemail on the Voicemail tab. 5. Route relevant calls to the Sales group by selecting it as the destination in the appropriate Incoming Call Routes.
Results	Any call received by the Sales hunt group is first presented to Jane if she is available. If Jane is not available or does not answer within 15 seconds the call is presented to Peter. If Peter is not available or does not answer within 15 seconds the call goes Anne. Since voicemail is not on, the call will continue to be presented around the group members in that order until it is answered or the callers hangs up.

2. Adding Voicemail Support

A voicemail server has now been added to the system. The Sales department wants to use it to take messages from unanswered callers. When messages are left, they want Jane to receive message waiting indication.

Actions	1. Open the Sales hunt group settings and select **Voicemail On** on the Voicemail tab. 2. Select the User settings for Jane. On the **Source Numbers** tab, add the entry **HSales**.
Results	Once a call to the Sales group has been presented to all the available members, if it is still unanswered then the call will be redirected to the group's voicemail mailbox to leave a message. When a message has been left, the message waiting indication lamp on Jane's phone is lit.

3. Using the Queuing Facility

The Sales department now wants calls queued when no one is available to answer. However if the number of queued calls exceeds 3 they then want any further callers directed to voicemail.

Actions	1. Open the Sales hunt group settings and select **Queuing On** on the **Queuing** tab. 2. Set the **Queue Limit** to **3**.
Results	When the Sales group are all on calls or ringing, any further calls to the group are queued and receive queuing announcements from the voicemail server. When the number of queued calls exceeds 3, any further calls are routed to the group's voicemail mailbox.

4. Using Out of Service Fallback

During team meetings, the Sales department want their calls redirected to another group, for this example Support.

Actions	1. Open the Sales hunt group settings and select the **Fallback** tab. In the **Out of Service Fallback Group** field select the **Support** group. 2. Create a system short code ***88/Set Hunt Group Out of Service/300**. 3. Create a system short code ***89/Clear Hunt Group Out of Service/300**.
Results	Prior to team meetings, dialing *88 puts the Sales group into out of service mode. Its calls are then redirected to the Support group. Following the meeting, dialing *89 puts the Sales group back In Service.

5. Using a Night Service Time Profile

Outside their normal business hours, the Sales department want their group calls automatically sent to voicemail. This can be done using a time profile and leaving the Night Service Fallback Group setting blank.

Actions	1. Create a Time Profile called **Sales Hours** and in it enter the times during which the Sales department are normally available. 2. Open the Sales hunt group settings and select the **Fallback** tab. 3. In the **Time Profile** field select **Sales Hours**.
Results	Outside the normal business hours set in the time profile, the Sales hunt group is automatically put into Night Service mode. Since no Night Service Fallback Group has been set, calls are redirected to voicemail.

Related links

Group Operation on page 883

CBC/CCC Agents and Hunt Groups

The use of and reporting on hunt groups is a key feature of call center operation. For IP Office, reporting is provided through the Compact Business Center (CBC) or Compact Contact Center (CCC) applications.

In order for these applications to provide hunt group and hunt group user (agent) reports, the following rules apply:

- The hunt group names must be restricted to a maximum of 12 characters.
- The hunt group and user extension numbers should be a maximum of 4 digits.
- Hunt group members should be given a Login Code and set to Force Login.
- The agent state Busy Not Available is equivalent to Do Not Disturb. The agent state Busy Wrap Up is equivalent to hunt group disable.

Related links

Group Operation on page 883

Coverage Groups

For users with a **Coverage Group** selected, coverage group operation is applied to all external calls that are targeted to the user.

For external calls:

In scenarios where an external call would normally have gone to voicemail, it instead continues ringing and also starts alerting the members of the coverage group.

- The follow me settings of Coverage Group members are used, the forwarding settings are not.
- If the user is not available, for example if they have logged off or set to do not disturb, coverage group operation is applied immediately.
- If the user is configured for call forward on busy, coverage operation is applied to the user's calls forwarded to the forward on busy destination.

Coverage group operation is not applied to the following types of call:

- Hunt group calls.
- Recall calls such as transfer return, hold recall, park recall, automatic callback.

The Coverage Group is set through the user's User | Telephony | Supervisor Settings or through their associated User Rights | Telephony | Supervisor Settings. The only group settings used are:

- The list of group members. They are treated as a collective group regardless of the group's configuration.
- If the group has **Night Server Fallback Group** and or **Out of Service Fallback Group** set, the members of those groups are used if the coverage group is set to night service mode or out of service mode respectively.

Related links

Group Operation on page 883

Chapter 90: Mobile Call Control

Mobile call control is only supported on digital trunks, including SIP trunks. It allows a user receiving a call on their twinned device to access system dial tone and then perform dialing action including making calls and activating short codes.

After answering a twinned call, the Mobile Call Control user can dial ** (within 1 second of each other) to place that call on hold and instead get dial tone from the system. Any dialing is now interpreted as if the user is logged into a basic single line extension on the system using their user settings. That also include user BLF status indication.

To use these features the user must be configured to support mobile call control.

⚠ Warning:

- This feature allows external callers to use features on your phone system and to make calls from the phone system for which you may be charged. The only security available to the system is to check whether the incoming caller ID matches a configured users' **Twinned Mobile Number** setting. The system cannot prevent use of these features by caller's who present a false caller ID that matching that of a user configured for access to this feature.

Trunk Restrictions

Mobile call control is only supported on systems with trunk types that can give information on whether the call is answered. Therefore, mobile call control is not supported on analog or T1 analog trunks. All other trunk types are supported (ISDN PRI and BRI, SIP (RFC2388), H323).

- Routing via trunks that do not support clearing supervision (disconnect detection) should not be used.
- DTMF detection is applied to twinned calls to a user configured for this feature. This will have the following effects:
- DTMF dialing is muted though short chirps may be heard at the start of any DTMF dialing.
- DTMF dialed by the user will not be passed through to other connected equipment such as IVR or Voicemail.

Mobile Call Control Features and FNE Services

Mobile call control uses a short code set to invoke an FNE service. The codes relevant to mobile call control are summarized below.

FNE	Description
31	**Mobile Call Control** This code allows a user called or calling the system to invoke mobile call control and to then handle and make calls as if they were at their system extension.
32	**Mobile Direct Access** Mobile direct access FNE32 immediately redials on switch the DDI digits received with the call rather than returning dial tone and waiting for DTMF digits as with FNE31 .
33	**Mobile Callback** Mobile callback allows the user to call the system and then hang up. The system will then make a call to the user's CLI and when answered, provide them with dial tone from the system to make calls.
35	**Simplified Mobile Call Control** In addition to the Mobile Call Control feature that enables your mobile to make and handle calls as if your are using your extension, this Simplified Mobile Call Control FNE 35 clears the dial tone when the call recipient ends the call. The dial tone is provided on the mobile phone for fresh calls after the current call is cleared.
36	**Simplified Mobile Direct Access** In addition to the Mobile Direct Access feature, the Simplified Mobile Direct Access FNE36 clears the dial tone when the call recipient ends the call.
37	**Simplified Mobile Callback** In addition to the Mobile Callback feature that enables your mobile to get call back from the system and lets you use the dial tone for making and handling calls, this Simplified Mobile Callback FNE 37 clears the dial tone when the call recipient ends the call. The dial tone is provided on the mobile phone for fresh calls after the current call is cleared.

The codes relevant to mobility are summarized in the table.

FNE Number	Feature
00	System Dial Tone
01	Steal Call
02	Auto Call Back
04	Forward All Calls
05	Forward Busy and No Answer Calls
06	Call Forward Disable
07	Park Call
08	Call UnPark
09	Pick Up Group
10	Directed Call Pick Up
12	Withheld CLI (To External Calls off IPO)
13	Enable CLI (To External Calls off IPO)

Table continues…

FNE Number	Feature
14	Conference Add
15	Drop Call
16	Private Call (cannot be intruded or recorded)
17	Held Appearance Select
18	Same as FNE 00–Dial Tone Appearance (a=)
19	Enable Twinning
20	Disable Twinning
24	DND On
25	DND Off
26	Blind Transfer
27	Transfer to Voicemail

Using Mobile Call Control

In addition to using ** to access mobile call control, the user has access to the following additional controls:

- **Clearing a Call: *52** It may be necessary to clear a connected call, for example after attempting a transfer and hearing voicemail or ringing instead. To do this dial **** for dial tone and then ***52** (this is a default system short code and can be changed if required).
- **Return to Dial Tone: ##** Return to dial tone after getting busy, number unobtainable or short code confirmation tones from the system.

Enabling Outgoing Mobile Call Control

1. **Configure the user for Mobile Twinning and Mobile Call Control** On the User | Mobility tab do the following:

- Enable **Mobility Features** for the user.
- Set the **Twinned Mobile Number** for the user's twinned calls destination.

1. Digits are matched from right to left.
2. The match must be at least 6 digits. If either the CLI or the Mobile Twinned Number is less than 6 digits no match will occur.
3. Matching is done for up to 10 digits. Further digits are ignored. If either the CLI or Mobile Twinned Number is less than 10 digits, matching stops at that shorter length.
4. If multiple matches occur the first user in the configuration is used. Manager will warn against configuration where such a conflict may exist.

- Select **Can do Mobile Call Control**.

On systems with some unsupported trunk types, further changes such as Outgoing Group ID, system shorts codes and ARS may be necessary to ensure that calls to the mobile twinned numbers are only routed via trunks that support mobile call control.

Incoming Mobile Call Control

The system can be configured to allow Mobile Call Control users to use this function when making an incoming call to the system. This requires the user to make the incoming call from the same CLI as their Mobile Twinning Number (even if they do not actually use Mobile Twinning).

The call will be rejected:

- If the caller ID is blank or withheld.
- If the caller ID does not match a Twinned Mobile Number of a user with **Can do Mobile Call Control** enabled.
- If the call is received on a trunk type that does not support Mobile Call Control.

Enabling Incoming Mobile Call Control

On the **User | Mobility** tab do the following:

1. Enable **Mobility Features** for the user.
2. Set the **Twinned Mobile Number** to match the CLI of the device from which the user will be making calls.
3. Select **Can do Mobile Call Control**.

Add a FNE Short Code In the system short codes section of the configuration add a short code similar to the following. Key points are the use of the **FNE Service** feature and the **Telephone Number** value **31**.

- **Short Code**: *89
- **Feature**: FNE Service
- **Telephone Number**: 31

Add an Incoming Call Route for the user Create an incoming call route that matches the user's CLI and with the FNE short code created above as its destination.

On systems with some unsupported trunk types, further changes such as Incoming Group ID changes may be necessary to ensure that only calls received on trunks that support Mobile Call Control are routed to this short code.

Related links

Mobile Direct Access (MDA) on page 897
Mobile Callback on page 899

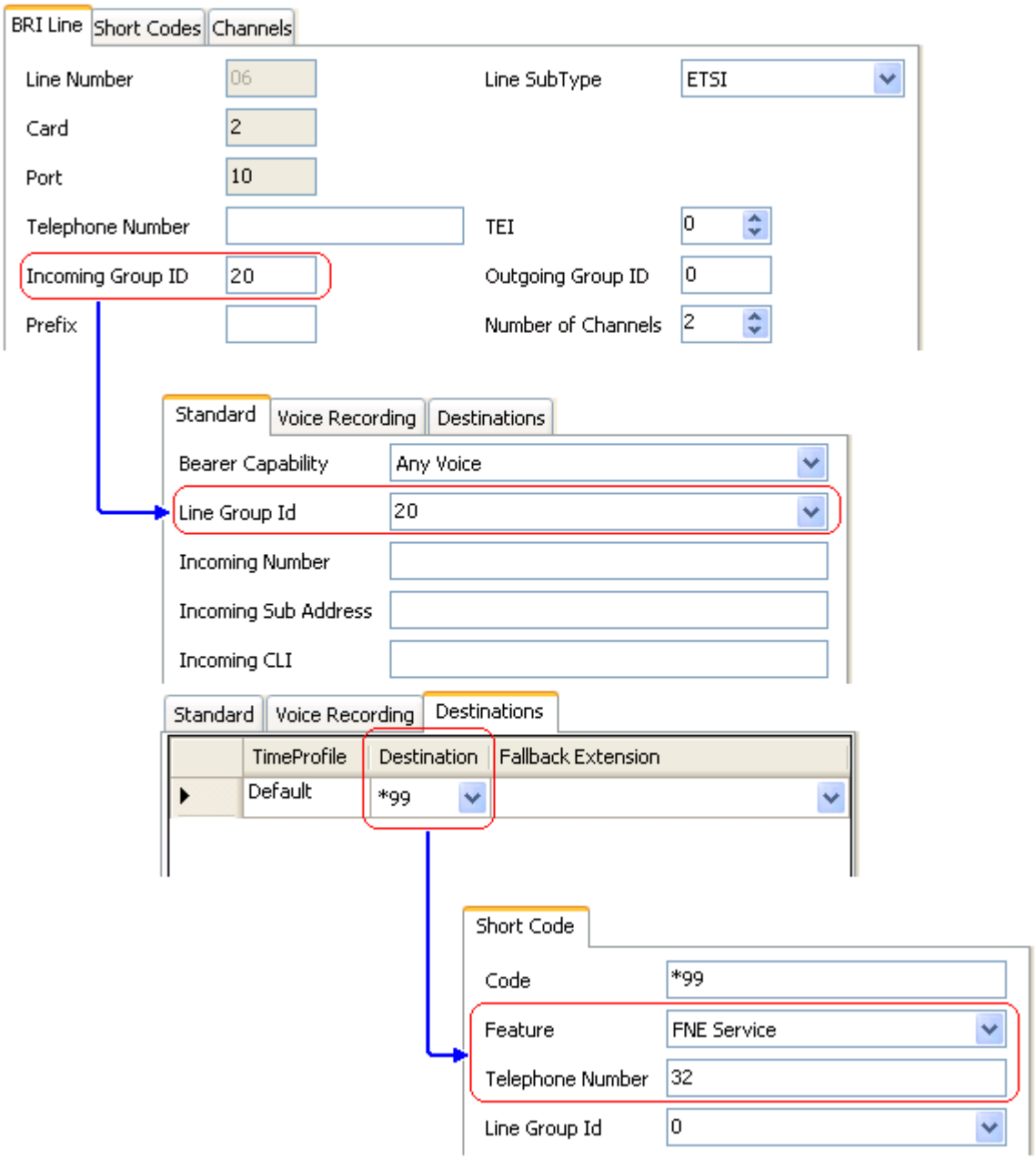
Mobile Direct Access (MDA)

For a Mobile Call Control or one-X Mobile client user, FNE32 immediately redials on switch the DDI digits received with the call rather than returning dial tone and waiting for DTMF digits as with FNE31. This is called Mobile Direct Access (MDA).

MDA requires the user's external telephony provider to provide a direct trunk with DDI to the system (ie. an ISDN or SIP trunk). By assigning a specific incoming line group ID to the trunk, an

incoming call route can be created for the same line group ID with blanks incoming number and incoming CLI fields. The destination is a short code set to FNE32.

User validation is performed using the CLI in the same way as for normal Mobile Call Control. In addition the call will be rejected no DDI digits are provided. Once connected the user can use the other Mobile Call Control features such as **.



Related links

Mobile Call Control on page 894

Mobile Callback

Mobile callback allows the user to call the system and then hang up. The system will then make a call to the user's CLI and when answered, provide them with dial tone from the system to make calls.

Mobile callback is subject to all the normal trunk type and user licensing restrictions of mobile call control. In addition the user must have the **Mobile Callback** (**User | Mobility**)setting enabled in the system configuration.

When the user makes a call using a DDI that is routed to an FNE33 short code, the system will not connect (answer) the call but will provide ringing while it waits for the user to hang up (after 30 seconds the system will disconnect the call).

- The system will reject the call if the CLI does not match a user configured for Mobile Callback or does not meet any of the other requirements for mobile call control.
- The system will reject calls using FNE33 if the user already has a mobile twinning or mobile call control call connected or in the process of being connected. This includes a mobile callback call in the process of being made from the system to the user.

If the CLI matches a user configured for mobile callback and they hang up within the 30 seconds, the system will within 5 seconds initiate a callback to that user's CLI.

- If the call is answered after the user's **Mobile Answer Guard** time and within the user's **No Answer Time**, the user will hear dial tone from the system and can begin dialling as if at their system extension.
- If the call is not answered within the conditions above it is cleared and is not reattempted.

Related links

Mobile Call Control on page 894

Chapter 91: Transferring calls

The IP Office system supports a range of methods for transferring calls.

Related links

Transferring call notes on page 900
Transferring call notes on page 901
Off-Switch Transfer Restrictions on page 902
Context Sensitive Transfer on page 903
Dial Tone Transfer on page 904
Handsfree Announced Transfers on page 906
One Touch Transferring on page 908
Centrex Transfer on page 909

Transferring call notes

The following are some of the methods usable to transfer calls.

Note	Description
Supervised Transfer	This is a transfer where the user waits for the transfer destination to answer and talks to that party before completing the transfer, this is referred to as a consultation call. They then either complete the transfer or drop the call and return to the held for transfer call. The call details, display, ringing and forwarding applied are appropriate to the type of call (internal or external) being transferred.
Unsupervised Transfer	This is a transfer that is completed whilst the destination is still ringing. This is also called a 'blind transfer'.
Automatic Transfer - Forwarding	The system allows users to automatically transfer calls using forwarding options. For full details, see DND, Follow Me and Forwarding on page 862.
Transferring to a Forwarded Extension	When transferring a call to another extension that has forwarding enabled, the type of call being transferred is used. For example, if transferring an internal call, if the transfer target has forwarding of internal calls enabled, then the forward is used.

Table continues…

Note	Description
Transferring Calls to Yourself	User's can transfer calls to their own extension number. This is useful for users with multiple devices registered to the same extension number or users with twinned devices. It allows the user to transfer a call answered on one device and then answer it on another one of their devices.
Reclaim	If a transferred call is still ringing unanswered, it may be possible to reclaim the call. The default shortcode for this is *46.
Transfer Return Time	Sets the delay after which any call transferred by the user, which remains unanswered, should return to the user. A return call will continue ringing and does not follow any forwards or go to voicemail. • Transfer return only occurs if the user has an available call appearance button. • Transfer return is not applied if the transfer is to a hunt group that has queuing enabled.

Related links

Transferring calls on page 900

Transferring call notes

The following are the basic methods for transferring calls.

Analog and single line phones

Action	Steps
Unsupervised Transfer	1. Press R. Note that broken dial tone is heard while a call is on hold. 2. Dial the transfer destination number. 3. Hang-up.
Supervised Transfer	1. Press R. 2. Dial the transfer destination number. 3. If the destination answers and accepts the call, hang-up. 4. If the called party does not answer or does not want to accept the call, press Ragain. 5. To return to the original caller press R.
Reclaim	*46

Avaya multiple line phones

Action	Steps
Unsupervised Transfer	1. Press **Transfer**. 2. Dial the transfer destination number. 3. Press **Transfer** again to complete the transfer.
Supervised Transfer	1. Press **Transfer**. 2. Dial the transfer destination number. 3. If the destination answers and accepts the call, press **Transfer** again to complete the transfer. 4. If the called party does not answer or does not want to accept the call, press **Drop**. 5. To return to the original caller press it's call appearance button.
Reclaim	*46

Related links

Transferring calls on page 900

Off-Switch Transfer Restrictions

Users cannot transfer calls to a destination that they cannot normally dial. This applies to manual transfers and also to automatic transfers (forwarding). In addition to call barring applied through short codes, the following system settings may restrict a users ability to transfer calls.

User Specific Controls

Setting	Description
Outgoing Call Bar	Default = Off (**Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Supervisor Settings**) When enabled, this setting stops a user from making any external calls. It therefore stops them making any external transfers or forwards.
Inhibit Off-Switch Forward/Transfer	Default = Off (**Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Supervisor Settings**). When enabled, this setting stops the specific user from transferring or forwarding calls externally. This does not stop another user transferring the restricted users calls off-switch on their behalf. • User attempts to set an external forward destination using a short code hear error tone. • User attempts to set an external forward destination using a programmable button on their phone do not allow the number to be saved.

Line Specific Control

Setting	Description
Analog Trunk to Trunk Connection	Default = Off (**System Settings** > **Line** > **Add/Edit Trunk Line** > **Analog Line** > **Analog Options**) When not enabled, users cannot transfer or forward calls on one analog trunk back off-switch using another analog trunk.

•

System Wide Controls

Setting	Description
Inhibit Off-Switch Forward/Transfer	Default = On(**System Settings** > **System** > **Telephony**) When enabled, this setting stops any user from transferring or forwarding calls externally. • User attempts to set an external forward destination using a short code hear error tone. • User attempts to set an external forward destination using a programmable button on their phone do not allow the number to be saved.
Restrict Network Interconnect	Default = Off (**System Settings** > **System** > **Telephony**). When this option is enabled, each trunk is provided with a Network Type option that can be configured as either **Public** or **Private**. The system will not allow calls on a **Public** trunk to be connected to a **Private** trunk and vice versa, returning busy indication instead.

Conference Control

Users can use conference controls to effectively transfer calls. This includes transferring an external call to another external number. The use of conferencing to effect off-switch transfers can be restricted using the **Inhibit External Only Impromptu Conference** setting (**System Settings** > **System** > **Telephony**).

Related links

Transferring calls on page 900

Context Sensitive Transfer

Calls and Button Status Indication The status indication for a call on hold pending transfer has changed to differentiate such calls from standard held calls:

- On phones with both dual lamp buttons, both the green and red lamps fast flash (flutter) when the button represents a call on hold pending transfer.
- On phones with single lamp buttons or status icons, **Xfer**: is now shown in front of the caller ID information rather than the button name. For example **Xfer:Extn299** is shown rather than **a = Extn299**.

- The call status information shown when the button of a call on hold pending transfer is the currently highlight line is now prefixed with **On-Hold-Xfer** rather than **On-Hold**.

Switching Between Calls Switching from a connected call to an existing call on hold pending transfer puts the connected call on hold pending transfer. The following table is an example of the resulting operation .

Call or answer A	Connected to A
Press `Transfer`	A on hold pending transfer
Call or answer B	A on hold pending transfer. Connected to B.
Reconnect to A	Connected to A. B on hold pending transfer
Press `Transfer`or **Complete***.	A transferred to B.

Requirement for a Free Call Appearance Before Starting a Transfer When the user already has a call or calls on hold, they can now put their current call on hold pending transfer even if there are no free call appearances available. Previously an available call appearance was required in order to then make a consultation call to the potential transfer destination.

Conferencing Calls For these phone there have also been changes to which calls are conferenced in different scenarios including when there is a call on hold pending transfer. See Context Sensitive Conferencing.

Related links

Transferring calls on page 900

Dial Tone Transfer

A user who is not able to make external calls to any or some external numbers, can be transferred to dial tone by a user who is able to make external calls.

- The restricted user wanting to make the external call, dials the unrestricted user and requests dial tone.
- The unrestricted user initiates a transfer and dials the prefix for an ARS form configured to provide secondary dial tone.

The prefix is a short code set up to access the required ARS form. While this can be a system short code, using a user or user rights short code will allow control over who can provide dial tone transfer for restricted users.

- When they hear the secondary dial tone, the unrestricted user completes the transfer.
- The restricted user now hears the secondary dial tone and is now able to make an external call.
- The restricted user is now able to make calls as permitted by the short codes in the ARS form.

- The restricted user is not able to transfer the dial tone to another user.

The ARS form being used can still contain short codes that restrict the dialing that can be attempted after the restricted user hears secondary dial tone. Other ARS features can also be used such as alternate routing or time profiles to provide out of hours routing. The ARS form timers are run from when the unrestricted caller dials the ARS form. They are not reset when the restricted user is transferred to the ARS form.

Multiple prefixes and ARS forms can be used if required to create more complex scenarios. For example, one where the unrestricted user can transfer the restricted users to an ARS forms that allows international calls or to an ARS form that only allows national dialing.

Example Configuration:

The example below is a simple configuration that allows the unrestricted user to use 8 as a transfer destination that provides secondary dial tone.

Create an ARS Form for Secondary Dial Tone The ARS form needs to be created before short codes can be added to route callers to it.

- Enter a **Route Name** to identify the ARS form, for example `Dial Tone Trans`.
- Select **Secondary Dial Tone**.
- Select either **System Tone** (this matches locale specific normal dial tone) or **Network Tone** (this matches locale specific secondary dial tone). For some locales both tones are the same.
- Enter short codes that will take any digits dialed by the restricted user and process them for external dialing to an outgoing line group. For this example we will allow any digits dialed to be presented to the first trunk seized in outgoing line group 0.

Code	N
Telephone Number	N
Feature	Dial
Line Group ID	0

- Other short codes can be used to allow or bar the dialing of specific numbers or types of numbers.
- Configure the rest of the ARS form as required. For full details on ARS form configuration see ARS.

Create a Short Code for Dial Tone Transfer For this example we will allow the prefix 8 to be used to access an ARS form created above.

In the user short codes of the unrestricted user, create a short code that invokes the ARS form created above. For example:

Code	8
Telephone Number	

Table continues…

Feature	Dial
Line Group ID	51 Dial Tone Trans

- It is important that the short code does not pass any digits to the ARS form. Once the ARS form receives any digits, it starts short code matching and ends secondary dial tone.
- The short code could also be setup as a system or user rights short code.

The unrestricted user is now able to provide secondary dial tone to other users by on request by pressing **Transfer**, dialing **8** and then pressing **Transfer** again.

Account and Authorization Codes:

If the restricted user enters an account or authorization code while calling the unrestricted user to request dial tone, that value is not carried forward with their external call once they have been provided with secondary dial tone.

If the unrestricted user enters an account or authorization code while dialing the ARS form, that value remains associated with the call made by the restricted user.

If the ARS form short code used to route the restricted users call requires an account or authorization code, the value already entered is used, otherwise the restricted user is prompted to enter a value.

Call Logging:

The restricted user's outgoing call log will include the call to the unrestricted user and the outgoing external call they subsequently make. The outgoing external call record will include the prefix dialed by the unrestricted user to access the ARS form.

The unrestricted users call log will include just an incoming call from the restricted user.

Within the SMDR output, the calls by the restricted user are included. The call by the unrestricted user is not included.

Related links

Transferring calls on page 900

Handsfree Announced Transfers

This feature allows the enquiry call part of a supervised transfer to be answered handsfree. In addition the system can be optionally configured to allow both the enquiry call and completed transfer call to be auto-answered.

Example:

1. User 201 answers a call that they then want to transfer to user 203.
2. They press **Transfer** to put the call on hold pending transfer.
3. They then press a **Dial Direct** button and dial 203.

4. The transfer enquiry call is auto answered by User 203's phone. User 201 is able to announce the pending transfer and hear if User 203 wants to accept the call.

The auto-answer only occurs if the target user's extension is idle. If the target is already connected to a call, the transfer enquiry will be presented as normal call.

If the transfer is accepted, User 201 can press **TRANSFER** again to complete the transfer process.

The transferred call will then ring at the target. However, if required the system can be configured to also auto-answer the completed transfer.

Configuration:

Handsfree announced transfers are supported when using one of the following features after having pressed **TRANSFER**.

Button Features	**Short Code Features**
Dial Direct Automatic Intercom Dial Intercom	Dial Direct

User Button Usability:

Following the use of any of the buttons above, if the button has not been programmed with a specific target, a User button can be used to indicate the target for the enquiry call. This gives the advantage of being able to see the target user's status before attempting the transfer.

- For **Automatic Intercom** and **Dial Intercom** buttons without a pre-specified target, the **User** button must be on a button module.
- For **Dial Direct** buttons without a pre-specified target, the **User** button can be on the phone or button module. Due to this and the support for **Dial Direct** across a network of systems, we recommend that a **Dial Direct** button is used for handsfree announced transfers.

Phone Support:

Handsfree announced transfer is supported for calls being transferred to the following phones:

Full Support	Partial Support	Not Supported
The following system phones support full announced transfer operation. **1603, 1608, 1616, 2410, 2420, 5410, 5420, 4610, 4621, 4625, 5610, 5620, 5621.** **Analog Off-Hook Stations** (See notes below).	The following phone can auto-answer announced transfers but require the user to use the handset to respond. **2402, 4601, 4602, 5402, 5601, 5602**.	Announced transfer is not supported for any phones not listed in the other column. On unsupported phones the transfer eqnuiry consultation call will be presented as a normal call.

Notes:

- On supported phones, if the target user's phone is not idle when the enquiry call attempt is made, the enquiry call is turned into a normal transfer attempt, eg. alerting on an available call appearance.
- Enabling the extension specific setting **Disable Speakerphone** will turn all auto-answer calls, including handsfree announced transfers to the extension, into normal calls.
- **Off-Hook Station Analog Phones** Analog phone extensions configured as Off-Hook Station can auto-answer transfers when off-hook and idle.
- **Headset Users** The following applies to users on supported phones with a dedicated **HEADSET** button. These users, when in headset mode and idle will auto-answer the announced transfer enquiry call through the headset after hearing 3 beeps. The transfer completion will require them to press the appropriate call appearance unless they are set to Headset Force Feed.
- **Twinning** Handsfree announced transfer calls to users with twinning enabled will be turned into normal calls.
- **Multi-site network Support** Dial Direct is supported to targets across a multi-site network, therefore allowing handsfree announced transfers to remote users.

Full Handsfree Transfer Operation:

If required the system can be configured to allow the full handsfree announced transfer process, ie. both the enquiry call and the transfer, to be auto-answered on supported phones. This is done by entering `FORCE_HANDSFREE_TRANSFER` into the Source Numbers of the NoUser user and rebooting the system

Related links

Transferring calls on page 900

One Touch Transferring

This feature allows selected users to transfer calls to each other using a reduced number of key presses.

With this option, a call can be transferred by simply selecting the transfer destination and then hanging up (or pressing **Transfer** if working handsfree).

Without this option the normal sequence is to press **Transfer**, dial the destination and then hanging up (or pressing **Transfer** if working handsfree).

For one touch transfer the transfer destination number must be selected using a button programmed to one of the following features:

- **User**
- **Dial**

- **Abbreviated Dial**
- **Automatic Intercom**
- **Dial Intercom**
- **Dial Direct**

This feature is enabled on a per user basis by adding `Enable_OTT` to the **Source Number** settings of the user. This feature is supported on all Avaya phones that support the programmable button features.

Related links

Transferring calls on page 900

Centrex Transfer

Centrex Transfer is a feature provided by some line providers on external analog lines. It allows the recipient of a calls on such a line to transfer that call to another external number. The transfer is performed by the line provider and the line is freed. Without Centrex Transfer, transferring an external call to another external number would occupy both a incoming and outgoing line for the duration of the call.

The following are the supported controls and usages for Centrex Transfer:

- **Centrex Transfer Button Operation** The action **Flash Hook** can be assigned to a programmable button. This button can be configured with or without a telephone number for an automatic or manual transfer.
  - **Manual Transfer** If the programmable button is setup without a target telephone number, pressing the button returns dial tone to the user. They can then dial the required transfer number and when they hear ringing or an answer, hang up to complete the Centrex Transfer.
  - **Automatic Transfer** If the programmable button is setup with a target telephone number, pressing the button performs the Centrex Transfer to the number as a single action.
- **Centrex Transfer Short Code Operation** The **Flash Hook** short code feature can be used with system short codes. It can be setup with or without a telephone number in the same way as a Flash Hook programmable button above. The line group must be the group of analog lines from the Centrex service line provider.
  - **Centrex Transfer Operation for Analog Extensions** Most analog phones have a button that performs the action of sending a hook flash signal. The marking of the button will vary and for example may be any of **R**, **H**, **Recall** or **Hold**. Pressing this button sends a hook flash to the system to hold any current call and return dial tone.
    - To perform a Centrex Transfer, pressing the analog extension's hook flash button should be followed by the dialing of a **Flash Hook** short code.
    - For analog extension users with call waiting enabled, pressing the hook flash button during a call will hold the current call and connect any call waiting. Therefore it is

recommend that analog extension users wanting to use Centrex Transfer should not also have call waiting enabled.

- **Auto Attendant Transfer** System's using embedded voicemail can select Centrex Transfer as an action. For system using Voicemail Pro, the equivalent can be achieved by transferring calls to a **Flash Hook** short code.

Additional Notes

- **Networked Systems** In networked systems, Centrex Transfer is only supported using **Flash Hook** or **Centrex Transfer** features on the system which hosts the Centrex analog trunks.
- **Addition Prefix Dialing** In some cases the Centrex service provider may require a prefix for the transfer number. If that is the case, that prefix must be inserted in the button programming or the short code used for the Centrex Transfer.
- **Application Transfers** Centrex Transfer is not supported for calls being held and transferred through applications such as SoftConsole.
- **Conference Calls** Centrex Transfer is not supported with conference calls.

Related links

Transferring calls on page 900

Chapter 92: Simultaneous mode

IP Office systems support 'simultaneous' mode operation. In that mode, users can be associated with multiple telephony devices at the same time. They can answer and make calls on any of those devices.

Related links

Simultaneous Mode Devices on page 911
Simultaneous Mode Notes on page 911
Moving Calls Between Simultaneous Devices on page 912

Simultaneous Mode Devices

An IP Office user can be logged in simultaneously on one of each of the following types of telephone devices:

Telephony Client	Notes
A physical desk phone	A physical phone, including a SIP, H.323 or DECT extension. This also includes clients running on a Vantage phone.
A desktop (PC) VoIP client:	• Avaya Workplace Client for Windows • Avaya Workplace Client for macOS
A mobile VoIP client:	• Avaya Workplace Client for Android • Avaya Workplace Client for iOS
A WebRTC client:	• Spaces Calling using the Chrome extension.

Related links

Simultaneous mode on page 911

Simultaneous Mode Notes

The following notes relate to the operation of simultaneous telephony:

- Incoming calls to the user alert on all their devices and they can choose which device they want to use to answer.

- Whilst the user has a call in progress on one of the devices, any additional incoming call is presented only to that device.
- It is recommended not to mix simultaneous mode operation with features such as such as mobile twinning, telecommuting and mobile call controls that can lead to multiple duplicate calls. For example, a mobile client's external PSTN numbers as a active mobile twinning destination will cause duplicate alerts for the same call.
- Users can have their desk phone and their softphone applications registered to different servers in an IP Office network.
- Use of simultaneous mode is not supported when also using a non-telephony CTI client to control call handling. In that scenario it is not always possible to predict which telephony client will be used when making/answering a call from the CTI client which can lead to confusion.

Related links

Simultaneous mode on page 911

Moving Calls Between Simultaneous Devices

The IP Office system supports a number of features to enable users to move calls between their simultaneous devices.

Action	Description
Transfer	Users can transfer calls to their own extension number. That causes the call to alert on their other simultaneous devices.
Steal	For IP Office R11.1.2.4 and higher, a **Call Steal** shortcode set to with the user's extension number will retrieve a current call from their other simultaneous device.
Workplace Clients	For IP Office R11.1.3 and higher, Avaya Workplace Client users can use their client to move and retrieve calls: • Using move, the user can send a call from their Avaya Workplace Client to their other simultaneous devices. • Using retrieve, the user can move a call answered on their simultaneous device to their Avaya Workplace Client. These features are enabled by a `SET IPO_CALL_HANDOVER_ENABLED 1` line in the `46xxsettings.txt` file.

Related links

Simultaneous mode on page 911

Chapter 93: User Source Numbers

Source numbers are used to configure features which do not have specific controls within the IP Office Manager or IP Office Web Manager interfaces.

Sources numbers are divided into two types:

- User source numbers are used to apply settings to individual users.
- NoUser source numbers are used to apply settings to the IP Office system or to all users on the system.

Note that the lists shown on the following pages are not exhaustive.

- Some source numbers are made obsolete when replaced by proper configuration controls in a later release of IP Office software. At that stage, the source number is no longer supported.
- This document covers the source numbers that are publicly supported. Other source numbers issued for particular customer sites to resolve specific issues at those sites are not included and are not supported on other IP Office systems.

Related links

Individual User Source Numbers on page 913
NoUser Source Numbers on page 915

Individual User Source Numbers

User Source Numbers

The following source numbers affect the particular user to which they are applied. They are mergeable unless stated otherwise.

- **AT<string>**

  Strings beginning with AT are used with a user called **DTEDefault** to configure the default settings of the control unit's DTE port.

- **BST_MESSAGE_FOR_YOU**

  Replace the date and time shown on BST phones when idle with `Message for you` or `Messages for you` when the user has new voicemail messages. This source number can be used as a `NoUser` source number to enable the feature for all BST phone users.

- **BST_NO_MESSAGE_FOR_YOU**

If the source number **BST_MESSAGE_FOR_YOU** has been used as a `NoUser` source number to enable the feature for all BST phone users, this individual user source number can be used to disable the feature for selected users.

- **C***<Conference ID>*

  Provides the user with message waiting indication and access to the conference mailbox of a system meet-me conference. Access is through Visual Voice and the User Portal application.

- **Enable_OTT**

  Enable one touch transfer operation for the user. See One Touch Transferring on page 908. This source number can be used as a `NoUser` source number to enable the feature for all users.

- **H***<Group Name>*

  Allows the user to receive message waiting indication of new group messages. The group is added to the user's Visual Voice menu. On suitable display extensions, the hunt group name and number of new messages is displayed. Refer to the appropriate telephone user guide.

  - If the user is not a member of the group, a voicemail code must be set for the group's mailbox (**Group | Voicemail | Voicemail Code**).

- **P***<Telephone Number>*

  This record sets the destination for callback (outbound alert) calls from voicemail. Enter `P` followed by the telephone number including any necessary external dialing prefix, for example `P917325559876`. This facility is only available when using Voicemail Pro on which a default or user specific **Callback** start point has been added. Refer to the Administering IP Office Voicemail Pro manual. This feature is separate from voicemail ringback andVoicemail Pro outcalling.

- **R***<Caller ICLID>*

  To allow Dial In/RAS call access only from a specified number prefix the number with a `R`. For example `R7325551234`.

- **U***<User Name or Extension Number>*

  Allows the user to receive message waiting indication of new messages. The specified user is added to the user's Visual Voice menu. On suitable display extensions, the user name and number of new messages is displayed. Refer to the appropriate telephone user guide.

  - If the user is not a trusted source for the mailbox, they will need to enter its **Voicemail Code** to access the mailbox.

- **V***<Caller ICLID>*

  Strings prefixed with a `V` indicate numbers from which access to the users mailbox is allowed without requiring entry of the mailbox's voicemail code. This is referred to as "trusted source".

  - For Voicemail Pro running in Intuity mode, trusted source is used for calls from programmable buttons set to **Voicemail Collect** and **Visual Voice**. Other controls are prompted for the mailbox number and then password.

Related links

User Source Numbers on page 913

NoUser Source Numbers

The following source numbers affect all users on the IP Office system. They are entered through the **Source Numbers** tab of the **NoUser** user. These source numbers are informally referred to as *NUSNs*.

Important:

- Adding and changing these source numbers require a system reboot to become effective.

NoUser Source Numbers

- `ATM4U_PCS7_RINGDETECT`

  For some cellular or mobile interfaces connected to a IP500 ATM4U card, the card may not detect the ring signal. For PCS4 and higher card, this `NoUser` source number can be used activate alternate ring detection.

- `ALLOW_5410_UPGRADES`

  This option must be present for 5410 phones to update their firmware.

- `B_DISABLE_SIP_IPADDR`

  Disables blacklisting of SIP device registration based on the device IP address. Refer to the Avaya IP Office™ Platform Security Guidelines manual.

- `BST_MESSAGE_FOR_YOU`

  Replace the date and time shown on BST phones when idle with `Message for you` or `Messages for you` when the user has new voicemail messages. This source number can also be set as a source number for individual users.

- `CIPHERS_LEVEL_H323=`*<N>*

  Sets the minimum cipher strength the IP Office accepts on TLS connections for H.323 phones and trunks. Not used for clients where ciphers are enabled and chosen based on those offered by the TLS server.

  - Supported for IP Office R11.1.2.x releases. For IP Office R11.3.1 and higher, this NUSN is replaced by the **System** > **Certificates** > **H.323 Security Level** security setting.
  - Note: The default level 1 (medium strength) is used if no source number is specified.

  The value <*N*> is set as follows:

  - **Low** (`0`) - Accept low, medium, and high-strength ciphers. Low and medium on IP500 V2 systems.
  - **Medium** (`1`) - Accept medium and high-strength ciphers. Medium on IP500 V2 systems.
  - **High** (`2`) - Accept high-strength ciphers. Not supported for IP500 V2 systems.
    - For a list of ciphers, see https://documentation.avaya.com/bundle/IPOfficeSecurity/page/Supported_Ciphers.html.
    - High-strength ciphers are GCM ciphers. These are not supported by any model of IP500 V2 system.

- CIPHERS_LEVELS_SIP=<*N*>

  Sets the minimum cipher strength the IP Office accepts on TLS connections for SIP phones and trunks. Not used for clients where ciphers are enabled and chosen based on those offered by the TLS server.

  - Supported for IP Office R11.1.2.x releases. For IP Office R11.3.1 and higher, this NUSN is replaced by the **System** > **Certificates** > **SIP Security Level** security setting.
  - Use the same values as CIPHERS_LEVEL_H323= but sets the cipher level the IP Office accepts for SIP TLS connections.

- DECT_REVERSE_RING

  By default, when this parameter is not set, calls on DECT phones associated with a CTI application will ring as a priority call. When this parameter is set, DECT phones ring as a normal, external or internal call.

- DISTINCT_HOLD_RINGBACK

  Used to display a specific message about the call type for calls returning after timing out from being parked or held. If set, such calls display **Return Call - Held** or **Return Call – Parked** rather than connected party name or line name.

- ENABLE_J100_FQDN

  Use FQDN rather than IP addresses in the server address values provided to J100 Series phones. This requires that the FQDN values are correctly routable by the customer DNS servers and that the phones use the DNS server address (either obtained through DHCP or set manually).

- ENABLE_J100_AUTO_UPDATE_POLICY

  Add settings for J100 Series phone auto-upgrade support to the system's auto-generated 46xxsettings.txt file. Refer to the IP Office SIP Telephone Installation Notes manual.

- Enable_OTT

  Enable one touch transfer for all users. See One Touch Transferring on page 908. This source number can also be set as a source number for individual users.

- EQNX_CONTACT_MATCHING_MIN_DIGITS=<*N*>

  By default the Avaya Workplace Client requires at least 10 digits for contact matching (8 for Bahrain). This NoUser source number can be used to define the minimum digits for contact matching for countries where national dial plan phone numbers are less than 10 digits.

- FORCE_HANDSFREE_TRANSFER

  If set, when using the handsfree announced transfer process (see Handsfree Announced Transfers on page 906), both the transfer enquiry and transfer completion calls are auto-answered. Without this setting only the transfer enquiry call is auto-answered.

- FORCE_SIP_SBC_TCP_SINGLE_PORT

  Force the IP Office to open only one socket to the ASBCE for each client, regardless of the number of calls. Doing this has can resolve issues with calls giving one ring on client and then appearing as a missed call.

- HIDE_CALL_STATE

Used to hide the call status information, for example `Dial` and `Conn`, shown on older DS phones such as 2400, 4400 and 5400 Series. Used in conjunction with the `LONGER_NAMES` source number.

- `HOLD_MUSIC_TIMEOUT=`*<seconds>*

  By default, line alternate music sources remain connected for 30 seconds after they stop being used. You can use this source number to change the disconnect timeout. The supported range is 1 to 600 seconds.

- `LONGER_NAMES`

  Used to increase the length of names sent for display on older DS phones such as 2400, 4400 and 5400 Series.

- `MEDIA_NAT_DM_INTERNAL=`*N*

  Used in conjunction with the setting **System | VoIP | Allow Direct Media Within NAT Location**. When **Allow Direct Media Within NAT Location** is enabled, the default behavior is to attempt direct media between all types of devices (H323 and SIP remote workers and IP Office Lines behind a NAT). For routers using H323 ALG or SIP ALG, it can be desirable to only attempt direct media between certain device types. In this case, set this `NoUser` user source number where `N` is the sum of the following values:

  - 1 = Include H323 phones.
  - 2 = Include SIP phones.
  - 4 = Include IP Office lines.

  For example, if the router has SIP ALG that cannot be disabled, to disable attempting NAT direct media for SIP devices, set `MEDIA_NAT_DM_INTERNAL=5` to include only H323 phones and IP Office Lines.

- `NI2_CALLED.../NI2_CALLING...`

  The following `NoUser` source numbers are applied to calls on ETSI PRI trunks:

  - `NI2_CALLED_PARTY_PLAN=`*X*

    Forces the NI2 Called Party Numbering plan for ETSI PRI trunks, where `X` equals `UNKNOWN` or `ISDN`.

  - `NI2_CALLED_PARTY_TYPE=`*X*

    Forces the NI2 Called Party Numbering type for ETSI PRI trunks, where `X` equals `UNKNOWN`, `INT`, `NATIONAL` or `SUBSCRIBER`.

  - `NI2_CALLING_PARTY_PLAN=`*X*

    Forces the NI2 Calling Party Numbering plan for ETSI PRI trunks, where `X` equals `UNKNOWN` or `ISDN`.

  - `NI2_CALLING_PARTY_TYPE=`*X*

    Forces the NI2 Calling Party Numbering type for ETSI PRI trunks, where `X` equals `UNKNOWN`, `INT`, `NATIONAL` or `SUBSCRIBER`.

- `NO_DIALLED_REF_EXTERNAL`

  On outgoing external calls made using short codes, the short code dialed is displayed on the user's phone and any directory matching is based on that number. This source number

changes the behavior to display the telephone number output by the short codes and base directory matching on that number.

- `onex_...`

  The following NoUser source numbers are used to alter the IP addresses used for Avaya one-X® Portal for IP Office access.

  - `onex_l1=`*<IP Address>*

    Sets the IP address of the one-X server that can be accessed by clients registered on the LAN1 interface.

  - `onex_l2=`*<IP Address>*

    Sets the IP address of the one-X server that can be accessed by clients registered on the LAN2 interface.

  - `onex_port_l1=`*<IP Address>*

    Sets the port of the one-X server that can be accessed by clients registered on the LAN1 interface.

  - `onex_port_l2=`*<IP Address>*

    Sets the port of the one-X server that can be accessed by clients registered on the LAN2 interface.

  - `onex_port_r1=`*<IP Address>*

    Sets the port of the one-X server that can be accessed by remote clients registered on the LAN1 interface.

  - `onex_port_r2=`*<IP Address>*

    Sets the port of the one-X server that can be accessed by remote clients registered on the LAN2 interface.

  - `onex_r1=`*<IP Address>*

    Sets the IP address of the one-X server that can be accessed by remote clients registered on the LAN1 interface.

  - `onex_r2=`*<IP Address>*

    Sets the IP address of the one-X server that can be accessed by remote clients registered on the LAN2 interface.

- `PHONE_LANGUAGES`

  Cause an IP Office system to output a set of language files that can then be used to customize the text used on some phones. Refer to the Avaya IP Office Locale Settings manual.

- `PRESERVED_CONN_DURATION=`*<Minutes (1 to 120)>*

  When **System | Telephony | Telephony | Media Connection Preservation** is enabled, active calls are preserved for up to 120 minutes before being disconnected.. This `NoUser` source number can be used to adjust the duration in the range 1 to 120 minutes.

- `PRESERVED_NO_MEDIA_DURATION=`*<Minutes (1 to 120)>*

When **System | Telephony | Telephony | Media Connection Preservation** is enabled, calls on which no RTP, RTCP or speech is detected are disconnected after 10 minutes. This `NoUser` source number can be used to adjust the duration in the range 1 to 120 minutes.

- `PUBLIC_HTTP=`*<File server address>*

  If the IP Office is using the HTTP Redirection settings, this source number can be used to set a separate redirection address to be given to remote phones.

- `REPEATING_BEEP_ON_LISTEN`

  By default, if you set **Beep on Listen**, when a user invokes **Call Listen** they hear an entry tone (3 beeps) only at the start of the call. When this parameter is set, they also hear a beep every 10 seconds.

- `RTCP_COLLECTOR_IP=`*<IP Address>*

  When using a Prognosis server for call quality monitoring, set the IP address of the IP Office system as configured in the Prognosis server.

- `RW_SBC_...`

  Set the IP addresses that remote SIP extensions should use to connect to the IP Office via an ASBCE. For R11.1.2.4 and higher, these have been replaced with settings on the **System | LAN | Network Topology** menus.

- `SET_46xx_PROCPSWD=`*<NNNNN>*

  Set the new password indicated to phones through the auto-generated `46xxsettings.txt` file.

- `SET_96xx_SIG=`*<X>*

  When set, inserts the line `SET SIG X` into the auto-generated `46xxsettings.txt` settings files.

- `SET_ADMINPSWD=`*<NNNNN>*

  Set the new admin password indicated to K100 Series phones through the auto-generated `46xxsettings.txt` file.

- `SET_B199_FW_VER=`*<NNNN>*

  If set, overrides the default B199 firmware version the IP Office system inserts into its auto-generated `avayab199_fw_version.xml` file. with `firmware-NNNN-release.kt`. Supported for IP Office R11.1.2.4 and higher.

- `SET_CDNL=`*"<NNNN>"* or `SET_CDNL=`*"<NNNN>","<MMMM>*

  For Avaya Workplace Client clients on mobile iOS and Android devices, this source number specifies numbers to dial using the device's native dialer rather than using by the client application. The IP Office adds the numbers to the auto-generated `46xxsettings` file as a `SET CELLULAR_DIRECT_NUMBER_LIST=` entry. For details, refer to the IP Office Avaya Workplace Client Installation Notes manual.

  - The source number can specify multiple numbers, separated by commas, in a string of up to 63 characters.
  - You can use multiple `SET_CDNL=` entries.

  - The maximum length of the SET CELLULAR_DIRECT_NUMBER_LIST= string is 127 characters.

- SIP_ENABLE_HOT_DESK

  By default, the use of hot-desking on J129 and H175 phones is blocked. This source numbers overrides that behavior.

- SIP_EXTN_CALL_Q_TIMEOUT=<Minutes>

  Sets the unanswered call duration after which unanswered SIP calls are automatically disconnected. If not set, the normal default is 5 minutes. This NoUser source number can be used to adjust the duration in the range 0 (unlimited) to 255 minutes.

- SET_HEADSYS_1

  If set, alters the operation of the headset button on 9600 Series phones via the auto-generated 46xxsettings.txt settings file. Normally the headset goes off-hook when the far end disconnects. When this option is set, the headset remains on-hook when the far end disconnects.

- SET_STIMULUS_SBC_REG_INTERVAL=<seconds>

  Set the registration interval used for remote J100 Series phones. Reducing this is necessary if the SBC fails to send TCP RST end-to-end. The recommend value is 180 seconds. If not specified, the default is 1 hour (3600 seconds). Range 180 to 3600 seconds.

- SIP_OPTIONS_PERIOD=<Minutes>

  On SIP trunks, the system periodically sends OPTIONS messages to determine if the SIP connection is active. The rate at which the messages are sent is determined by the combination of the **Binding Refresh Time (seconds)** set on the Network Topology tab and the **SIP_OPTIONS_PERIOD** parameter (in minutes). The frequency of sent messages is determined as follows:

Target	Method
300 seconds	If no **SIP_OPTIONS_PERIOD** parameter is defined and the **Binding Refresh Time (seconds)** is **0**, then the default value of 300 seconds is used.
Less than 300 seconds	Do not define a **SIP_OPTIONS_PERIOD** parameter and set the **Binding Refresh Time (seconds)** to a value less than 300 seconds.
More than 300 seconds	Set both the **SIP_OPTIONS_PERIOD** and **Binding Refresh Time (seconds)** to a value greater than 300 seconds. The OPTIONS message period used is the smaller of the **Binding Refresh Time (seconds)** and the **SIP_OPTIONS_PERIOD**.

- SUPPRESS_ALARM=**1**

  When set, the NoCallerID alarm is not shown in system alarms, SysMonitor and System Status Application .

- TUI:J139_REDUCED_FEATURE_SET

  For R11.1.2.4 and higher, reinstate the pre-R11.1.2.4 feature restrictions applied to J139 phones.

- TUI:NAME_SEARCH_MODE=<n>

The default directory search matching used on feature phones is to simultaneously show matches against all parts of names. This source number can be used to change the name matching behavior.

- 1 = Match starting from start of name.
- 2 - Match starting from last word in name.
- 3 = Match simultaneously from both 1 & 2.
- 4 = Match from the penultimate word in name.
- 7 = Match simultaneously from first, last and penultimate words in name.

- `TUI:NO_TOVM_SK_WHEN_VMOFF`

  On feature phones, suppress the display of the **To VM** softkey when the user's VoiceMail setting is off.

- `VM_TRUNCATE_TIME=<Seconds: 0 to 7>`

  Analog trunks can use busy tone detection to end calls. On calls that go to voicemail, to be recorded or to leave a message, when busy tone detection occurs, the IP Office indicates to the voicemail server how much to remove from the end of the recording in order to remove the busy tone segment. By default, the amount varies to match the system locale (refer to the Avaya IP Office Locale Settings manual).

  For some systems, it may be necessary to override the default if the end of analog call recordings is either being clipped or includes busy tone. This `NoUser` source number can be used to adjust the amount removed in the range 0 to 7 seconds.

- `VMAIL_WAIT_DURATION=<Milliseconds>`

  Sets the number of milliseconds to system waits before passing call audio to Voicemail. On some systems, a delay may be required to allow completion of codec negotiation.

- `VMPRO_OOB_DTMF_OFF`

  Disable the sending of out-of-band digits to the Voicemail Pro voicemail server. This may be necessary on some systems if digit presses are being recorded on calls.

- `WEBRTC_...`

  These source numbers are used for WebRTC support when the User Portal user connects to the remotely using either STUN and/or TURN. For R11.1.2.4 and higher, these have been replaced with settings on the **System | LAN | Network Topology** menus.

- `xmpp_port...`

- These `NoUser` source numbers can be used Avaya one-X® Portal for IP Office to alter the ports used for XMPP connections.

  - `xmpp_port_l1=<Port>`

    Set the port of the XMPP server used by clients registered on the LAN1 interface.

  - `xmpp_port_l2=<Port>`

    Set the port of the XMPP server used by clients registered on the LAN2 interface.

  - `xmpp_port_r1=<Port>`

    Set the port of the XMPP server used by remote clients registered on the LAN1 interface.

- `xmpp_port_r2=<Port>`

  Set the port of the XMPP server used by remote clients registered on the LAN2 interface.

Related links

User Source Numbers on page 913

Part 12: SIP Trunks

Editing Configuration Settings

Chapter 94: SIP Trunk Overview

A growing number of service providers now offer PSTN access to businesses via public SIP trunk connections, either to extend their reach beyond their typical copper based network coverage areas, or so that multiple services (voice and internet access) can be bundled into a single network connection. Although detailed public SIP trunk service offerings vary depending on the exact nature of the offer from the specific service provider, SIP trunks can potentially provide several advantages compared to traditional analog or digital trunks. These advantages include:

- cost savings resulting from reduced long distance charges, more efficient allocation of trunks, and operational savings associated with managing a consolidated network
- simplified dialing plans and number portability
- geographic transparency for local accessibility creating a virtual presence for incoming calls
- trunk diversity and redundancy
- multi-media ready to roll out future SIP enabled applications
- fewer hardware interfaces to purchase and manage, reducing cost and complexity
- faster and easier provisioning

IP Office delivers functionality that enhances its ability to be deployed in multi-vendor SIP-based VoIP networks. While this functionality is primarily based on the evolving SIP standards, there is no guarantee that all vendors, interpret and implement the standards in the same way. To help the SIP service provider, Avaya operates a comprehensive SIP Compliance Testing Program referred to as GSSCP. Avaya's DevConnect program validates the operation of the IP Office solution with the service provider's SIP trunk offering.

Related links

Configuring a SIP Trunk on page 924
SIP Line Requirements on page 925

Configuring a SIP Trunk

This procedure provides the basic steps for configuring a SIP trunk between two IP Office systems.

Before you begin

- You must know the IP address of both ends of the trunk.

- You must have valid licenses on both IP Office systems.
- On Server Edition, make sure you have a non-zero value in the **SIP Trunk Sessions** field on the **License | Remote Server** tab. If you do not, you will see Monitor messages about insufficient licenses.

Procedure

1. In the Manager navigation pane, right click **Line** and select **New** > **SIP Line**.
2. Record the **Line Number** value that appears on the SIP Line page for use later.
3. In the **ITSP Domain Name** field, enter the domain name required by the far end. If nothing is configured in this field, then IP Office inserts the far end's **ITSP Proxy Address** from the **Transport** tab as the ITSP domain in the SIP messaging.
4. Use the default values for the remaining fields.
5. Select the **Transport** tab.
6. In the **ITSP Proxy Address** field, enter the IP Address of the far end.
7. Select the **SIP URI** tab.
8. Click **Add**.
9. Enter values for the **Incoming Group** and **Outgoing Group** fields. You can use the **Line Number** from the **SIP Line** tab for both values.
10. In the Manager navigation page, select **Incoming Call Route**.
11. On the **Standard** tab, in the **Line Group ID** field, enter the **Line Number** from the **SIP Line** tab.
12. Select the **Destinations** tab.
13. In the **Destination** column, replace the value with a period (“.”).
14. In the Manager navigation pane, select **Short Code**.
15. Add a short code to dial the trunk you have just added.
16. One end of the trunk is now configured. Save the configuration to the IP Office.
17. Using Manager, open the configuration for the IP Office at the other end of the SIP trunk and repeat the steps.

Related links

SIP Trunk Overview on page 924

SIP Line Requirements

Use of SIP requires the following:

- **SIP Service Account**

An account or accounts with a SIP internet service provider (ITSP). The method of operation and the information provided will vary. The key requirement is a SIP URI, a web address of the form **name@example.com**. This is the equivalent of a SIP telephone number for making and receiving calls via SIP.

- **Voice Compression Channels**

  SIP calls use system voice compression channels in the same way as used for standard IP trunks and extensions. For an IP500 V2 system, these are provided by the installation of VCM modules within the control unit. RTP relay is applied to SIP calls where applicable.

- **Licensing**

  SIP trunks require licenses in the system configuration. These set the maximum number of simultaneous SIP calls supported by the system.

- **Firewall Traversal**

  Routing traditional H.323 VoIP calls through firewalls often fails due to the effects of NAT (Network Address Translation). For SIP a number of ways to ensure successful firewall traversal can be used. The system does not apply any firewall between LAN1 and LAN2 to SIP calls.

  - **STUN (Simple Traverse of UDP NAT)**

    UDP SIP can use a mechanism called STUN to cross firewalls between the switch and the ITSP. This requires the ITSP to provide the IP address of their STUN server and the system to then select from various STUN methods how to connect to that server. The system can attempt to auto-detect the required settings to successfully connect. To use STUN, the line must be linked to the Network Topology settings of a LAN interface using the line's Use Network Topology Info setting.

  - **TURN (Traversal Using Relay NAT)**

    TCP SIP can use a mechanism called TURN (Traversal Using Relay NAT). This is not currently supported.

  - **Session Border Control**

    STUN does not have to be used for NAT traversal when SBC is between IP Office and the ITSP, since the SBCE will be performing NAT traversal.

- **SIP Trunks**

  These trunks are manually added to the system configuration. Typically a SIP trunk is required for each SIP ITSP being used. The configuration provides methods for multiple URI's from that ITSP to use the same trunk. For each trunk at least one SIP URI entry is required, up to 150 SIP URI's are supported on the same trunk. Amongst other things this sets the incoming and outgoing groups for call routing.

- **Outgoing Call Routing**

  The initial routing uses any standard short code with a dial feature. The short code's Line Group ID should be set to match the Outgoing Group ID of the SIP URI channels to use. However the short code must also change the number dialed into a destination SIP URI

suitable for routing by the ITSP. In most cases, if the destination is a public telephone network number, a URI of the form **123456789@example.com** is suitable. For example:

- **Code**: 9N#
- **Feature**: Dial
- **Telephone Number**: N"@example.com"
- **Line Group ID**: 100

While this can be done in the short code, it is not an absolute necessity. The ITSP Proxy Address or ITSP Domain Name will be used as the host/domain part.

- **Incoming Call Routing**

  Incoming SIP calls are routed in the same way as other incoming external calls. The caller and called information in the SIP call header can be used to match Incoming CLI and Incoming Number settings in normal system Incoming Call Route records.

- **DiffServ Marking**

  DiffServ marking is applied to calls using the DiffServ Settings on the **System** > **LAN** > **VoIP** tab of the LAN interface as set by the line's **Use Network Topology Info** setting.

SIP URIs

Calls across SIP require URI's (Uniform Resource Identifiers), one for the source and one for the destination. Each SIP URI consists of two parts, the user part (for example **name**) and the domain part (for example **example.com**) to form a full URI (in this case **name@example.com**). SIP URI's can take several forms:

- name@117.53.22.2
- name@example.com
- 012345678@example.com

Typically each account with a SIP service provider will include a SIP URI or a set of URI's. The domain part is then used for the SIP trunk configured for routing calls to that provider. The user part can be assigned either to an individual user if you have one URI per user for that ITSP, or it can also be configured against the line for use by all users who have calls routed via that line.

Resource Limitation

A number of limits can affect the number of SIP calls. When one of these limits is reached the following occurs: any further outgoing SIP calls are blocked unless some alternate route is available using ARS; any incoming SIP calls are queued until the required resource becomes available. Limiting factors are:

- the number of licensed SIP sessions.
- the number of SIP sessions configured for a SIP URI.
- the number of voice compression channels.
  - **SIP Line Call to/from Non-IP Devices** Voice compression channel required.
  - **Outgoing SIP Line Call from IP Device** No voice compression channel required.
  - **Incoming SIP Line Call to IP Device** If using the same codec, voice compression channel reserved until call connected. If using differing codecs then 2 channels used.

SIP Information Display

The full `from` and `to` SIP URI will be recorded for use by SMDR. For all other applications and for telephone devices, the SIP URI is put through system directory matching the same as for incoming CLI matching. First a match against the full URI is attempted, then a match against the user part of the URI. Directory wildcards can also be used for the URI matching.

Related links

SIP Trunk Overview on page 924

Chapter 95: SIP Headers and URIs

During SIP calls, various request and response messages are exchanged (see Request methods on page 970 and Response methods on page 971). For example, a SIP call is started by the caller sending an `INVITE` request to which `180 Ringing` and `200 OK` responses are expected.

These request and response messages contain various 'headers' detailing different information values, see Headers on page 971. Some of these headers contain contact information in the form of SIP URIs (Uniform Resource Identifier). For example; the caller, the original destination, the current destination, and so on.

Related links

SIP URI Formats on page 929
Standard SIP Headers on page 930
Setting the SIP URI Host on page 930
Setting the SIP URI Content on page 931
Selecting the SIP Header Format Used on page 933

SIP URI Formats

When a header contains contact information, it is typically added using the 'SIP URI' format:

- A SIP URI is like an email address. In its simplest form, it appear as `sip:content@hostname`.
- The SIP URI can also indicate the target port: `sip:content@hostname:port`
- For some headers, the SIP URI can also include preferred display name. When that happens, the `sip:` part is enclosed in `< >` brackets. For example: `display <sip:content@hostname>`.
  - From the caller name, the line's **Name Priority** setting sets whether this name is displayed on internal phones or replaced by a name match from the system or user directories.
- Some line providers may use a different format called `TEL URI`. That takes the form `tel:123456789`.
- The system can use SIPS format which replaces `sip:` with `sips:`. This is used to indicate that the connection should use TLS from end to end. That is, every hop should use TLS.

The header format used by each SIP line in the system configuration is set by its URI Type setting. See Selecting the SIP Header Format Used on page 933.

Related links

SIP Headers and URIs on page 929

Standard SIP Headers

Most request messages exchanged during SIP calls include the following headers:

Header	Description
`Request-URI`	Also known as `Request-Line-URI` or `R-URI`. The first line of the request message indicates the destination for routing the message. If the message is routed through multiple hops, this header changes each time to indicate the next destination. Similarly, if the call is redirected, the header is changed to show the new destination.
`Via`	Every intermediate proxy that has been involved in the routing of the request is included as a SIP URI. These are used in reverse order to process response messages.
`To`	This header indicates the original intended call target. It contains a SIP URI and can include a display name. • On outgoing calls, the identity of the called party is not known at the time of the initial `INVITE`. Therefore the `To:` field only contains the information necessary to route the call. That is, the dialed digits after any short code and prefix manipulation.
`From`	This header indicates the identity of the caller. It contains a SIP URI and can include a display name.
`Contact`	This header indicates the return address for responses to the call request. This is a SIP URI. The SIP URI is similar to the `From` header. However, if anonymous calling is enabled, the field becomes semi-anonymous. For example; `Contact: <sip:anonymous@135.55.86.70:5060;transport=udp>`
`P-Asserted-Identity`	The SIP URI is similar to the `From` header. The field is unchanged even if anonymous calling is enabled.

Related links

SIP Headers and URIs on page 929

Setting the SIP URI Host

When the system needs to send a SIP URI in a header, the information used for the @host part of SIP URI is taken from the following settings (listed in order of priority, starting with the highest):

Source/Setting	Descriptions
Short Code	Short codes used to route calls to a SIP line can specify the host for the calls `To` and `R-URI` headers. • This is done in the short code's **Telephone Number** field by adding the host as a quoted suffix. For example, `N"@example.com"`. • The value must be enclosed in `" "` quotation marks to prevent any part being interpreted as short code wildcard characters.
Local Domain Name	If set, this setting is used for the host part the From, Contact and Diversion headers sent by the system, overriding the ITSP Domain Name below. It is also used for the PAI header if **Use Domain for PAI** is selected on the SIP line.
ITSP Domain Name	If set, this setting is used for the host part of the `From`, `To`, `Diversion` and `R-URI` headers sent by the system.
ITSP Proxy Address	This setting is used for the host part of most headers sent by the system if none of the values above are set. However, if several addresses are set here, then either the **ITSP Domain Name** and/or **Local Domain Name** settings must be used.

Related links

SIP Headers and URIs on page 929

Setting the SIP URI Content

Each SIP line in the system has a **Call Details** form which can contains SIP URI entries. They set which headers are used and how the header data is populated or the values against which headers are matched.

Every incoming and outgoing call which uses the line is matched to one of these.

Display

As above, the line URI associated with the call also sets the display name source for any headers that require it, for example the From and To headers.

Setting	Description
Auto	The system automatically determines the appropriate value to use. It will use external numbers if forwarding incoming calls, and internal numbers for calls made by a local user. • On incoming calls, if the **Local URI** is set to **Auto**, the system looks for matches against extension numbers and system short codes. • On outgoing calls, it allows short code manipulation of the caller number and name. For example: **S** to explicitly set the caller number, **W** to set withheld, **A** to allow (override any previous withhold setting), **Z** to set the caller name.

Table continues…

Setting	Description
Use Internal Data	Use the SIP settings of the user (**User** > **SIP**), group (**Group** > **SIP**) or voicemail services (**System** > **Voicemail** > **SIP**) making or receiving the call: • Use the **SIP Display Name (Alias)** setting. • If the Anonymous is selected, use that value instead.
Manual Entry (Explicit)	If required, you can type in a value. This is only used for fields configured as **Explicit**. This is typically used to set the DDI to be associated with SIP line appearances.
Credential Values	If a set of SIP Credentials has been selected in the URI settings, then the **User name**, **Authentication Name** or **Contact** values from the SIP credentials can be selected as values.

Content

On both incoming and outgoing SIP calls, the system associates one of the SIP line's URI entries with the call. The settings of that URI specify how the system should populate and use the `content` part of the SIP URI in various header. The possible settings are:

Setting	Description
Auto	If **Auto** is selected, the system automatically determines the appropriate value to use. It uses external numbers when forwarding incoming calls, and internal extension numbers for calls made by a local user. • On incoming calls, the system looks for matches against extension numbers and system short codes. • On outgoing calls, the system allows short code manipulation of the caller number and name. For example: **S** to explicitly set the caller number, **W** to set withheld, **A** to allow (override any previous withhold setting), **Z** to set the caller name.
Use Internal Data	Use the SIP settings of the user (**User** > **SIP**), group (**Group** > **SIP**) or voicemail services (**System** > **Voicemail** > **SIP**) making or receiving the call: • Use the **SIP Display Name (Alias)** setting. • If the Anonymous is selected, use that value instead.
Manual Entry	If required, you can manually type in a value to use. The value is then used by other fields configured as **Explicit**. This is typically used to set the DDI to be associated with SIP line appearances.
Credential Values	If a **Credentials** entry has been selected above, then the **User name**, **Authentication Name** and **Contact** values from the selected credentials entry can be selected as values. The value is then used by other fields configured as **Explicit**. • URI values should only be set using credentials when required by the line provider. For example, some line providers require the `From` header to always contains the credentials used for registration, whilst other headers are used to convey information about the caller ID.

Related links

SIP Headers and URIs on page 929

Selecting the SIP Header Format Used

The header format used by the system is set by the **SIP Line** > **URI Type** setting. This has the following options:

- **SIP** - Use `sip:` format SIP URIs.
- **Tel** - When selected, the system uses the Tel URI format, for example `tel:+1-816-555-1212`, in **To** headers.
- **SIPS** - When selected, the system replace the `sip:` part of the SIP URIs it sends with `sips:`. That indicates that TLS must be used for all stages of the call. To use this, the line's **Layer 4 Protocol** needs to be set to TLS.

Related links

SIP Headers and URIs on page 929

Chapter 96: Outgoing SIP Call Routing

This section describes the overall processes used by the IP Office to route outgoing SIP trunk calls.

Related links

SIP Outgoing Call Routing on page 934
Anonymous SIP Calls on page 935
SIP ARS Response Codes on page 936
Typical outgoing call scenarios on page 938

SIP Outgoing Call Routing

When a user makes a call by dialing a number:

1. **Dial Short Code Completed:**

   The dialing is processed though user, user rights, system and ARS short codes.

2. **SIP Line URI/Line Appearance Matching:**

   The IP Office looks for a SIP URI with the same **Outgoing Group** as the short code's **Line Group ID**.

   a. Each line is checked in **Line Number** order.
   b. **SIP Line Appearance** entries are checked first, then **SIP URI** entries.
   c. Entries that have reached their **Max Sessions** or **Outgoing Sessions** are skipped.
   d. Once a match is found, it and the SIP line to which it belongs are used:
      - The line's **Call Initiation Timeout (s)** (default 4 seconds) sets how long the IP Office waits for a response to the attempt to initiate a call before following any alternate routes set in the ARS form.
      - The line's **Call Queuing Timeout (m)** (default 5 minutes) sets how long the IP Office waits for the call to be answered after receiving a provisional response.

3. **No Available URI:**

   If all possible matches have reached their **Max Sessions** or **Outgoing Sessions** value:

   - If the call was routed via an ARS short code, the ARS settings determine whether the call can be redirected to an alternate route.
   - Otherwise, the call waits for a matching URI to become available (`"Waiting for Line"`).

Related links

Outgoing SIP Call Routing on page 934

Anonymous SIP Calls

Calls can be made and received with indication that the caller ID should be withheld. In SIP terminology, these are 'anonymous' calls.

Important:

- Some line providers do not support the use of anonymous and will drop those calls. Others may require additional configuration in order to accept the use of anonymous status.

For outgoing calls, the call can be set as anonymous using the following methods:

- **W Short Code Character**

  Adding a **W** as a suffix to the Telephone Number setting of a short code indicates withhold the caller ID. For SIP calls, this is supported if the line URI being used is set to **Auto**.

- **User/Group Anonymous Setting**

  Each system user and hunt group has a set of SIP settings (**User** > **SIP**, **Group** > **SIP**, **System** > **Voicemail** > **SIP**). If selected, the **Anonymous** setting indicates that the user or group should treated as anonymous when making/receiving SIP calls. The voicemail service also has SIP settings that include the option to be anonymous. For SIP calls, this is supported if the line URI used is set to **Use Internal Data**.

- **Withhold Number Option**

  Avaya feature phones can be configured to withhold the caller ID (**Features** > **Call Settings** > **Withhold Number**). That matches the **W** short code operation above.

How Does Setting a Call as Anonymous Affect the Call Headers?

Setting anonymous/caller ID withheld has the following effect on the information added to SIP URIs sent by the system:

- The system adds a `Privacy` header to the call information.
- If **Send From In Clear** is not enabled (the default):
  - The SIP URI in the From header is anonymized:
    - The display name part is set to `"Anonymous"`.
    - The content and host parts are set to dummy values (`anonymous@anonymous.invalid`).
  - The `Privacy` header is set to user, otherwise it is set to id.
  - A `PPI` or `PAI` header is used to contain the caller's number. This is done using the line's **Use PAI for Privacy** setting (off and so `PPI` is used by default). `PAI` headers should only be used in a trusted network.

- If **Send From In Clear** is enabled:
  - The `From` header is not anonymized,
- When used in SIP URI and SIP Line Appearances, the **P Preferred ID** or **P Asserted ID** entries should be configured to be the same or only one of them should be configured.

Related links

Outgoing SIP Call Routing on page 934

SIP ARS Response Codes

Through SIP RFC3398, many of the response codes used for SIP calls are translations of ISDN codes. For outgoing calls, these can affect the routing through ARS as follows:

Do Not Use This Line Group

The following response codes will cause the system's ARS to no longer target the particular outgoing line group. It depends on other settings whether the ARS attempts to target the call to a different line group or escalate it to another ARS entry.

Code	Cause Code
1	Unallocated Number.
2	No route to specific transit network/(5ESS) Calling party off hold.
3	No route to destination./(5ESS) Calling party dropped while on hold.
4	Send special information tone/(NI-2) Vacant Code.
5	Misdialed trunk prefix.
8	Preemption/(NI-2) Prefix 0 dialed in error.
9	Preemption, cct reserved/ (NI-2) Prefix 1 dialed in error.
10	(NI-2) Prefix 1 not dialed.
11	(NI-2) Excessive digits received call proceeding.
22	Number Changed.
28	Invalid Format Number.
29	Facility Rejected.
50	Requested Facility Not Subscribed.
52	Outgoing calls barred.
57	Bearer Capability Not Authorized.
63	Service or Option Unavailable.
65	Bearer Capability Not Implemented.
66	Channel Type Not Implemented.
69	Requested Facility Not Implemented.

Table continues…

Code	Cause Code
70	Only Restricted Digital Information Bearer Capability Is Available.
79	Service Or Option Not Implemented.
88	Incompatible.
91	Invalid Transit Network Selection.
95	Invalid Message.
96	Missing Mandatory IE.
97	Message Type Nonexistent Or Not Implemented.
98	Message Not Implemented.
99	Parameter Not Implemented.
100	Invalid IE Contents.
101	Msg Not Compatible.
111	Protocol Error.
127	Interworking Unspecified.

Stop ARS

The following response codes end the outgoing call routing and any further ARS targeting of the call.

Code	Cause Code
17	Busy.
21	Call Rejected.
27	Destination Out of Order.

No Affect

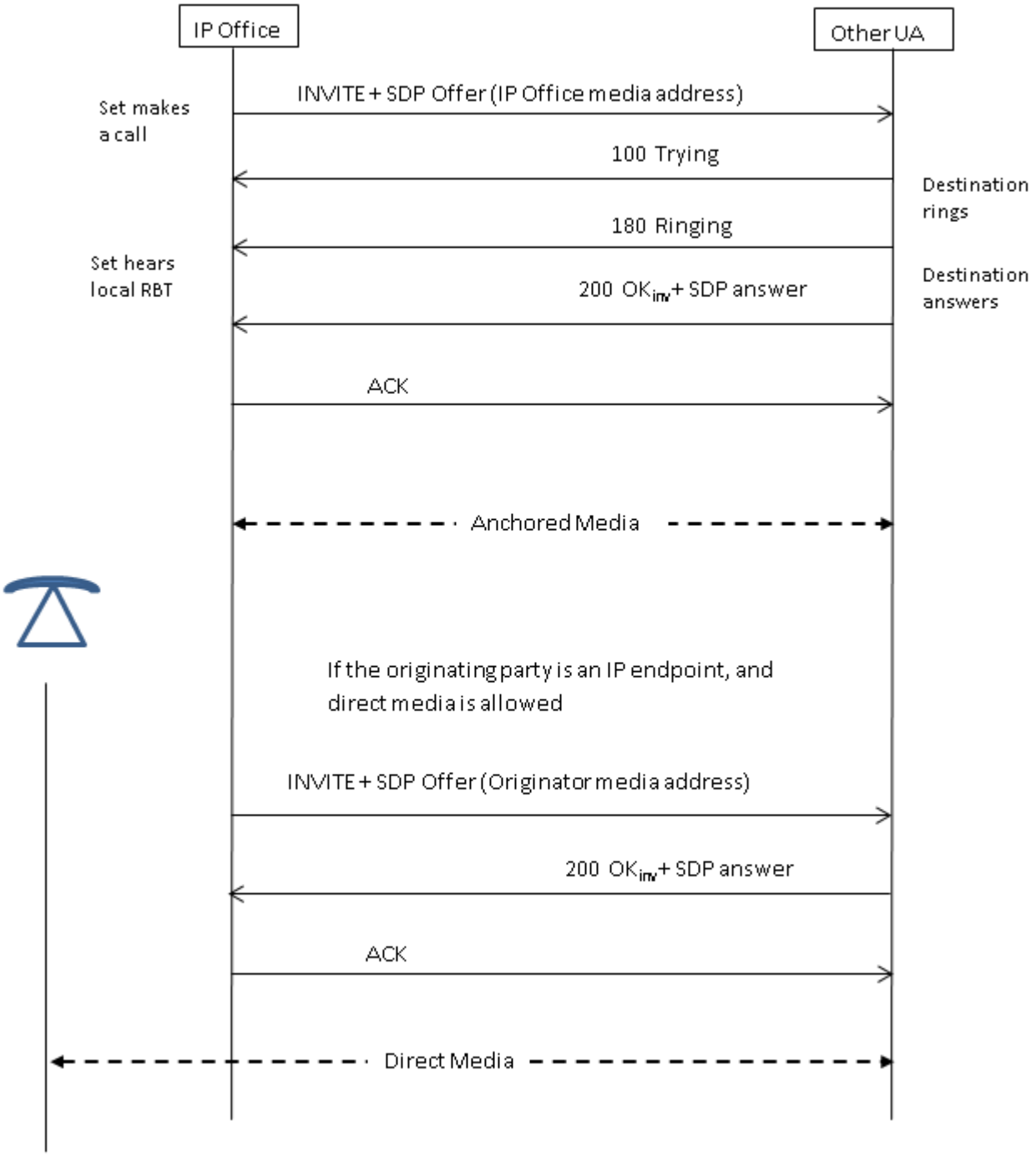
All other cause codes do not affect ARS operation.

Related links

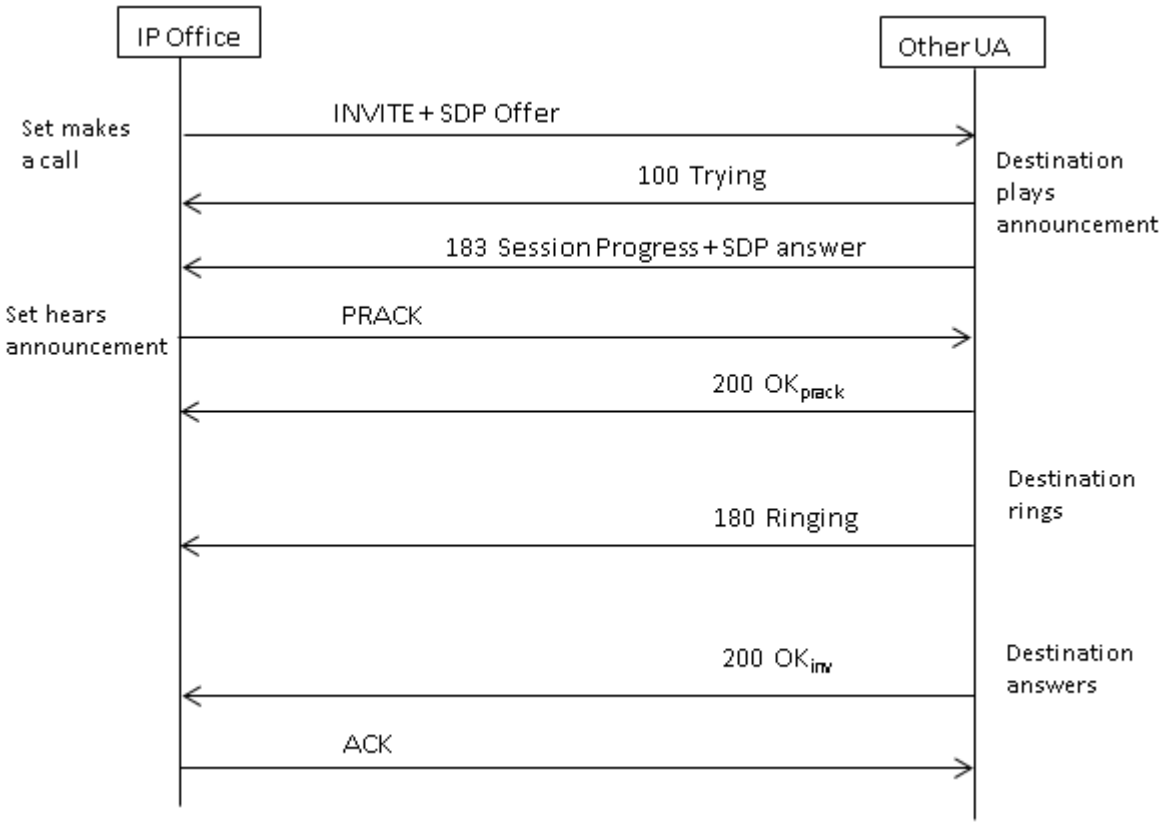
Outgoing SIP Call Routing on page 934

Typical outgoing call scenarios

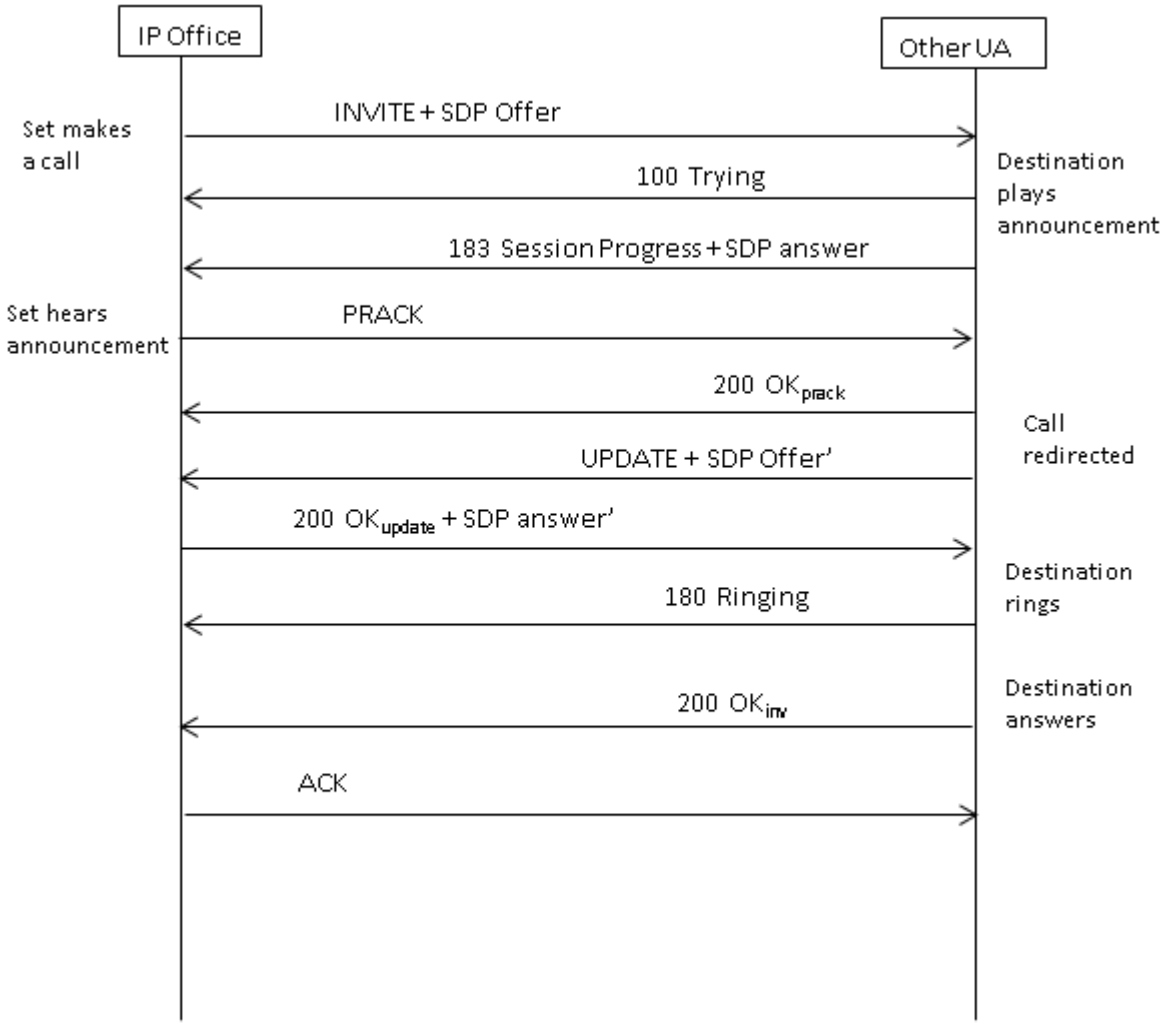
INVITE with SDP, local ringback



INVITE with SDP, early media



INVITE with SDP, early media re-directed by destination



Related links

Outgoing SIP Call Routing on page 934

Chapter 97: Incoming SIP Call Routing

This section describes the overall processes used by the IP Office to route incoming SIP trunk calls.

Related links

SIP Short Codes on page 941
SIP Incoming Call Routing on page 942
SIP Prefix Operation on page 944
Media path connection on page 944
SIP Caller Name and Number Display on page 945
Typical incoming call scenarios on page 946

SIP Short Codes

Outgoing SIP calls are largely processed through short codes in the same way as for other line types. The following specific notes apply:

Note	Description
En-Bloc Dialing is Required	SIP Lines do not use overlap dialing. They expect to receive the full destination number, called 'en-bloc' dialing. • The short code used to route calls to a SIP Line should use a **;** (semi-colon) character at the end of the short code field. That character instructions the system to wait for dialing to be completed before using the short code. • Dialing complete is indicated by either: - the dialer pressing # - the device or application being used sending a dialing complete signal. - the IP Office's **Dial Delay Time** expiring. The default is 4 seconds.
Caller ID Characters	For SIP URIs configured to **Auto** (the default), the short code **Telephone Number** field characters used to control the sending of the caller ID number are supported. Those characters are **A**, **W**, **S** and **SS**.
Host ID	Short codes used to route the call to a SIP line can specify the host to be used for `To` and `R-URI` headers. This is done in the short code's **Telephone Number** field by adding the host as a quoted suffix. For example, `N"@example.com"`. The value must be enclosed in `" "` quotation marks in order to prevent its characters being interpreted as short code wildcards.

Related links

Incoming SIP Call Routing on page 941

SIP Incoming Call Routing

When the IP Office receives a SIP call, it determines the routing of the call as follows:

1. **Line Matching:**

   The incoming SIP call is matched to a SIP line. If no match is found, the call is ignored. SIP line matching is done in two stages:

   a. **Protocol Matching:**

      The call is matched with lines configured with the same protocol (UDP, TCP or TLS) and listening port settings.

   b. **Line Association:**

      If there are several possible line matches, they are checked in **Line Number** order, for a match between the incoming call's source and each line's **Association Method** setting.

2. **Line Call Details Matching:**

   Using the line's **Call Routing Method**, either the `To` or `Request-URI` of the incoming SIP request is used to find a matching **Local URI**.

   - The IP Office first looks for a matching **SIP Line Appearances**. If a match is found, the call is associated with the first available line appearance number in the **Incoming ID** order setting.
   - If no **SIP Line Appearances** match is found, the IP Office checks the line's **SIP URIs** in their URI number order.
   - Entries at their **Max Session** or **Incoming Sessions** values are ignored.
   - When an match is found, its **Incoming Group ID** setting is used for incoming call route matching. For **SIP Line Appearances**, this is in addition to altering on matching line appearance buttons.
   - If no match is found, the IP Office uses its **Service Busy Response** setting (`486 Busy here` or `503 Service Unavailable`) to end the call.

3. **Incoming Call Route matching:**

   The IP Office's incoming call route entries are checked for a match.

   a. The matching uses the following options in order:

      a. **Line Group Match:**

         Only incoming call routes with a **Line Group ID** setting that matches the SIP lines appearance/SIP URI's **Incoming Group ID** setting are checked.

      b. **Incoming Number Match:**

         The IP Office looks for call routes with a match between their **Incoming Number** setting and the **Local URI** value received. There is always a received number

value with incoming SIP calls, so always a potentially incoming number matching value.

- Incoming calls routes with a blank **Incoming Number** field match any incoming number.
- If the incoming call route's **Destination** is set to **.** (period), the **Local URI** received is used to look for destination matches.
  - If set to **Auto**, the IP Office looks for a matching extension number or system short code.
  - If set to **Use Internal Data**, the system looks for a match against the **SIP Name** of users and then groups.

c. **Incoming CLI Match**

From the possible matches, the IP Office looks for a match between the each route's **Incoming CLI**, if set, and the caller details in the `From` header. For `SIP URI` and `TEL URI` headers, partial matching starting from the left is supported. For IP addresses, only exact matches are supported.

b. If the call matches more than one incoming call route:

a. The most precise match is used. For example, the highest number of matching criteria and highest number of exact digit rather than wildcard character matches.

b. If the call stills matches more than one incoming call route, the one added to the configuration first is used.

c. If there is no match:

a. For calls using a line's SIP URI entry with its **Local URI** set to **Auto**, the incoming number is checked for a direct match to an internal extension number.

b. Otherwise, busy indication is sent to the caller and the call is dropped.

4. **Incoming Call Route Match:**

Once a match is resolved, this determines the incoming call route’s current destination:

a. Each incoming route can include multiple pairs of main and fallback destinations.

b. Apart from the default pair, each pair uses an associated time profile. The time profile defines when that destination pair should be used.

a. With multiple destination pairs, the entry used is the first, working from bottom up, whose time profile is currently 'true'. If no match occurs, the **Default Value** options are used.

b. The system attempts to present the call to the destination. If the destination is busy, it presents the call to the fallback extension.

5. **Call Presentation:**

The call is presented to the destination. If the call was routed via a **SIP Line Appearance**, the call also alerts on any matching **Line Appearance** buttons.

Related links

Incoming SIP Call Routing on page 941

SIP Prefix Operation

The SIP line settings include settings for **Prefix**, **National Prefix**, **Country Code** and **International Prefix** values. These values are used in the following order:

1. If the number starts with a + symbol, the symbol is replaced with the **International Prefix**.
2. If the **Country Code** has been set:
   a. If the number begins with the **Country Code**, or **International Prefix** plus **Country Code**, the IP Office replaces them with the **National Prefix**.
   b. If the number does not start with the **National Prefix** or **International Prefix**, the IP Office adds the **International Prefix**.
3. If the incoming number does not begin with the **National Prefix** or **International Prefix**, the IP Office adds the **Prefix**.

Examples

For example, if the SIP Line is configured with prefixes as follows:

- **Prefix**: 9 - The external dialing prefix used to make outgoing external calls.
- **National Prefix**: 90 - The expected prefix for outgoing national calls, including the external dialing prefix.
- **International Prefix**: 900 - The expected prefix for outgoing international calls, including the external dialing prefix.
- **Country Code**: 44 - The local country code.

Number Received	Processing	Resulting Number
+441707362200	Following rule 1, the + is replace with the **International Prefix**. The number now matches the **International Prefix** and **Country Code**. Following rule 2a, they are replace with the **National Prefix**.	901707362200
00441707362200	Following rule 2a, the **International Prefix** and the **Country Code** are replaced with the **National Prefix**.	90107362200
441707362200	Following rule 2a, the **Country Code** is replace with the **National Prefix**.	901707362200
6494770557	Following rule 3, the **International Prefix** (900) is added.	9006494770557

Related links

Incoming SIP Call Routing on page 941

Media path connection

IP Office does not provide in-band ringback to incoming SIP trunk calls. The only normal scenario in which an incoming SIP trunk call hears in-band ringback occurs when the call terminates on an

analog trunk. With analog trunks, the media path is cut through immediately because IP Office has no way of determining the state (ringing, busy, answered) of the trunk.

IP Office can connect “early” media before the call is answered by sending a 183 `Session Progress` response. This is only done when the following two conditions are met:

- A `PROGRESS` (in-band tone indication or 183 Session Progress with SDP) message is received from the destination. This can only happen in a SIP-to-PRI or SIP-to-SIP tandem call scenario.
- The `INVITE` message contains `SDP`.
  - IP Office does not attempt to connect early media on `PROGRESS` when there is no `SDP` in the initial `INVITE`, since this is unlikely to succeed. The likely reason there is no `SDP` in the `INVITE` is probably that the originating system does not know the originator’s media address yet. A typical scenario where this is the case occurs when the call on the originating system comes from an H.323 SlowStart trunk.

Related links

Incoming SIP Call Routing on page 941

SIP Caller Name and Number Display

For incoming SIP calls, the caller name and number are obtained from the following headers:

Value	Description
Caller Name	Unless withheld (see notes below), the caller number for incoming calls is taken from `PAI` header if present, otherwise from the `From` header. The SIP line's advanced settings **Caller ID FROM Header** option can be used to force use of the `FROM` header only.
Caller Number	The caller name for incoming calls is taken from the name supplied with the following headers, in order of priority with highest first: 1. `PPI` header 2. `PAI` header 3. `Remote Party ID` header 4. `Contact` header

Notes

1. The above apply regardless of the header settings of the SIP URI handing the incoming call. For example, for incoming caller details, you do not need to have **P Preferred ID** selected and configured in the SIP URI or SIP line appearance. The `PPI` header info is used if present in the incoming request.
2. If the receiving IP Office system has **Caller ID from From** header enabled (disabled by default), then the `From` header name is used regardless of `PAI` or `PPI` headers.
3. If the header to be used for the caller’s name does not contain a name, `“Unknown”` is displayed.

4. Calls from a source that is anonymous display "Withheld" as the caller name and no number.

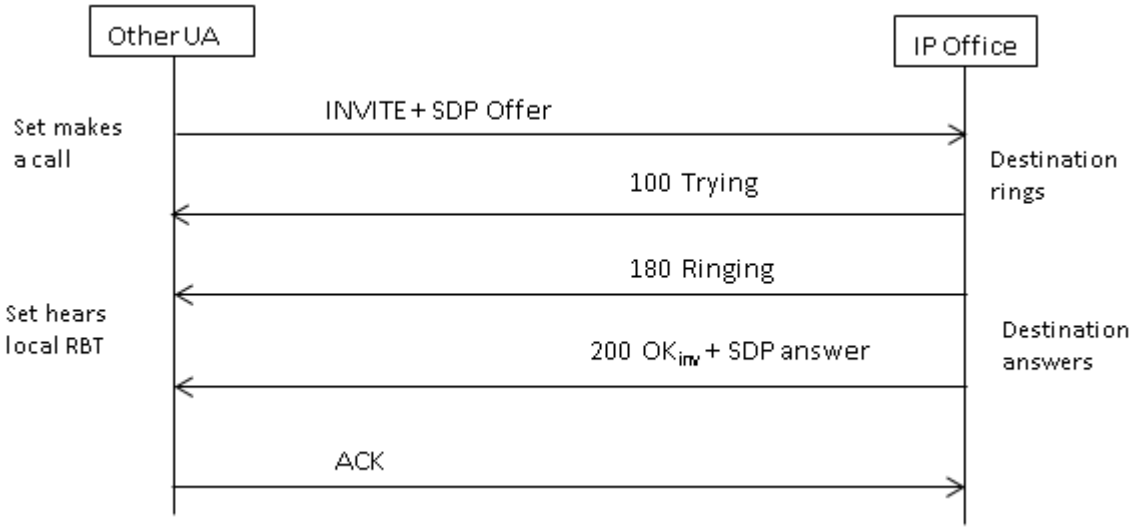
Related links

Incoming SIP Call Routing on page 941

Typical incoming call scenarios

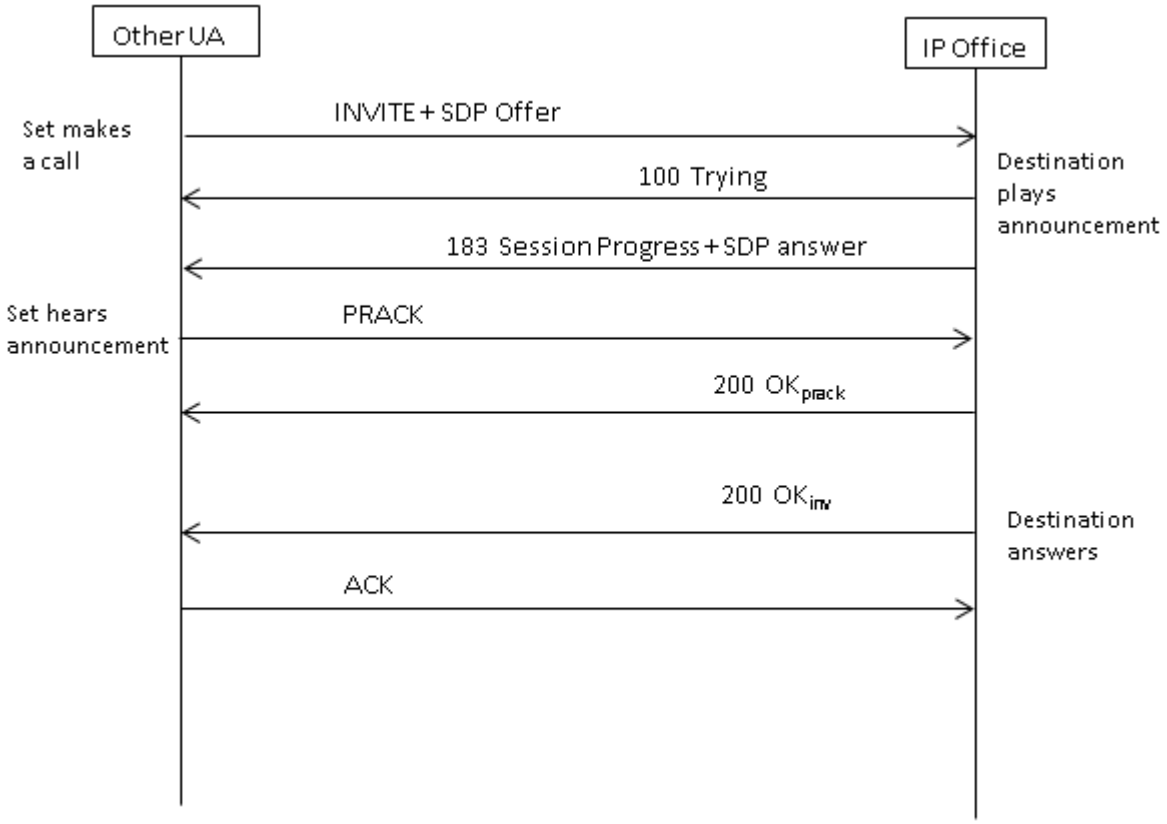
INVITE with SDP, local ringback

If the destination is an analog trunk, the 180 Ringing will be replaced with a 183 Progress with SDP followed immediately by a “fake” answer in order that the media will be connected right away so that the originator hears whatever in-band tones are present on the analog trunk (ringback or busy). If the target is an extension that is unconditionally call forwarded over an analog trunk, then there will be a 180 Ringing without SDP, followed immediately by the “fake” answer.



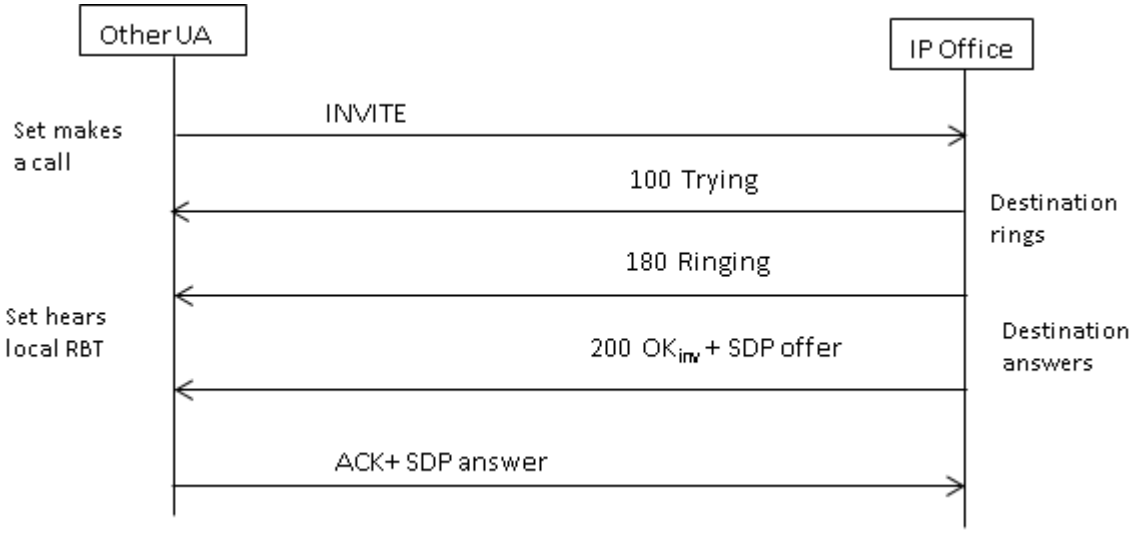
INVITE with SDP, early media

If the SIP Trunk receives a FAR_PROGRESS (in-band) message from its peer in the core (e.g. from a tandem PRI or SIP trunk), it sends a 183 Session Progress message with SDP to the far end. IP Office will connect the media on receipt of 180 or 183 with SDP.



INVITE without SDP, local ring back

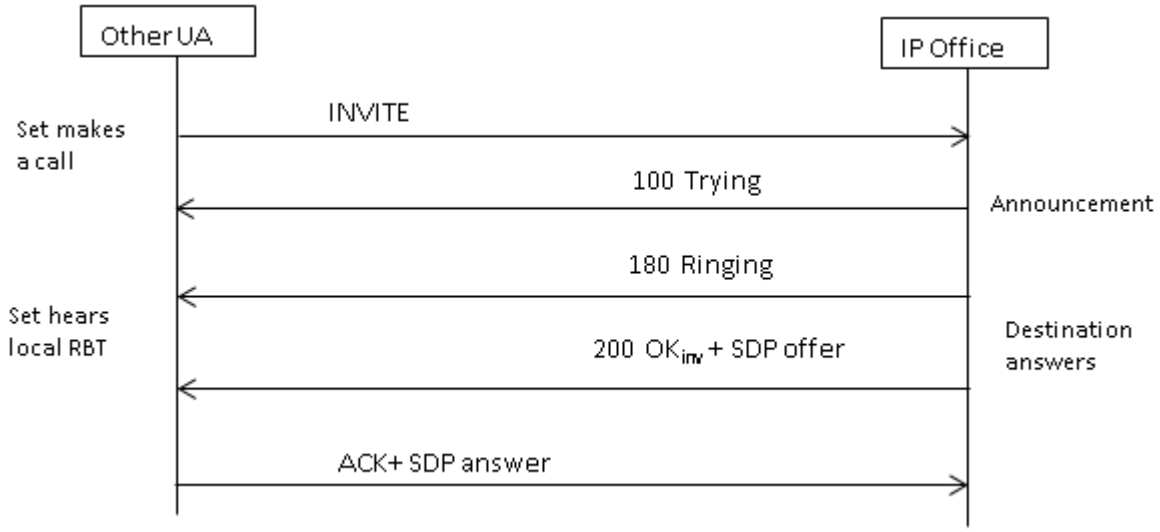
IP Office does not attempt to send early media in this scenario.



INVITE without SDP, early media

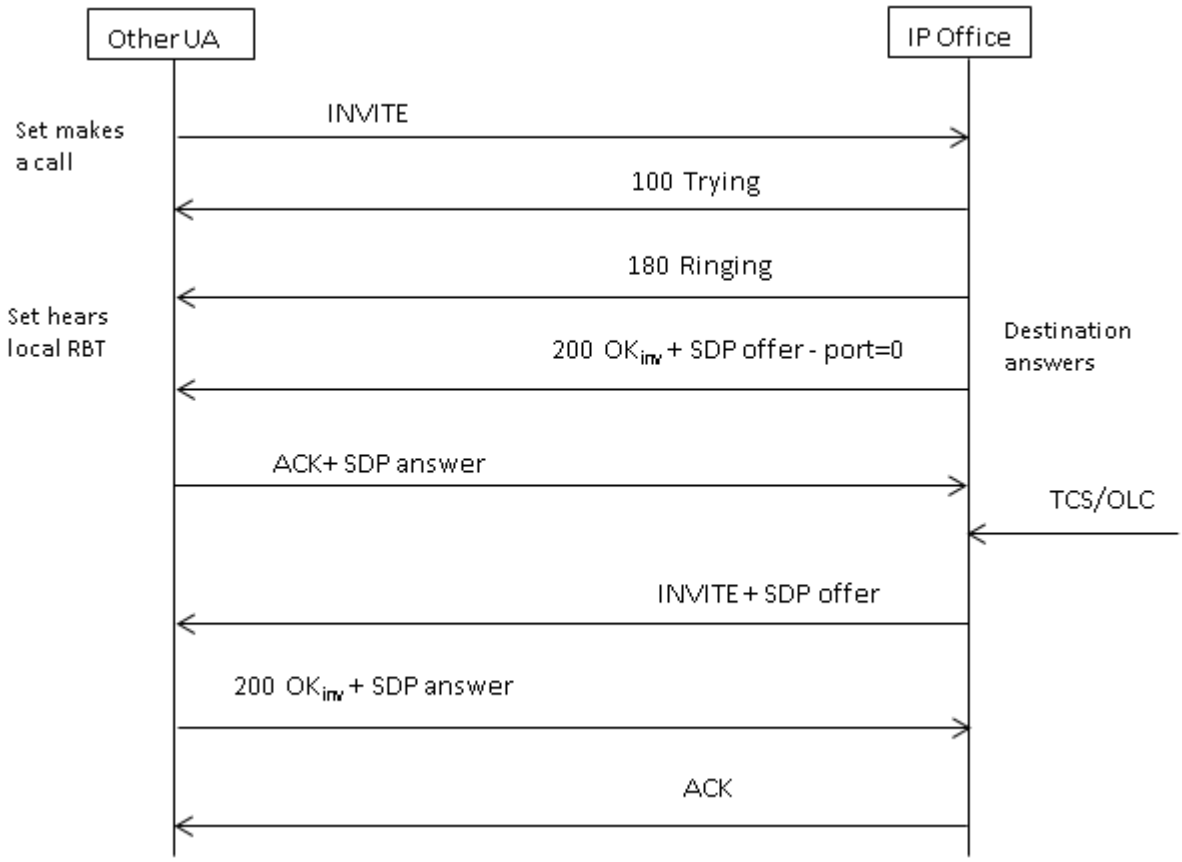
In this scenario, the far end attempts to connect media before the call is answered. IP Office does not provide early media when receiving an empty INVITE, but rather 180 Ringing instead. There is

no requirement to provide an SDP in the 180 Ringing provisional response, as that response is not sent reliably using the PRACK mechanism.



INVITE without SDP, call terminates on H.323 endpoint

If the destination of the call is an H.323 trunk, the destination media address is not known when the call is answered. Therefore, the SDP offer in 200 OK will contain a null port number (and IP address). Once the logical channels are opened on the H.323 side, IP Office sends a re-INVITE using the real media address.



Related links

[Incoming SIP Call Routing](#) on page 941

Chapter 98: SIP messaging

SIP trunk prerequisites

Before any calls can be made, the system must have sufficient SIP trunk licenses for the maximum number of simultaneous SIP trunk calls expected.

On Server Edition systems, the **System | Telephony | Telephony | Maximum SIP Sessions** value must match the total number of SIP extension and trunk calls that can occur at the same time.

Related links

Codec selection on page 950
SIP DTMF Transmission on page 951
Fax over SIP on page 952
SIP Call Hold Scenarios on page 952
SIP Call Transfers (Refer) on page 954
Ringback Tone on page 955
Hold Reminders on page 956

Codec selection

Normal Codec Selection

Codec selection is based on the Offer/Answer model specified in RFC 3264.

1. The calling endpoint issues an offer that includes a list of the codecs it supports.
   - For IP Office SIP trunks, the IP Office offers the codecs set on the SIP trunks **VoIP** tab. It does not offer those set on the extension.
2. The called endpoint sends an answer that normally contains a single codec from the offered list.
   - If there are multiple codecs in the answer, IP Office only considers the first codec. If the SIP Line is configured to do **Codec Lockdown**, it will send another `INVITE` with the single chosen codec.

Codec Changes with reINVITE

For R11.0 and higher, the IP Office supports codec selection following a `reINVITE`. Previously, when a `reINVITE` was received during a call, if the `reINVITE` contained the codec currently in

use, that codec was preferred and kept. For R11.0 and higher, the IP Office reevaluates the codec to use based on any preferences included in the `reINVITE`:

- For example, if the endpoint/trunk has a different codec preference to the system, hold/unhold sequences will result in codec changes. When held, the system codec preference is used to play music-on-hold. When unheld, the codec preferences are reevaluated.

When using this behavior:

- Direct media is supported for SRTP phones that change keys on each `reINVITE`.
- The IP Office supports the transfer of video calls.

Note:

- The new behavior also applies to SM lines and SIP extensions.
- On IP Office systems upgraded to R11.0 and higher, `SLIC_PREFER_EXISTING_CODEC` is automatically added to the **SIP Engineering** tab of any existing SIP lines to retain the existing pre-R11.0 behavior.

Related links

SIP messaging on page 950

SIP DTMF Transmission

DTMF key presses can be transmitted either in-band as audio tones or signaled using DTMF over RTP (RFC 2833)

When using DTMF over RTP (RFC 2833), the IP Office supports asymmetric dynamic payload negotiation when it is necessary to bridge SIP endpoints that do not support payload negotiation. The value used for an initial offer is configured on the **System | Codecs** tab. The default value is 101. Upon receipt of an offer with an RFC2833 payload type, IP Office automatically uses the proposed value rather than its own configured value. This helps to support networks that do not negotiate payload types.

Direct Media Calls

There are cases in which direct media is desirable between SIP trunks and endpoints that do not support RFC2833. To allow for this, if a key presses is indicate from the extension, the IP Office temporarily switches the call back to indirect media. It then injects the digits in-band using the negotiated dynamic payload and, after fifteen seconds of no further key presses, the call is switched back to direct media.

Related links

SIP messaging on page 950

Fax over SIP

T.38 Fax over SIP is supported on the IP500 V2 platform deployed as standalone or as an expansion gateway. G.711 fax is also supported, and is supported on Linux servers. For networks that do or do not support T.38, IP Office allows both G3 and Super G3 fax machines to interoperate.

There are configuration parameters that control the behavior in different networks. If T.38 is supported in a network, then it may make sense to select T.38 as the Fax Transport preference in order to make use the inherent quality provided by the redundancy mechanisms. On the other hand, if all of the fax machines in the network are Super G3 capable, there may be a need to take advantage of the increased speed that this encoding provides. Since T.38 is not capable of encoding Super G3, G.711 may be a better choice for the Fax Transport. In either case, IP Office will accept codec change requests from the far SIP endpoint to switch to T.38 or to G.711.

T.38 Fax Transport and Direct Media are mutually exclusive on a given SIP Line. IP Office keeps itself in the media path so that it can detect fax tones to make the switch to T.38.

Related links

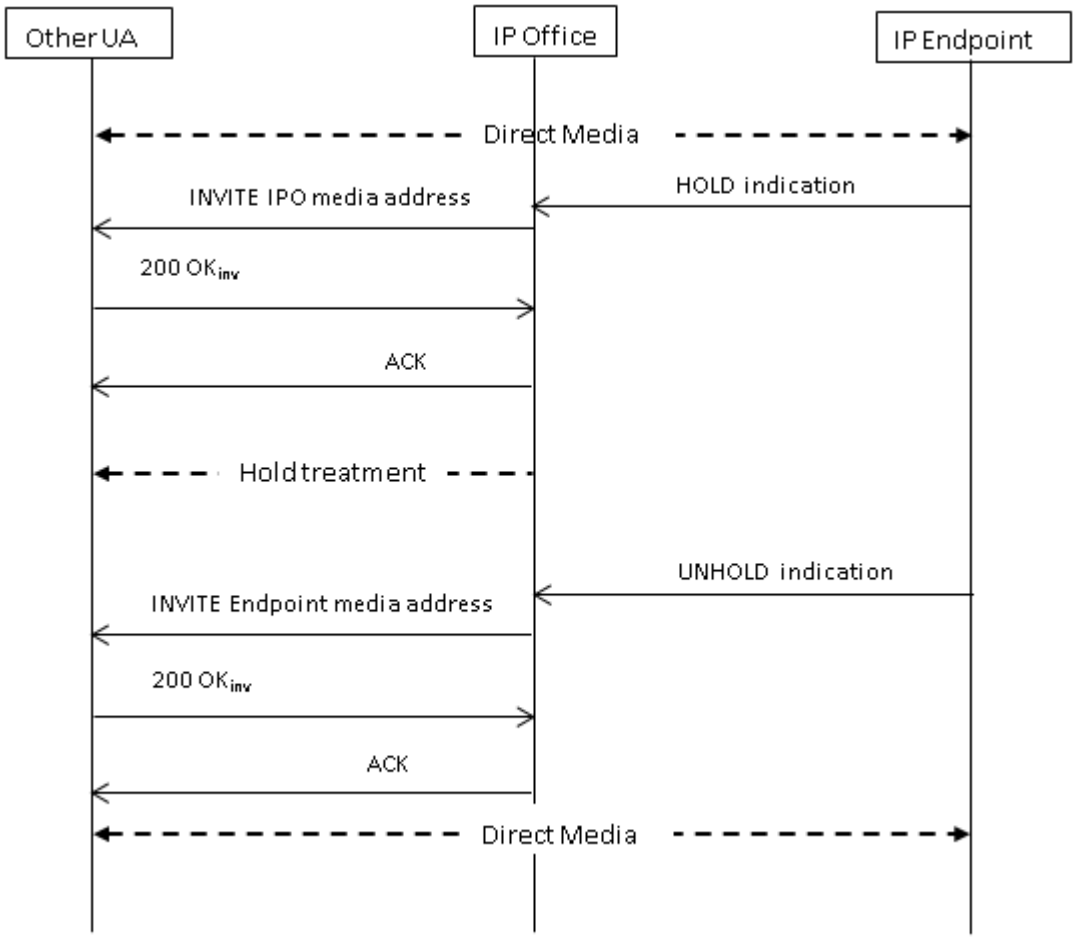
SIP messaging on page 950

SIP Call Hold Scenarios

Hold originated by IP Office

When an IP Office DS extension or non-IP trunk puts a SIP trunk on hold, there is no indication to the network. The voice path is merely switched in the TDM domain to the appropriate hold treatment source (tones, silence or music).

For IP extensions and trunks, be they H.323 or SIP, if the call uses direct media, there will be a re-INVITE sent to redirect the media source from the extension or trunk endpoint to a port on the IP Office in order to connect hold treatment. When the call is then unheld, another `INVITE` will go out to connect the extension with the far end.



Hold originated by far end

The far end of a SIP trunk can put the IP Office call on hold by sending it an re-`INVITE` with an `SDP Offer` containing:

- A **sendonly** attribute. IP Office replies with an `SDP Answer` containing the **recvonly** attribute.
- An **inactive** attribute. IP Office replies with **inactive**.
- A zero media connection address (c=0.0.0.0). IP Office replies with **inactive**.

Unhold

A held call is unheld by means of an `SDP Offer` with the **sendrecv** attribute (or no direction attribute, since **sendrecv** is assumed if not specified).

Unhold from mutual hold

Either end can unhold the other end by sending a new `Offer` with the **sendrecv** or **recvonly**attribute. The other end replies with **sendonly** if the call is still on hold at its end.

Related links

SIP messaging on page 950

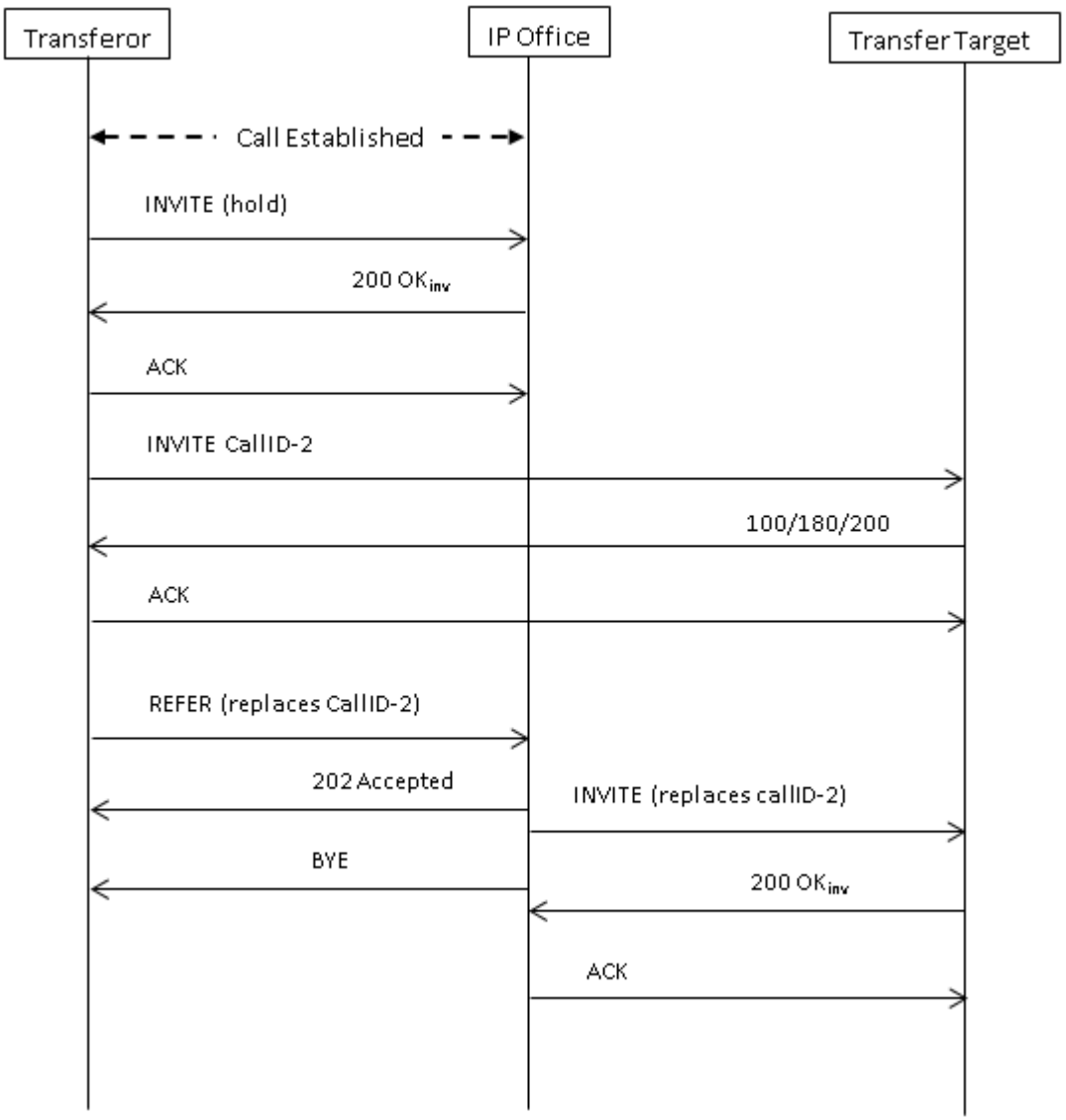
SIP Call Transfers (Refer)

After a SIP call has been established, the `SIP REFER` method is used by the transferor end of the call to transfer the transferee end to a the transfer target. The `REFER` message provides the transfer target's contact information in a `Refer-To` header. That information is used to establish complete the transfer.

For public SIP trunks, IP Office supports only consultative call transfer using `REFER`. Consultative transfers are also known as attended or supervised transfers. With consultative transfer, the transferor puts the first call on hold and establishes a consultation call to the transfer target. After the consultation call, the transferor completes the transfer, causing the transferee to connect to the transfer target, replacing the transferor.

`REFER` can be configured to accept incoming, reject incoming, or decide based on the presence of `REFER` in the **Allow:** header in responses to `OPTIONS` messages. Similarly, there is the same configuration for outgoing `REFER`.

Although the transferor and transferee must be SIP endpoints, the transfer target can be a TDM, PRI, H.323 or SIP terminal on the same IP Office, or an endpoint reachable over the same SIP line as the `REFER` request is received from.



Related links

SIP messaging on page 950

Ringback Tone

The ringback tone behavior of IP Office systems has changed for IP Office R11.0 and higher.

After sending an `INVITE` request, if the IP Office receives an `18X` response with SDP, it starts playing remote ringback tone. Prior to R11.0, if it then receives an 18X response without SDP, the IP Office would continue playing remote ringback tone. For R11.0 and higher, following the 18X without SDP, the IP Office now switches to local ringback tone.

In summary:

1. The IP Office sends an `INVITE`.
2. The IP Office receives `18X` with SDP. The IP Office plays remote ringback tone.
3. The IP Office receives `18X` without SDP:
   - **Pre-R11.0:** Continue playing remote ringback tone.
   - **R11.0+:** Switch to playing local ringback tone.

This feature is supported regardless of whether provisional response reliability (PRACK/100rel) is enabled or not.

When SIP call signaling transitions from remote to local ringback, the IP Office hosting the SIP trunk play the local ringback tone to the other end (phone or trunk).

Ringback Tone with Early Media

A special case applies for SIP trunks configured to use `p-early-media`. For `18x` responses with or without SDP to be considered, a `p-early-media` header must be present in the response. If otherwise, the message is not considered with regards to early media (the system continues playing either local ringback or remote early media).

For example: The IP Office receives a `183` response with SDP and a `p-early-media` header with a `sendonly` or `sendrecv` parameter. The IP Office then receives a `183` response (with or without SDP):

- **Example 1:** If the response does not include a `p-early-media` header, the IP Office continues listening to the remote early media.
- **Example2:** If the response includes a `p-early-media` header with an inactive parameter, the IP Office switches to playing local ringback tone.

Related links

SIP messaging on page 950

Hold Reminders

For IP Office R11.0 and higher:

- For SIP phones, the IP Office only provides hold reminders to Avaya SIP phones.
- If the user is on the video call, there will be no reminder call.
- The IP Office supports direct media when using SRTP with 1100, 1200, J129, E129, B179 and H175.

Related links

SIP messaging on page 950

Chapter 99: SIP Line Appearances

The system can implement some degree of line appearance emulation on SIP trunks. Note the word 'emulation'.

Related links

SIP Line Appearance Incoming Call Routing on page 957
SIP Line Appearance Outgoing Call Routing on page 957
SIP Line Appearance User Button Programming on page 958

SIP Line Appearance Incoming Call Routing

The routing of incoming SIP calls, including SIP line appearances, is covered in SIP Incoming Call Routing on page 942. However, the following key points should be observed:

- Call matching to an incoming call route destination (or an extension match to the **Local URI** value) is still required. The call is rejected if that does not occur.
  - This is necessary to associate the call with a user or group whose settings (for example forwarding and voicemail) it follows until answered.
  - If the incoming call route destination is a user with a matching line appearance button for the call, then the additional private line features for a line appearance call are applied. See Line Appearance Buttons on page 1215.
- As normal, if the call is answered by the voicemail service, whilst it is indicated on line appearance buttons, they cannot be used to answer or bridge into the call.

Related links

SIP Line Appearances on page 957

SIP Line Appearance Outgoing Call Routing

The SIP line appearance entries can be access for outgoing calls in two ways:

Method	Description
Short Code Routing	If the **Line Group ID** of a **Dial** short code matches the **Outgoing Group ID** of the SIP line appearance entry, with available outgoing sessions, then that SIP line appearance can potentially be used as a match for outgoing SIP calls. See Outgoing SIP Call Routing on page 934. • SIP Line Appearances matches are used before SIP URI entries. • This allows the SIP line appearance entries to be used by any user routed to that short code. They do not need to have an programmed Line Appearance buttons available. • For users without programmed line appearance buttons to also receive calls from the SIP line appearance, they need to be targeted by its matching incoming call route.
Line Appearance Buttons	For users with **Line Appearance** buttons programmed to the particular Line Appearance ID numbers being used, they can initiate outgoing calls by pressing any idle line appearance button (pressing a button that is in use, will potentially bridge into that call unless it is connected to voicemail). • The users dialing is still processed through short code matching. This allows normal short code manipulation of the outgoing number and/or barring of selected numbers. • The short code used to route calls to a SIP Line should use a ; (semi-colon) character at the end of the short code field. That character instructions the system to wait for dialing to be completed before using the short code. Dialing complete is indicated by either: - the dialer pressing #. - the device/application being used sending a dialing complete signal. - the system's **Dial Delay Time** expiring. • In this scenario, the **Line Group ID** of the short code needs to match the **Outgoing Group** of the SIP line appearance entry.

Related links

SIP Line Appearances on page 957

SIP Line Appearance User Button Programming

Line appearances buttons for SIP line appearances are programmed in the same way as for any type of line appearance. However, the following additional requirement applies:

- Users with line appearance buttons for a particular SIP Line appearance entry must be assigned buttons for all line appearance numbers allocated to that entry. By default that is 3 line appearance numbers.

Related links

SIP Line Appearances on page 957

Chapter 100: SIP Calling Number Verification (STIR/SHAKEN)

Calling number verification is a SIP feature where the calling number is verified by the ISP and the results of that verification is included with the incoming call. The aim of this is to help reduce call spoofing.

- Support for and use of SIP calling number verification is mandated by law for US/Canadian locales. However, the feature can be enabled in any locale if supported by the local SIP ISP.
- This feature only does calling number verification. The display name information supplied with calls is not verified.

Verification is done by the ITSP by looking at several factors:

- Is the calling number associated with the subscriber making the call?
- Is the call coming from a known customer?
- Is the call originated by the known ITSP?
- Was the call digitally signed and was the ITSP able to fetch the public certificate of the originating service provider in order to verify that the `SIP INVITE` has not be changed during transit.

The result of the verification process is then indicated in the call's headers using a `verstat` value:

- `TN-Validation-Passed` plus an attestation level (see the table below). For example, `TN-Validation-Passed-A`.
- `TN-Validation-Failed` plus an attestation level (see the table below). For example, `TN-Validation-Failed-A`.
- `No-TN-Validation` -

The attestation levels are:

Attestation Level		Description
A	**Full Attestation**	The customer is known and the calling number is one associated with that customer. • Note that for calls where no authentication level is indicated or can be obtained, the IP Office treats the call as attestation level A.

Table continues…

Attestation Level		Description
B	**Partial Attestation**	The customer is known. However, the number not one associated with that customer. For example: • the customer is forwarding a call from with a original calling number that is not associated with them. • the call is originating from another known ITSP. Common for international calls.
C	**Gateway Attestation**	The call has come via a trusted source, but the original customer and number are not known.

When calling number verification is available, the IP Office system can use the results to determine how to handle calls.

- Use of calling number verification is enabled on a per line basis.
- On lines where it is enabled, the line can either use the system default settings or line specific settings
- The settings determine whether a call should accepted or not.
  - If not accepted, the call is rejected by the system with a `666` response code.
  - If accepted, the call is routed as normal by features such as **Incoming Call Route** matching. However, if required, the specific result of the calling number verification can be used to vary the routing.
- The attestation level is included in the call's SMDR record. That includes rejected calls.

Related links

[The STIR/SHAKEN SIP Protocols](#) on page 960
[Obtaining a call's number verification result](#) on page 961
[Setting the system's number verification default behavior](#) on page 961
[Enabling calling number verification on a SIP line](#) on page 962
[SIP Calling Number Verification (STIR/SHAKEN)](#) on page 963
[Changing the rejected call responses](#) on page 965
[Changing the authentication header used](#) on page 965
[Customizing the call handling behavior](#) on page 966
[Call Records](#) on page 966

The STIR/SHAKEN SIP Protocols

Calling number verification is implemented by ITSPs using a number of SIP RFCs, collectively referred to as STIR/SHAKEN.

- **STIR** *(Secure Telephony Identity Revisited)*
  - This protocol uses digital certificates between the customer (the call originator) and the ITSP to establish customer authentication. The ISP can then examine known numbers allocated to that customer for number authentication.

- **SHAKEN** *(Signature-base Handling of Asserted information using toKENs)*
  - These are guidelines for PSTN network providers handling calls which transit from the non-SIP PSTN to SIP networks. Currently, it has mainly been implemented as a service for SS7 carriers in USA and Canada.

For more details, refer to https://en.wikipedia.org/wiki/STIR/SHAKEN.

Related links

SIP Calling Number Verification (STIR/SHAKEN) on page 959

Obtaining a call's number verification result

The methods implemented by different ITSPs to send a call's number verification can vary. The method used by IP Office to obtain the result is as follows:

- The IP Office looks for a `verstat` parameter in the `tel` or `sip uri` included in the call's **From** or **PAI** header. If both are present, preference is given to the **PAI** header. For example:
  - `PAI: tel:+123456789;verstat=TN-Validation-Passed-A`
  - `PAI: sip:+123456789;verstat=TN-Validation-Passed-A@foo.com;user=phone`
- The `verstat` parameter is used even if associated with an anonymous `sip/sips URI`.
- If there are multiple **PAI** headers with `verstat` information, only the first one is used.
- The attestation level is taken from the `verstat` parameter if it contains one of the recognized authentication levels `A`, `B` and `C`.
- If the `verstat` parameter is not available, the IP Office checks whether the level is available in any other headers such as **Attestation-Info** (used by ASBCE) or **X-Attestation-Info** (used by Verizon).
- The checking of further headers can also be enabled. See Changing the authentication header used on page 965.
- If no header provides an attestation level, level `A` is assumed.

Related links

SIP Calling Number Verification (STIR/SHAKEN) on page 959

Setting the system's number verification default behavior

This process sets the default behaviors applied by SIP lines on which calling number verification is enabled.

Procedure

1. Access the **System** > **VoIP** > **VoIP Security** settings.
2. In the **Calling Number Verification** section, set the required behavior:

Field	Description
Incoming Calls Handling	Default = **Allow Not Failed** Sets the defaults for which calls are accepted by the system based on the authentication level of the call. This default can be overridden in the individual line configuration. • **Allow All** - Allow all calls regardless of calling number verification. • **Allow Validated** - Only accept verified calls with full or partial attestation. • **Allow Not Failed** - Accept all calls expect those that specifically failed verification. Note this can include calls with no reported verification result.
Validation Presentation	Default = Off If enabled, the system will prefix the caller ID information displayed on phones with a character indicating the result of the call's validation result. This will be: • A tick mark for full verification. • A question mark for partial verification. • A cross for authentication failed. When enabled, the system will also inspect the display information on all received trunk calls to ensure they do not start with these characters in order to avoid spoofing.

3. Save the settings.

Next steps

- Enable calling number validation on the individual SIP lines. See Enabling calling number verification on a SIP line on page 962.

Related links

SIP Calling Number Verification (STIR/SHAKEN) on page 959

Enabling calling number verification on a SIP line

This process configures the SIP line specific settings for calling number verification.

Procedure

1. Access the SIP line's settings and select the **SIP Advanced** tab.
2. In the **Calling Number Verification** section, set the required behavior:

Field	Description
Calling Number Verification	Default = Off Sets whether the line uses calling number verification.
Incoming Calls Handling	Default = **Allow Not Failed** Set which calls are accepted by the system based on the attestation level of the call. • **System** - Use the default system setting (**System VoIP** > **VoIP Security** > **Callng Number Verification**). • **Allow All** - Allow all calls regardless of calling number verification. • **Allow Validated** - Only accept verified calls with full or partial attestation. • **Allow Not Failed** - Accept all calls expect those that specifically failed verification. Note this can include calls with no reported verification result.

3. Save the changes.

Related links

SIP Calling Number Verification (STIR/SHAKEN) on page 959

SIP Calling Number Verification (STIR/SHAKEN)

For calls with are allowed following calling number verification, normal incoming call routing is applied. However, that routing can be made to be specific to the verification result and attestation level of the call.

This is achieved using the following characters in the **Code** field of short codes or **Incoming CLI** field of incoming call routes:

Character	Meaning	Description
P	**Passed**	Matches calls where the `verstat` value is set to `TN-Validation-Passed` plus the attestation level. For example, `TN-Validation-Passed-A`. If required, the specific level of attestation to match can be specified. That is done by following the **P** character with the required level or levels inside " " marks. For example: • `P"A"` matches calls with an attestation of A. • `P"B"` matches calls with an attestation of B. • `P"AB"` matches calls with an attestation of A or B.
F	**Failed**	Matches calls that specifically failed verification. That is, the call's `verstat` value is set to `TN-Validation-Failed`.
Q	**Unknown**	Matches calls which do not have any verification result or where the `verstat` value received is `No-TN-Validation`.

Example Incoming Call Routing

In this example, the system has the following incoming call routes are defined for calls to the business's main sales number. Apart from the setting below, each of the incoming call routes has the same settings and matches the incoming group ID used by the SIP trunks URI.

Incoming Call Route	Incoming CLI	Destination	Description
1.	`P"A"`	Hunt Group	The business's sales hunt group.
2.	*blank*	Auto-Attendant	The business's auto-attendant. The use of an auto-attendant to answer calls deflects automated calls with potential spoofed caller ID numbers but still allows callers to select to be connected to the sales group via the provided auto-attendant options.
3.	`P"B"`	Auto-Attendant	
4.	`Q`	Auto-Attendant	
5.	`F`	Barred	A short code set to the barred feature.

The following calls to the sales number are received:

Incoming Call Details	Incoming CLI	Attestation Level	Destination
1.	111	A	A fully validated call. The call details match the 2nd call route only. Therefore, the call is routed the sales hunt group.
2.	222	B	A partially validated call. The call details match both the 2nd and 3nd call routes. However, the 3rd match is more precise, so the call is routed to the auto-attendant.
3.	333	C	The call details match both the 2nd and 5th call routes. However, the 5th match is more precise, so the call is routed to the barred short code.
4.	444	None	A call with no attestation level. The call details match the 2nd and 4th call routes. However, the 3rd match is more precise, so the call is routed to the auto-attendant.

Calling Name Display

Calling number validation only validates the caller's number, not the display name information provided with the call.

Related links

SIP Calling Number Verification (STIR/SHAKEN) on page 959

Changing the rejected call responses

For rejected calls, by default the rejection is done using the response code 666 and the string "Unwanted". However, if required by the ISP, a different code and/or string can be used, configured using the process below.

- Rejected calls are included in the system's SMDR and CDR outputs.
- Rejected calls are not included in the individual user's call logs and call histories.

Procedure

1. Open the SIP line's settings and select **SIP Engineering**.
2. Click **Add** and enter one of the following custom strings:
   - To change the reject code, enter SLIC_STIR_REJECT_CODE=N where N is the response code number to use.
   - To change the reject string, enter SLIC_STIR_REJECT_STRING=Y where Y is the string to use.
3. Click **Create new**.
4. Save the settings.

Related links

SIP Calling Number Verification (STIR/SHAKEN) on page 959

Changing the authentication header used

Obtaining a call's number verification result on page 961 describes the normal process by which the IP Office system normally obtains a call's verification result from its headers. However, if required, the IP Office can look for the verstat value in another specified header.

- As per normal operation, if verstat values are present in more than one header, only the first is used.

Procedure

1. Open the SIP line's settings and select **SIP Engineering**.
2. Click **Add** and enter one of the following custom strings:
   - To specify the header to check, enter SLIC_STIR_ATTEST="W" where W is the name of the header used by the ITSP.
     - For example, SLIC_STIR_ATTEST="X-StirResult" instructs the IP Office to also check for a value in the X-StirResult header if present. .
3. Click **Create new**.

4. Save the settings.

Related links

SIP Calling Number Verification (STIR/SHAKEN) on page 959

Customizing the call handling behavior

The behavior applied to calls can be customized. This is done on a per-line basis, using the decimal sum of a binary bit string, where bit 0 is least significant bit (right-to-left).

The custom behavior provided by each bit when enabled (set to 1) are:

Bit	Attestation Level	Custom Behavior if bit set to 1
0	Attestation Passed Calls (A and B)	Retain the Caller ID display.
1		Perform directory matching.
2	No Attestation Calls (Assumed A)	Retain the Caller ID display.
3		Perform directory matching.
4	Attestation Failed Calls (C)	Retain the Caller ID display
5		Perform directory matching.

Procedure

1. Open the SIP line's settings and select **SIP Engineering**.
2. Click **Add** and enter one of the following custom strings:
   - To change the reject code, enter `SLIC_STIR_CUSTOM=Z` where `Z` is the decimal sum of the binary bits.
     - For example, `SLIC_STIR_CUSTOM=15` retains the caller ID display and does directory matching for all calls expect those that have attestation level C. That is, bits 0 to 3 all set to 1, bits 4 and 5 set to 0. The decimal sum of that bit string is 15.
3. Click **Create new**.
4. Save the settings.

Related links

SIP Calling Number Verification (STIR/SHAKEN) on page 959

Call Records

The authentication level (`A`, `B` or `C`) provided by the ISP is included in the SMDR call logging records output by the system. If no authentication level is provided, `N/A` is shown instead.

An SMDR call record is produced even for calls which are rejected by the system based on the calling number verification settings.

Related links

SIP Calling Number Verification (STIR/SHAKEN) on page 959

Chapter 101: IP Office SIP trunk specifications

This section outlines the SIP trunk capabilities supported by IP Office.

Related links

SIP RFCs on page 968
Transport protocols on page 970
Request methods on page 970
Response methods on page 971
Headers on page 971

SIP RFCs

IP Office supports the following SIP RFCs:

RFC	Title
–	*ITU-T T.38 Annex D, Procedures for real-time Group 3 facsimile communication over IP networks*
1889	*RTP: A Transport Protocol for Real-Time Applications*
2327	*SDP: Session Description Protocol*
2617	*HTTP Authentication: Basic and Digest Access Authentication*
2833	*RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*
2976	*The SIP INFO Method*
3087	*Control of Service Context using SIP Request-URI*
3261	*Session Initiation Protocol*
3262	*Reliability of Provisional Responses in the Session Initiation Protocol (SIP)*
3263	*Session Initiation Protocol (SIP): Locating SIP Servers*
3264	*An Offer/Answer Model with the Session Description Protocol (SDP)*
3311	*The Session Initiation Protocol (SIP) UPDATE Method*
3323	*A Privacy Mechanism for the Session Initiation Protocol (SIP)*

Table continues…

RFC	Title
3325	*Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted*
3326	*The Reason Header Field for the Session Initiation Protocol (SIP)*
3329	*Security Mechanism Agreement for the Session Initiation Protocol (SIP)*
3388	*Grouping of Media Lines in the Session Description Protocol (SDP) in the Session Initiation Protocol (SIP)* (R12.1+ IPv6)
3398	*Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping*
3407	*Session Description Protocol (SDP) Simple Capability*
3489	*STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*
3515	*The Session Initiation Protocol (SIP) Refer method*
3550	*RTP: A Transport Protocol for Real-Time Applications*
3551	*RTP Profile for Audio and Video Conferences with Minimal Control*
3665	*Session Initiation Protocol Basic Call Flow Examples*
3666	*Session Initiation Protocol PSTN Call Flows*
3725	*Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)*
3824	*Using E.164 numbers with the Session Initiation Protocol (SIP)*
3842	*A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol*
3891	*The Session Initiation Protocol (SIP) "Replaces" Header*
3960	*Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)*
4028	*Session Timers in the Session Initiation Protocol (SIP)*
4091	*The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework* (R12.1+ IPv6)
4092	*Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics* (R12.1+ IPv6)
4119	*A Presence-based GEOPRIV Location Object Format*
4566	*SDP: Session Description Protocol*
4733	*RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*
5139	*Revised Civic Location Format for Presence Information Data Format Location Object*
5359	*Session Initiation Protocol Service Examples*
5373	*Requesting Answering Modes for the Session Initiation Protocol*
5379	*Guidelines for Using the Privacy Mechanism for SIP*
5806	*Diversion Indication in SIP*
5876	*Updates to Asserted Identity in the Session Initiation Protocol (SIP)*
5922	*Domain Certificates in the Session Initiation Protocol (SIP)*
6337	*Session Initiation Protocol (SIP) Usage of the Offer/Answer Model*

Table continues…

RFC	Title
6432	*Carrying Q.850 Codes in Reason Header Fields in SIP (Session Initiation Protocol) Responses*
8224	*Authenticated Identity Management in the Session Initiation Protocol (SIP)*
8225	*PASSporT: Personal Assertion Token*
8226	*Secure Telephone Identity Credentials: Certificates*
8588	*Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN)*

Related links

IP Office SIP trunk specifications on page 968

Transport protocols

- UDP
- TCP
- RTP
- RTCP

Related links

IP Office SIP trunk specifications on page 968

Request methods

- INVITE
- ACK
- BYE
- CANCEL
- INFO
- REFER
- REGISTER
- SUBSCRIBE
- NOTIFY
- PRACK
- OPTIONS
- UPDATE
- PUBLISH
- MESSAGE
- PING

Related links

IP Office SIP trunk specifications on page 968

Response methods

- 100 Trying
- 180 Ringing
- 181 Call Is Being Forwarded
- 182 Call Queued
- 183 Session progress
- 200 OK
- 202 ACCEPTED
- 3XX
- 4XX
- 5XX
- 6XX

Related links

IP Office SIP trunk specifications on page 968

Headers

- Accept
- Alert-Info
- Allow
- Allow-Event
- Authorization
- Call-ID
- Contact
- Content-Length
- Content-Type
- CSeq
- Diversion
- From
- History-Info
- Max-Forwards
- P-Asserted-Identity
- P-Early-Media
- P-Preferred-Identity
- Privacy
- Proxy-Authenticate
- Proxy-Authorization
- Proxy-Require
- Require
- Remote-Party-ID
- Server
- Session-Timers
- Supported
- To
- User-Agent
- Via
- WWW-Authenticate

Additional Information

- The IP Office supports `Call-ID` headers of up to 256 characters.
- For IP Office R11.1 FP2 SP3 and higher, the maximum length of the `tag` element in `From` and `To` headers has increased to 150 characters (previously 80 characters).

Related links

IP Office SIP trunk specifications on page 968

Part 13: Short Codes

Chapter 102: Short Code Overview

Whenever the system receives a set of digits to process, if those digits do not match a user or group extension number, the system will look for a short code match. The matching short code then defines what action (short code feature) should be applied to the call, where it should be routed and which of the dialed digits, if any, should be used in the subsequent action.

This applies to digits dialed by a telephone user, sent by a user selecting a directory contact or speed dial, and in some cases to digits received with an incoming call on a line.

This section provides an overview of short codes configuration and use.

⚠ Warning:

- The dialing of emergency numbers must not be blocked. Whenever short codes are edited, you must ensure that the ability of users to dial emergency numbers is tested and maintained. See Configuration for Emergency Calls on page 772.

Short Code Fields

Each short code has the following fields:

- **Short Code:** The digits which, if proved to be a best match to the dialed digits, trigger use of the short code. In addition to the normal dialing digits (0 to 9 plus * and #), characters can also be used as follows:
  - Some characters have special meaning. For example, the wildcard **X** to match any single digit or **N** to match any set of digits. See Short Code Characters on page 975
  - Using characters also allows the creation of short codes which cannot be dialed from a phone but can be dialed from some applications.
- **Telephone Number:** The number used by the short code feature if needed, for example the outgoing number for a call to be passed to an external telephone line. Again special characters can be used in this field, see Short Code Characters on page 975.
- **Line Group ID:** This field is used for short codes that result in a number to be dialed, that is any short code set to one of the various **Dial** short code features. When that is the case, this field specifies the outgoing line group or ARS form to be used for the call.
  - For **Dial Emergency** short codes, this is overridden by the **Emergency ARS** setting of the extension's **Location** if configured.
- **Feature:** This sets the action to performed by the short code. See Short Code Features on page 993.
- **Locale:** Features that transfer the call to voicemail indicate the language required. If the required set of language prompts is not available, the voicemail system will fallback to another appropriate language if possible (refer to the appropriate voicemail installation manual for

details). The locale sent to the voicemail server by the system is determined in the following order of priority:

1. **Short Code Locale**: The short code locale, if set, is used if the call is routed to voicemail using the short code.
2. **Incoming Call Route Locale**: The incoming call route locale, if set, is used if caller is external.
3. **User Locale**: The user locale, if set, is used if the caller is internal.
4. **System Locale**: If no user or incoming call route locale is set, the system locale is used unless overridden by a short code locale. Systems using Embedded Voicemail, if the required set of upgraded language prompts to match the locale is not present on the system SD card, Manager will display an error. The required prompt set can be uploaded from Manager using the Add/Display VM Locales option.

- **Force Account Code:** When selected, if the short code results in the dialing of an external number, the user is prompted to enter a valid account code before the call is allowed to continue. See Account Code Configuration on page 840.
- **Force Authorization Code:** When selected, if the short results in the dialing of an external number, the user is prompted to enter a valid authorization code before the call is allowed to continue. See Configuring authorization codes on page 823.

Short Code Descriptions

The short method for describing short codes in this manual, for example **9N/Dial/./0**, indicates the settings of main short code fields, each separated by a **/** as follows:

- **Code:** In this case **9N**.
- **Feature:** In this case **Dial**.
- **Telephone Number:** In this case the symbol **.** representing all dialed digits.
- **Line Group ID:** In this case the call is sent to outgoing line group **0**.

Example Short Codes

- ***17/VoicemailCollect/?U** A user dialing ***17** is connected to their own mailbox to collect messages.
- ***14*N#/FollowMeTo/N** If a user dials ***14*210#** at their own extension, their calls are redirected to extension 210.

Types of Short Code

In addition to different short code features, there are different types of short code:

- **Dialing Short Codes:** The following types of short code applied to on-switch dialing. The result may be an action to be performed by the system, a change to the user's settings or a number to be dialed. The order below is the order of priority in which they are used when applied to user dialing.
  - **User Short Codes:** These are usable by the specific user only. User short codes are applied to numbers dialled by that user and to calls forwarded via the user.
  - **User Rights Short Codes:** These are usable by any users associated with the user rights in which they are set. User Rights short codes are only applied to numbers dialed by that user. For example they are not applied to calls forwarded via the user.

  - **System Short Codes:** These are available to all users on the system. They can be overridden by user or user rights short codes.
- **Post-Dialing Short Codes:** When any the short code above result in a number to be dialed, further short code can be applied to that number to be dialed. This is done using the following types of short codes.
  - **ARS (Alternate Route Selection) Short Codes:** The short code that matches dialing can specify that the resulting number should be passed to an ARS form. The ARS form can specify which routes should be used for the call by using further short code matches and also provide option to use other ARS forms based on other factors such as time and availability of routes.
  - **Transit Network Selection (TNS) Short Codes:** Used on T1 ISDN trunks set to use AT&T as the Provider. Applied to the digits presented following any other short code processing.
- **Incoming Number Short Codes:** On certain types of trunks short codes can be applied to the incoming digits received with calls.
  - **Line Short Codes:** These short codes are used to translate incoming digits received with calls. The stage at which they are applied varies between different line types and may be overridden by an extension number match.

Related links

Short Code Characters on page 975
User Dialing on page 980
Application Dialing on page 982
Secondary Dial Tone on page 982
? Short Codes on page 984
Short Code Matching Examples on page 984
Default System Short Code List on page 987

Short Code Characters

The short code fields **Short Code** and **Telephone Number** can contain the normal dialable digits *, # and 0 to 9. In addition they can also use a range of special characters as listed below.

Short Code Field Characters

	Description
?	**Default Match** This character can be used on its own to create a short code match in the absence of any other short code match.
?D	**Default Number Dialing** This character combination makes a call to the defined phone number as soon as the user goes off-hook.

Table continues…

	Description
?D(t)	**Default Number Dialing Timeout** The character x represents time in seconds. If a phone is off-hook or speaker is enabled and no number is dialed for **t** seconds, the phone makes a call to the defined phone number. A maximum of 30 seconds is used for **t** though system accepts values more than 30 on the interface.
F	**Failed Authentication** Match incoming SIP calls which failed authentication. See SIP Calling Number Verification (STIR/SHAKEN) on page 963.
N	**Match Any Digits** Matches any dialed digits (including none). The **Dial Delay Time** or a following matching character is used to resolve when dialing is complete.
P	**Authenticated** Match incoming SIP calls which were authenticated. The character can be followed by the required attestation level or levels in " " quote marks. See SIP Calling Number Verification (STIR/SHAKEN) on page 963.
Q	**Unauthenticated** Match incoming SIP calls which were not authenticated. See SIP Calling Number Verification (STIR/SHAKEN) on page 963.
X	**Match a Digit** Matches a single digit. When a group of X's is used, the short code matches against the total number of X's.
[ ]	**Secondary Dial Tone Trigger** For pre-4.0 IP Office systems used to trigger secondary dial tone. Not used for Release 4.0+. See Secondary Dial Tone on page 982.
;	**Receive Sending Complete** When used this must be the last character in the short code string. • If the **Dial Delay Count** is **0**, a **;** instructs the system to wait for the number to be fully dialed, using the **Dial Delay Time** or the user dialing #, to indicate completion and then acting on the short code. • If the **Dial Delay Count** is not zero, the dialing is only evaluated when **#** is pressed. The majority of North-American telephony services use en-bloc dialing. Therefore the use of a ; is recommended at the end of all dialing short codes that use an N before routing those calls to a trunk or ARS. This is also recommended for all dialing where secondary dial tone short codes are being used.

Telephone Number Field Characters

	Description
A	**Allow Outgoing CLI** Allow the calling party number sent with the call to be used. This character may be required by service providers in some locales.

Table continues…

	Description
C	**Use Called Number Field** Place any following digits in the outgoing call's Called number field rather than the Keypad field.
D	**Wait for Connect** Wait for a connect message before sending any following digits as DTMF.
E	**Extension Number** Replace with the extension number of the dialing user. Note that if a call is forwarded this will be replaced with the extension number of the forwarding user.
h	**Hold Music Source** When used as part of the short code telephone number field, this character allows the source for music on hold to be selected. Enter `h(X)` where **X** indicates the required hold music source if available. This overrides any previous hold music selection that may have been applied to the call. • For IP500 V2 systems, the value of **X** can be 1 to 4. • For systems on a Linux based server, the value of **X** can be 1 to 32. • When used with Park Call short codes, the **h(X)** should be entered before the park slot number part of the telephone number.
I	**Use Information Packet** Send data in an Information Packet rather than Set-up Packet.
K	**Use Keypad Field** Place any following digits in the outgoing call's Keypad field rather than the Called Number field. Only supported on ISDN and QSIG.
l	**Last Number Dialed** (lower case L) Use the last number dialed.
L	**Last Number Received** Use the last number received.
N	**Dialed Digit Wildcard Match** Substitute with the digits used for the **N** or **X** character match in the Short Code number field.

Table continues…

	Description
p	**Priority** The priority of a call is normally assigned by the Incoming Call Route or else is **1-Low** for all other calls. Dial Extn short codes can use **p(x)** as a suffix to the **Telephone Number** to change the priority of a call. Allowable values for **x** are **1**, **2** or **3** for low, medium or high priority respectively. In situations where calls are queued, high priority calls are placed before calls of a lower priority. This has a number of effects: • Mixing calls of different priority is not recommended for destinations where Voicemail Pro is being used to provided queue ETA and queue position messages to callers since those values will no longer be accurate when a higher priority call is placed into the queue. Note also that Voicemail Pro will not allow a value already announced to an existing caller to increase. • If the addition of a higher priority call causes the queue length to exceed the hunt group's Queue Length Limit, the limit is temporarily raised by 1. This means that calls already queued are not rerouted by the addition of a higher priority call into the queue.
r	**Ring Tone Plan** When used as part of the short code telephone number field, this character can specify a Ring Tone Plan number. Enter `r(X)` where **X** is 1 to 8 indicating the Ring Tone Plan number to use.
S	**Calling Number** Place any following digits into the outgoing call's calling number field. Using **S** does not alter any allow or withhold CLI setting associated with the call, the short code characters **A** or **W** should be used respectively. • On mobile twinned calls, if the original party information is used or a specific calling party information CLI is set, that number overrides setting the outgoing CLI using short codes. • Note that for SIP trunks, the SIP URI configuration options override this setting. **Warning:** • Changing the outgoing CLI for calls requires the line provider to support that function. You must consult with your line provider before attempting to change the outgoing CLI, failure to do so may result in loss of service. If changing the outgoing CLI is allowed, most line providers require that the outgoing CLI used matches a number valid for return calls on the same trunks. Use of any other number may cause calls to be dropped or the outgoing CLI to be replaced with a valid number. On mobile twinned calls, if the original party information is used or a specific calling party information CLI is set, that number overrides setting the outgoing CLI using short codes.
SS	**Pass Through Calling Number** Pass through the Calling Party Number. For example, to provide the incoming ICLID at the far end of a VoIP connection, a short code **?** with telephone number **.SS** should be added to the IP line.
i	**National** Both the **S** and **SS** characters can be followed by an **i**, that is **Si** and **SSi**. Doing this sets the calling party number plan to ISDN and number type to National. This may be required for some network providers.

Table continues…

	Description
t	**Allowed Call Duration** Set the maximum duration in minutes for a call plus or minus a minute. Follow the character with the number of minutes in brackets, for example **t(5)**.
U	**User Name** Replace with the User Name of the dialing user. Used with voicemail.
W	**Withhold Outgoing CLI** Withhold the sending of calling ID number. Operation is service provider dependent.
Y	**Wait for Call Progress Message** Wait for a Call Progress or Call Proceeding message before sending any following digits as DTMF. For example, the Y character would be necessary at a site where they have signed up with their telephone service provider to withhold international dialing until a DTMF pin/account number is entered that initiates the call progress/proceeding message.
Z	**Calling Party Name** This option can be used with trunks that support the sending of name information. The **Z** character should be followed by the name enclosed in **" "** quotation marks. Note that their may be name length restrictions that vary between line providers. The changing of name information on calls being forwarded or twinned may also not be supported by the line provider.
@	**Use Sub Address Field** Enter any following digits into the sub-address field.
.	**Dialed Digits** Replace with the full set of dialed digits that triggered the short code match.
,	**One Second Pause** Add a one second pause in DTMF dialing.
;	**Receive Sending Complete** When used this must be the last character in the short code string. If the **Dial Delay Count** is **0**, a **;** instructs the system to wait for the number to be fully dialed, using the **Dial Delay Time** or the user dialing #, to indicate completion and then acting on the short code. If the **Dial Delay Count** is not zero, the dialing is only evaluated when **#** is pressed.
" "	**Non-Short Code Characters** Use to enclose any characters that should not be interpreted by the IP Office as possible short code special characters. For example, characters being passed to the voicemail server for interpretation there. • Ensure you use straight quotation marks like "…" when entering short codes into the IP Office configuration. Various editing, publishing and copying tools often replace those with angled or smart-quotes such as ‟…‟.

Related links

Short Code Overview on page 973

User Dialing

The following rules are used when short code matching is performed for user dialing:

- A short code is used immediately an exact match is found unless followed by a **;** semi-colon.
  - If a ; semi-colon is present, dialing complete can be indicated by the user pressing # or the **Dial Delay Time** (see below) expiring.
- If no match is found but partial matches exist, the user can continue dialing.
- If no match or partial matches are found, incompatible is returned.
- The following precedence is used to determine which short codes are used:
  - Extension number matches override all short codes.
  - User short codes override user rights and system short codes.
  - User Rights short code matches override system short codes.
- When multiple exact matches exist:
  - The match with the most specified digits rather than wildcards is used.
  - If there are still more than one match, the match with the most exact length is used. This means X single-digit wildcards will override N multiple0digit wildcards when both match.
- The rules above are applied even if the number is dialed by selection from a directory or using any other method of stored number dialing.

User Digit Dialing Settings

The following system settings influence user dialing.

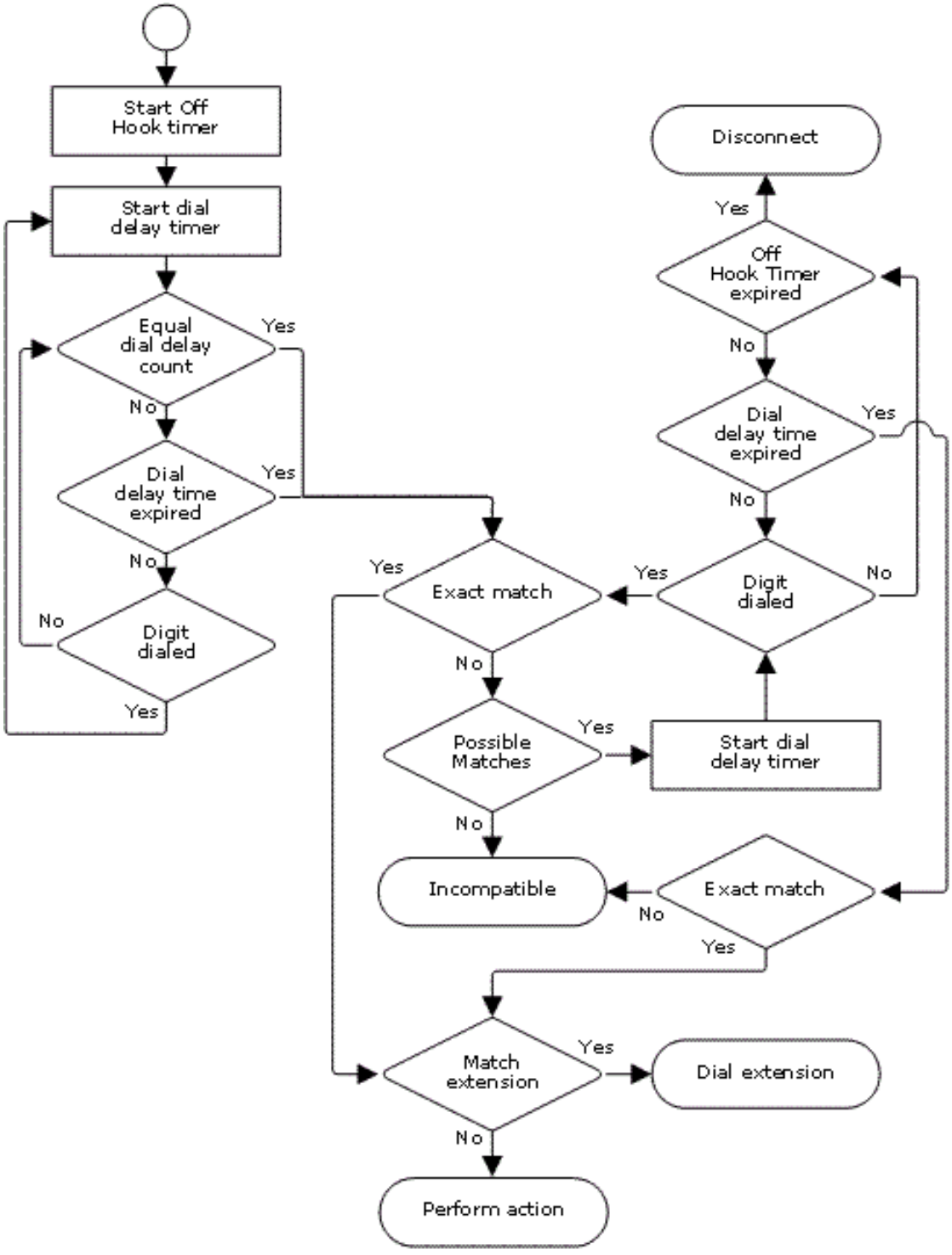
- **Dial Delay Count:** *Default = 0 (US/Japan), 4 (ROW).*

  This value sets the number of digits dialed before the system starts looking for short code matches.
- **Dial Delay Time:** *Default = 4 seconds (US/Japan), 1 second (ROW).*

  This value sets the maximum allowed interval between the dialing of each digit. If exceeded, the system treats dialing as completed and looks for a short code match even if the **Dial Delay Count** has not been reached.
- **Off-Hook Timer:**

  When a user goes off-hook, the system starts a 30 second off-hook timer (10 seconds in Italy). If the off-hook timer expires before a short code match occurs, the user is disconnected.

User Dialing Flowchart



Related links

Short Code Overview on page 973

Application Dialing

Numbers speed dialed by system applications such as SoftConsole are treated differently. Since the digits are received en bloc as a single group, they can override some short code matches. The same applies to short codes used within system configuration settings such as Incoming Call Route destinations.

Example:

- Telephone Number: 12345678
- Short Code 1: 1234XX/Dial/Extn/207
- Short Code 2: 12345678/Dial Extn/210

If dialed manually by the user, as soon as they have dialed 123456 a match to short code 1 occurs. They can never dial short code 2.

If dialed using an application, 12345678 is sent as a string and a match to short code 2 occurs.

Partial Dialing

If the application dialing does not trigger an exact match, the user can dial additional digits through their extension. The processes for normal user dialing are applied.

Non-Digit Short Codes

Short codes can be created that use alphabetic characters instead of numbers. While these short codes cannot be dialed from a phone, they can be dialed using application speed dials and settings. However characters that are interpreted as special short code characters will still be interpreted as such.

Related links

Short Code Overview on page 973

Secondary Dial Tone

Some locales prefer to provide users with secondary dial tone once they have started dialing external calls. This dial tone is heard by the user until they have completed dialing and a trunk is seized at which point call progress tones are provided by the trunk, or camp on/busy tone is provided by the system if the required trunk cannot be seized.

Release 4.0 and Higher

The use of secondary dial tone is provided through the **Secondary Dial Tone** check box option on the ARS form to which the call is routed. When on, this setting instructs the system to play secondary dial tone to the user.

The tone used is set as either **System Tone** (normal dial tone) or **Network Tone** (secondary dial tone). Both tone types are generated by the system in accordance with the system specific locale setting. Note that in some locales normal dial tone and secondary dial tone are the same.

When **Secondary Dial Tone** is selected, the ARS form will return tone until it receives digits with which it can begin short code matching. Those digits can be the result of user dialing or digits passed by the short code which invoked the ARS form. For example with the following system short codes:

In this example, the 9 is stripped from the dialed number and is not part of the telephone number passed to the ARS form. So in this case secondary dial tone is given until the user dials another digit or dialing times out.

- **Code**: 9N
- **Telephone Number**: N
- **Line Group ID**: 50 Main

In this example, the dialed 9 is included in the telephone number passed to the ARS form. This will inhibit the use of secondary dial tone even if secondary dial tone is selected on the ARS form.

- **Code**: 9N
- **Telephone Number**: 9N
- **Line Group ID**: 50 Main

Pre-4.0 IP Office Secondary Dial Tone

Pre-4.0 systems provided dial tone through the use of the short code feature Secondary Dial Tone and the [ ] special characters. For example, on a system where 9 is used as a prefix for external dialing, the system short code 9/./Secondary Dial Tone/0 will trigger secondary dial tone when users dial a number prefixed with 9. This method is not supported by Release 4.0 which provides ARS forms for the control of outgoing calls.

In order to allow further digit matching, the digits dialed are put back through short code matching against any short codes that start with [n] where n is the digit used to trigger the system secondary dial tone short code.

On all systems where secondary dial tone is used, a ; should also be used in dialing short codes that contain N.

For example:

System Short Codes

- 9/SecondaryDialTone/.
- [9]0N;/Dial/0

User Short Code

[9]0N;/Busy/0

The user dials 90114445551234. The 9 is matches the system secondary dial tone short code and unlike other short codes this is applied immediately. The user's dialing is put through short code matching again using the normal order of precedence but matched to possible short codes beginning [9]. In this case the user's [9]0N; short code would take precedence over the system [9]0N; short code.

Related links

Short Code Overview on page 973

? Short Codes

The ? character can be used in short codes in the following ways:

Default Short Code Matching:

? short codes are used in short code matching in the following way. If no user or system short code match is found, the system will then look for a ? short code match. It will look first for a user ? short code and then, if not found, a system ? short code.

Example: On systems outside North America, the system short code **?/Dial/./0** is added as a default short code. This short code provides a match for any dialing to which there is no other match. Therefore, on systems with this short code, the default is that any unrecognized number will be dialed to Outgoing Line Group 0.

Hot-Line Dialing:

A user short code **?D** can be used to perform a short code action immediately the user extension goes off-hook. This is supported with Dial type short code features. Typically it is used with door, lift and lobby phones to immediately connect the phone to a number such as the operator or reception.

Voicemail Collect Short Codes:

The ? character can appear in the **Telephone Number** field of a short code. This is done with short codes using the VoicemailCollect feature. In this instance the ? character is not interpreted by the system, it is used by the voicemail server.

Related links

Short Code Overview on page 973

Short Code Matching Examples

The following examples are not meant as practical examples. However they are simple to implement and test on real system without conflicting with its normal operation. They illustrate the interaction between different short codes in resolving which short code is an exact match. They assume that extension numbers are in the 200 to 299 range.

- The term 'dials' means dialing the indicated digit or digits without the inter-digit Dial Delay Time expiring.
- The term 'pause' means a wait that exceeds the inter-digit Dial Delay Time.

Scenario 1

- Short Code 1 = 60/Dial Extn/203
- Dial Delay Count = 0. Dial Delay Time = 4 seconds.

Test	Dialing	Effect
1	8	No possible match, incompatible returned immediately
2	6	No exact match but there is a potential match, so the system waits. When the Dial Delay Time expires, no exact match is found so incompatible is returned.
3	60	Exact match to Short Code 1. Extension 203 called immediately.
4	61	No possible match, the system returns incompatible.

Scenario 2

- Short Code 1 = 60/Dial Extn/203
- Short Code 2 = 601/Dial Extn/210
- Dial Delay Count = 0. Dial Delay Time = 4 seconds.

Test	Dialing	Effect
1	8	No possible match, incompatible returned immediately
2	60	Exact match to Short Code 1. Extension 203 called immediately.
3	601	Exact match to Short Code 1 as soon as the 0 is dialed. The user cannot manually dial 601.

Scenario 3

Short Code 1 = 60/Dial Extn/203

Short Code 2 = 601/Dial Extn/210

Dial Delay Count = 3. Dial Delay Time = 4 seconds.

Test	Dialing	Effect
1	8	Insufficient digits to trigger matching. The system waits for additional digits or for Dial Delay Time to expire. When Dial Delay Time expires, no possible match is found so incompatible is returned.
2	60	Insufficient digits to trigger matching. The system waits for additional digits or for Dial Delay Time to expire. When Dial Delay Time expires, matching started and exact match to Short Code 1 occurs. .
3	601	Third digit triggers matching. Exact match to Short Code 2. Extension 210 dialed immediately.
4	60#	# is treated as a digit and as the third digit triggers matching. No exact match found. The system returns incompatible.

Scenario 4

- Short Code 1 = 60;/Dial Extn/203
- Short Code 2 = 601/Dial Extn/210

- Dial Delay Count = 3. Dial Delay Time = 4 seconds.

Test	Dialing	Effect
1	8	Insufficient digits to trigger matching. The system waits for additional digits or for Dial Delay Time to expire. When Dial Delay Time expires, no possible match is found so incompatible is returned.
2	6	Insufficient digits to trigger matching. The system waits for additional digits or for the interdigit Dial Delay Time to expire. If the Dial Delay Time expires, a potential match exists to a short code that uses ; so the system waits for an additional digit until the off-hook timer expires.
3	60	As above but an additional digit now may create a match. If 1 is dialed, it creates an exact match to Short Code 2 and is used immediately. If 0, * or 2 to 9 is dialed, no possible match exists. The system returns incompatible. If the next digit is a #, it is treated as signaling dialing complete rather than being a digit. Short code 1 becomes an exact match and is used immediately.
4	601	Third digit triggers matching. Exact match to Short Code 2. Extension 210 dialed immediately.

Scenario 5

- Short Code 1 = 601/Dial Extn/203
- Short Code 2 = 60N/Dial Extn/210
- Dial Delay Count = 0. Dial Delay Time = 4 seconds.

Test	Dialing	Effect
1	6	No exact match but there is a potential match, so the system waits for additional dialing. If the Dial Delay Time expires, no exact match is found so incompatible is returned.
2	60	Potential match to both short codes. The system waits for additional dialing. If the Dial Delay Time expires, Short Code 2 becomes an exact match with N blank.
3	601	Exact match to Short Code 1. Used immediately
4	602	Exact match to Short Code 2. Used immediately.

Scenario 6

- Short Code 1 = 601/Dial Extn/203
- Short Code 2 = 60N/Dial Extn/210
- Short Code 3 = 60X/Dial Extn/207
- Dial Delay Count = 0. Dial Delay Time = 4 seconds.

Test	Dialing	Effect
1	6	No exact match but there are potential matches so the system waits for additional dialing. If the Dial Delay Time expires, no exact match has occurred so incompatible is returned.
2	60	Potential match to all short codes. System waits for additional dialing. If the Dial Delay Time expires, Short Code 2 becomes an exact match with N blank. If a digit is dialed, Short Code 3 becomes a more exact match and is used.
3	601	Exact match all short code, however Short Code 1 is treated as being more exact (more matching digits) and is used immediately
4	602	Exact match to short codes 2 and 3, however the Short Code 3 is treated as being more exact (length match) and is used immediately.

Scenario 7

- Short Code 1 = 601/Dial Extn/203
- Short Code 2 = 60N/Dial Extn/210
- Short Code 3 = 6XX/Dial Extn/207
- Dial Delay Count = 0. Dial Delay Time = 4 seconds.

Test	Dialing	Effect
1	6	No exact match but there are potential matches so the system waits for additional dialing. If the Dial Delay Time expires, no exact match has occurred so incompatible is returned.
2	60	Potential match to all short codes. System waits for additional dialing. If the Dial Delay Time expires, Short Code 2 becomes an exact match with N blank. If a digit is dialed, Short Code 3 becomes an more exact match and is used.
3	601	Exact match all short code, however Short Code 1 is treated as being more exact (more matching digits) and is used immediately
4	602	Exact match to short codes 2 and 3, however the Short Code 2 is treated as being more exact (more matching digits) and is used immediately.
5	612	Exact match to Short Code 3.

Related links

Short Code Overview on page 973

Default System Short Code List

Most control units are available in A-Law and U-Law models. Typically U-Law models are supplied to North American locales, A-Law models are supplied to the rest of the world. In addition to the using different default companding for digital lines and phone, A-Law and U-Law models support different default short codes. The following table lists the default system short codes present in a system's configuration.

Standard Mode

Short Code	Telephone Number	Feature	A-Law	U-Law
***00**	Blank	Cancel All Forwarding	✓	✓
***01**	Blank	Forward Unconditional On	✓	✓
***02**	Blank	Forward Unconditional Off	✓	✓
***03**	Blank	Forward On Busy On	✓	✓
***04**	Blank	Forward On Busy Off	✓	✓
***05**	Blank	Forward On No Answer On	✓	✓
***06**	Blank	Forward On No Answer Off	✓	✓
***07*N#**	N	Forward Number	✓	✓
***08**	Blank	Do Not Disturb On	✓	✓
***09**	Blank	Do Not Disturb Off	✓	✓
***10*N#**	N	Do Not Disturb Exception Add	✓	✓
***11*N#**	N	Do Not Disturb Exception Del	✓	✓
***12*N#**	N	Follow Me Here	✓	✓
***13*N#**	N	Follow Me Here Cancel	✓	✓
***14*N#**	N	Follow Me To	✓	✓
***15**	Blank	Call Waiting On	✓	✓
***16**	Blank	Call Waiting Off	✓	✓
***17**	?U	Voicemail Collect	✓	✓
***18**	Blank	Voicemail On	✓	✓
***19**	Blank	Voicemail Off	✓	✓
***20*N#**	N	Set Hunt Group Night Service	✓	✓
***21*N#**	N	Clear Hunt Group Night Service	✓	✓
***22*N#**	N	Suspend Call	✓	✗
***23*N#**	N	Resume Call	✓	✗
***24*N#**	N	Hold Call	✓	✗
***25*N#**	N	Retrieve Call	✓	✗
***26**		Clear CW	✓	✗
***27*N#**	N	Hold CW	✓	✗
***28*N#**	N	Suspend CW	✓	✗
***29**	Blank	Toggle Calls	✓	✓
***30**	Blank	Call Pickup Any	✓	✓
***31**	Blank	Call Pickup Group	✓	✓
***32*N#**	N	Call Pickup Extn	✓	✓
***33*N#**	N	Call Queue	✓	✓

Table continues…

Short Code	Telephone Number	Feature	A-Law	U-Law
***34N;**	N	Hold Music	✓	✓
***35*N#**	N	Extn Login	✓	✓
***36**	Blank	Extn Logout	✓	✓
***37*N#**	N	Call Park	✓	✓
***38*N#**	N	Unpark Call	✓	✓
***39**	1	Relay On	✓	✓
***40**	1	Relay Off	✓	✓
***41**	1	Relay Pulse	✓	✓
***42**	2	Relay On	✓	✓
***43**	2	Relay Off	✓	✓
***44**	2	Relay Pulse	✓	✓
***45*N#**	N	Acquire Call	✓	✓
***46**	Blank	Acquire Call	✓	✓
***47**	Blank	Conference Add	✓	✓
***48**	Blank	Voicemail Ringback On	✓	✓
***49**	Blank	Voicemail Ringback Off	✓	✓
***50**	Blank	Forward Huntgroup On	✓	✓
***51**	Blank	Forward Huntgroup Off	✓	✓
***52**	Blank	Cancel or Deny	✓	✓
***53*N#**	N	Call Pickup Members	✓	✓
***55**	Blank	Stamp Log	✓	✓
***57*N#**	N	Forward On Busy Number	✓	✓
***70**	Blank	Call Waiting Suspend	✓	✗
***70*N#**	N	Dial Physical Extn by Number	✗	✓
***71*N#**	N	Dial Physical Extn by Id	✗	✓
9000	"MAINTENANCE"	Relay On	✓	✓
***91N;**	N".1"	Record Message	✓	✓
***92N;**	N".2"	Record Message	✓	✓
***99;**	"edit_messages"	Voicemail Collect	✓	✓
9N	N	Dial	✗	✓
?	.	Dial	✓	✗

Server Edition

Short Code	Telephone Number	Feature	A-Law	U-Law
***00**	Blank	Cancel All Forwarding	✓	✓

Table continues…

Short Code	Telephone Number	Feature	A-Law	U-Law
***01**	Blank	Forward Unconditional On	✓	✓
***02**	Blank	Forward Unconditional Off	✓	✓
***03**	Blank	Forward On Busy On	✓	✓
***04**	Blank	Forward On Busy Off	✓	✓
***05**	Blank	Forward On No Answer On	✓	✓
***06**	Blank	Forward On No Answer Off	✓	✓
***07*N#**	N	Forward Number	✓	✓
***08**	Blank	Do Not Disturb On	✓	✓
***09**	Blank	Do Not Disturb Off	✓	✓
***10*N#**	N	Do Not Disturb Exception Add	✓	✓
***11*N#**	N	Do Not Disturb Exception Del	✓	✓
***12*N#**	N	Follow Me Here	✓	✓
***13*N#**	N	Follow Me Here Cancel	✓	✓
***14*N#**	N	Follow Me To	✓	✓
***17**	?U	Voicemail Collect	✓	✓
***18**	Blank	Voicemail On	✓	✓
***19**	Blank	Voicemail Off	✓	✓
***20*N#**	N	Set Hunt Group Night Service	✓	✓
***21*N#**	N	Clear Hunt Group Night Service	✓	✓
***29**	Blank	Toggle Calls	✓	✓
***30**	Blank	Call Pickup Any	✓	✓
***31**	Blank	Call Pickup Group	✓	✓
***32*N#**	N	Call Pickup Extn	✓	✓
***33*N#**	N	Call Queue	✓	✓
***34N;**	N	Hold Music	✓	✓
***35*N#**	N	Extn Login	✓	✓
***36**	Blank	Extn Logout	✓	✓
***37*N#**	N	Call Park	✓	✓
***38*N#**	N	Unpark Call	✓	✓
***44**	2	Relay Pulse	✓	✓
***45*N#**	N	Acquire Call	✓	✓
***46**	Blank	Acquire Call	✓	✓
***47**	Blank	Conference Add	✓	✓
***48**	Blank	Voicemail Ringback On	✓	✓
***49**	Blank	Voicemail Ringback Off	✓	✓

Table continues…

Short Code	Telephone Number	Feature	A-Law	U-Law
***50**	Blank	Forward Huntgroup On	✓	✓
***51**	Blank	Forward Huntgroup Off	✓	✓
***52**	Blank	Cancel or Deny	✓	✓
***53*N#**	N	Call Pickup Members	✓	✓
***55**	Blank	Stamp Log	✓	✓
***57*N#**	N	Forward On Busy Number	✓	✓
***66*N#**	N	Conference Meet Me	✓	✓
***70**	Blank	Call Waiting Suspend	✓	✗
***70*N#**	N	Dial Physical Extn by Number	✗	✓
***71*N#**	N	Dial Physical Extn by Id	✗	✓
***99;**	"edit_messages"	Voicemail Collect	✓	✓
9N	N	Dial	✗	✓ [1]
?	.	Dial	✓	✓ [1]

Embedded Voicemail

The following additional short codes are automatically added when an auto-attendant is cadded to the configuration.

Short Code	Telephone Number	Feature: Auto Attendant
***81XX**	"AA:"N".1"	These short codes correspond to the morning, afternoon, evening and menu actions prompts respectively. When dialed, the value XX is replaced with the auto-attendant number.
***82XX**	"AA:"N".2"	
***83XX**	"AA:"N".3"	
***84XX**	"AA:"N".4"	
***87XX**	"AA:"N".7"	This short code is used on systems using a Voicemail Pro auto-attendant to record the no match prompt.
***800XX**	"AA:"N".00	These short codes are used to record prompts for Park and Page actions. Each short code corresponds to the different key to which the action might be assigned, from 0 to 9, * and # respectively. When dialed, the value XX is replaced with the auto-attendant number.
***801XX**	"AA:"N".01	
***802XX**	"AA:"N".02	
***803XX**	"AA:"N".03	
***804XX**	"AA:"N".04	
***805XX**	"AA:"N".05	
***806XX**	"AA:"N".06	
***807XX**	"AA:"N".07	
***808XX**	"AA:"N".08	
***809XX**	"AA:"N".09	
***850XX**	"AA:"N".10	
***851XX**	"AA:"N".11	

General

For U-Law systems, a **9N** is a default short code on the Primary Server while a **?** short code is a default on all other servers.

Additional short codes of the form *DSSN, *SDN, *SKN, these are used by the system for internal functions and should not be removed or altered. Short codes *#N and **N may also visible, these are used for ISDN functions in Scandinavian locales.

The default ***34** short code for music on hold has changed to ***34N;**.

Related links

Short Code Overview on page 973

Chapter 103: Short Code Features

The following descriptions cover all short code features. However, the short codes available on a system depend on the system type and software release of that system.

Related links

Auto Attendant on page 996
Auto Intercom Deny Off on page 997
Auto Intercom Deny On on page 997
Break Out on page 998
Barred on page 998
Busy On Held on page 999
Call Intrude on page 1000
Call Listen on page 1000
Call Park on page 1002
Call Park and Page on page 1002
Call Pickup Any on page 1003
Call Pickup Extn on page 1003
Call Pickup Group on page 1004
Call Pickup Line on page 1005
Call Pickup Members on page 1005
Call Pickup User on page 1006
Call Queue on page 1006
Call Record on page 1007
Call Steal on page 1008
Call Waiting On on page 1009
Call Waiting Off on page 1009
Call Waiting Suspend on page 1010
Cancel All Forwarding on page 1010
Cancel Ring Back When Free on page 1011
Change Login Code on page 1012
Clear After Call Work on page 1012
Clear Call on page 1013
Clear CW on page 1013
Clear Hunt Group Night Service on page 1014
Clear Hunt Group Out Of Service on page 1015

Clear Quota on page 1015
Coaching Intrusion on page 1016
Conference Add on page 1016
Conference Meet Me on page 1017
CW on page 1018
Dial on page 1019
Dial 3K1 on page 1020
Dial 56K on page 1020
Dial 64K on page 1021
Dial CW on page 1021
Dial Direct on page 1022
Dial Direct Hot Line on page 1022
Dial Emergency on page 1023
Dial Extn on page 1023
Dial Fax on page 1024
Dial Inclusion on page 1024
Dial Paging on page 1025
Dial Physical Extension by Number on page 1026
Dial Physical Extension By ID on page 1026
Dial Speech on page 1027
Dial V110 on page 1027
Dial V120 on page 1028
Dial Video on page 1028
Disable ARS Form on page 1028
Disable Internal Forwards on page 1029
Disable Internal Forward Unconditional on page 1029
Disable Internal Forward Busy or No Answer on page 1030
Display Msg on page 1030
Do Not Disturb Exception Add on page 1031
Do Not Disturb Exception Delete on page 1032
Do Not Disturb On on page 1033
Do Not Disturb Off on page 1033
Enable ARS Form on page 1034
Enable Internal Forwards on page 1034
Enable Internal Forward Unconditional on page 1035
Enable Internal Forward Busy or No Answer on page 1035
Extn Login on page 1035
Extn Logout on page 1037
Flash Hook on page 1037
FNE Service on page 1038
Follow Me Here on page 1038

Follow Me Here Cancel on page 1039
Follow Me To on page 1039
Forward Hunt Group Calls On on page 1040
Forward Hunt Group Calls Off on page 1041
Forward Number on page 1041
Forward On Busy Number on page 1042
Forward On Busy On on page 1043
Forward On Busy Off on page 1043
Forward On No Answer On on page 1044
Forward On No Answer Off on page 1044
Forward Unconditional On on page 1045
Forward Unconditional Off on page 1045
Group Listen Off on page 1046
Group Listen On on page 1046
Headset Toggle on page 1047
Hold Call on page 1047
Hold CW on page 1048
Hold Music on page 1049
Hunt Group Disable on page 1049
Hunt Group Enable on page 1050
Last Number Redial on page 1050
MCID Activate on page 1051
Mobile Twinned Call Pickup on page 1051
Off Hook Station on page 1052
Outgoing Call Bar Off on page 1052
Outgoing Call Bar On on page 1053
Private Call Off on page 1054
Private Call On on page 1054
Priority Call on page 1055
Record Message on page 1055
Relay On on page 1056
Relay Off on page 1057
Relay Pulse on page 1057
Resume Call on page 1058
Retrieve Call on page 1059
Ring Back When Free on page 1059
Secondary Dial Tone on page 1060
Set Absent Text on page 1060
Set Account Code on page 1062
Set Authorization Code on page 1062
Set Fallback Twinning Off on page 1063

Set Fallback Twinning On on page 1063
Set Hunt Group Night Service on page 1063
Set Hunt Group Out Of Service on page 1064
Set Inside Call Seq on page 1065
Set Mobile Twinning Number on page 1066
Set Mobile Twinning On on page 1066
Set Mobile Twinning Off on page 1066
Set No Answer Time on page 1067
Set Outside Call Seq on page 1067
Set Ringback Seq on page 1068
Set Time Profile on page 1069
Set Wrap Up Time on page 1070
Speed Dial on page 1071
Shutdown Embedded Voicemail on page 1071
Stamp Log on page 1072
Startup Embedded Voicemail on page 1072
Suspend Call on page 1073
Suspend CW on page 1073
Start After Call Work on page 1074
Toggle Calls on page 1074
Unpark Call on page 1075
Voicemail Collect on page 1075
Voicemail Node on page 1077
Voicemail On on page 1077
Voicemail Off on page 1078
Voicemail Ringback On on page 1078
Voicemail Ringback Off on page 1079
Whisper Page on page 1080

Auto Attendant

This feature is used with auto-attendants for recording greetings and to transfer calls to an auto-attendant.

Details

- **Telephone Number**: ✓
  - System short codes (`*81XX`, `*82XX`, `*83XX` and `*84XX`) are automatically added for use with all auto-attendants. These are used for morning, afternoon, evening and menu options greetings respectively. These short codes use a **Telephone Number** of the form

"AA:"N".Y" where N is the replaced with the auto attendant number dialed and Y is 1, 2, 3 or 4 for the morning, afternoon, evening or menu option greeting.

- To add a short code to call an auto-attendant, omit the XX part. For example, add the short code *80XX/Auto Attendant/"AA:"N if internal dialed access to auto-attendants is required.
- System short codes *800XX, *801XX, ..., *809XX, *850XX, and *851XX are also automatically added for recording prompts for any **Page and Page** actions. The codes correspond to the key to which the action has been assigned; 0 to 9, * and # respectively. These short codes use a **Telephone Number** of the form "AA:"N".00", ..., "AA:"N".01", "AA:"N".10" and "AA:"N".11" respectively.

- **Release**: 2.0+.
- **Programmable Button Control**: ✗
- **Default Short Code**: ✓ See Configuration Settings | Auto Attendant.

Related links

Short Code Features on page 993

Auto Intercom Deny Off

Details

- **Telephone number:** ✗
- **Default short code:** ✗
- **Programmable Button Control:** ✓ Auto Intercom Deny Off

Related links

Short Code Features on page 993

Auto Intercom Deny On

Details

- **Telephone number:** ✗
- **Default short code:** ✗
- **Programmable Button Control:** ✓ Auto Intercom Deny On

Related links

Short Code Features on page 993

Break Out

This feature is usable within a system multi-site network. It allows a user on one system in the network to specify that the following dialing be processed by another system on the network as if the user dialed it locally on that other system.

Details

- **Telephone Number**: The IP Address or Name of the system, using * characters in place of . characters.
- **Default Short Code**: ✗
- **Programmable Button Control**: BkOut
- **Release**: 4.0+.

Examples

On a system, to break out via a system called RemoteSwitch with the IP Address 192.168.42.3, either of the following short codes could be used.

Example 1 allows break out using any remote switch by dialing its IP address, for example *80*192*168*42*3#. Example 2 does this for a specific remote system by dialing just *81.

- **Example 1**
  - **Feature**: Break Out
  - **Telephone Number**: N
  - **Code**: *80*N#
- **Example 2**
  - **Code**: *81
  - **Telephone Number:** RemoteSwitch
  - **Feature**: Break Out

Related links

Short Code Features on page 993

Barred

This short code feature can be used for call barring by using the short code as the call destination. This short code feature was previously called **Busy**. It has been renamed but its function has not changed.

When used in an ARS form that has been configured with an Alternate Route, for callers whose dialing has matched the short code no further routing is applied.

Details

- **Telephone Number**: ✗

- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **Release**: 1.0+.

Related links

Short Code Features on page 993

Busy On Held

When on, busy on held returns busy to new calls when the user has an existing call on hold. This short code feature is useful when a user does not want to be distracted by an additional incoming call when they have a call on hold.

Details

- **Telephone Number**: ✓ Y or 1 for on, N or 0 for off.
- **Default Short Code**: ✗
- **Programmable Button Control:** ✓ BusyH
- **Release:** 1.0+.

Example: Turning Busy on Held on

If on, when the user has a call on hold, new calls receive busy tone (ringing if analog) or are diverted to Voicemail if enabled, rather than ringing the user.

This overrides call waiting when the user has a call on hold.

- **Short Code**: *12
- **Telephone Number**: Y
- **Feature:** BusyOnHeld

Example: Turning Busy on Held off

Another short code must be created to turn the Busy on Held feature off. If off, when the uses has a call on hold, new calls will still get directed to the user.

- **Short Code**: *13
- **Telephone Number**: N
- **Feature:** BusyOnHeld

Related links

Short Code Features on page 993

Call Intrude

This feature allows you to intrude on the existing connected call of the specified target user. All call parties are put into a conference and can talk to and hear each other. A **Call Intrude** attempt to a user who is idle becomes a Priority Call.

- Intrusion features are controlled by the **Can Intrude** setting of the user intruding and the **Cannot Be Intruded** setting of user being intruded on. By default, no users can intrude and all users cannot be intruded.
- Intrusion features uses system conference resources during the call. If insufficient conference resource are available, the feature cannot be used.
- Users can use privacy features to set a call cannot be intruded on and recorded.
- Intruding onto a user doing silent monitoring (see Call Listen on page 1000) is turned into a silent monitoring call.

The system support a range of other call intrusion methods in addition to this feature.

Details

- **Telephone Number**: ✓ Target extension number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ Intru
- **See also**: Call Listen on page 1000, Coaching Intrusion on page 1016, Dial Inclusion on page 1024, Whisper Page on page 1080.
- **Release**: 1.0+.

Related links

Short Code Features on page 993

Call Listen

This feature allows you to monitor another user's call without being heard.

- By default, monitoring is accompanied by a tone heard by all parties. Use of the tone is controlled by the **Beep on Listen** setting on the **System** > **Telephony** > **Tones and Music** tab.

⚠ Warning:

- Listening to a call without the other parties being aware is subject to local regulations. You must ensure that you have complied with the local regulations. Failure to do so can result in penalties.

The use of call listen is dependent on:

- The target being a member of the group set as the user's **Monitor Group** (**User** > **Telephony** > **Supervisor Settings**). The user does not have to be a member of the group.

- Intrusion features are controlled by the **Can Intrude** setting of the user intruding and the **Cannot Be Intruded** setting of user being intruded on. By default, no users can intrude and all users cannot be intruded.
- Intrusion features uses system conference resources during the call. If insufficient conference resource are available, the feature cannot be used.

A number of features are supported for call listening:

- Users can use privacy features to set a call cannot be intruded on and recorded.
- IP extensions can be monitored including those using direct media.
- The monitoring call can be initiated even if the target user is not currently on a call and remains active until the monitoring user clears the monitoring call.
- The user who initiated the call listen can also record the call.

Intruding onto an a user doing silent monitoring (Call Listen) is turned into a silent monitoring call.

1400, 1600, 9500 and 9600 Series phones with a user button can initiate listening using that button if the target user meets the criteria for listening.

The system support a range of other call intrusion methods in addition to this feature.

Details

- **Telephone Number**: ✓ Target extension number (extension must be local).
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ Listn
- **See also**: Call Intrude on page 1000, Coaching Intrusion on page 1016, Dial Inclusion on page 1024, Whisper Page on page 1080.
- **Release:** 1.0+.

Example

User 'Extn205' wants to be able to monitor calls received by members of the Hunt Group 'Sales'.

1. For user 'Extn205', in the **Monitor Group** (**User** > **Telephony** > **Supervisor Settings**) list box, select the hunt group.
2. Ensure that **Can Intrude** is checked.
3. Create a user short code to allow Extn205 to start monitoring.
   - **Short Code**: *89*N#
   - **Telephone Number**: N
   - **Line Group ID**: 0.
   - **Feature**: CallListen
4. For each member of the hunt group, check that their **Cannot be Intruded** setting is unchecked.
5. Now when a member of the 'Sales' hunt group is on a call, Extn205 can replace N in the short code with the extension number of that member and monitor their call.

Related links

Short Code Features on page 993

Call Park

Parks the user's current call into the specified park slot number. The call can then be retrieved by other extensions (refer to the appropriate telephone user guide). While parked the caller hears music on hold if available. The 'Unpark Call' feature can be used to retrieve calls from specific park slots.

Park Timeout (System | Telephony | Telephony) controls how long a call will remain parked. When this expires the call will recall to the parking user if they are idle or when they next become idle. The recall call will continue ring and does follow any forwards or go to voicemail.

Details

- **Telephone Number**: ✓ Park slot number.
  - Park slot IDs can be up to 9 digits in length. Names can also be used for application park slots.
  - If no park slot number is specified when this short code is used, the system automatically assigns a park slot number based on the extension number of the user parking the call plus one digit 0 to 9.
- **Default Short Code**: ✓ *37*N#
- **Programmable Button Control**: ✓ Call Park
- **See also**: Unpark Call.
- **Release:** 1.0+.

Example

This short code is a default within the system configuration. This short code can be used to toggle the feature on/off. N represents the park slot number in which the call will be parked. For example, if a user wants to park a call to slot number 9, the user would dial *37*9#. The call will be parked there until retrieved by another extension or the original extension.

- **Short Code**: *37*N#
- **Telephone Number**: N
- **Feature:** ParkCall

Related links

Short Code Features on page 993

Call Park and Page

Parks the user's current call into the highest park slot number within the range specified on the **System | Telephony | Park & Page** tab, in the **Central Park Range** field. For example, if the specified **Central Park Range** is 1XX, then the Park & Page short code would attempt to Park on 199. If the range is 567XX, then the call would attempt to Park on 56799.

Call Park and Page via short code is primarily useful for phones with no display, or phones on which a Call Park operation is seldom performed. It provides a way for the user to Central Park

in a pre-known location. If the highest Central Park slot is already in use, then the short code Call Park and Page attempt will not be successful.

In order to perform a Page after a successful Call Park via short code, the user must enter a valid Page short code.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ Call Park and Page
- **Release:** 9.0+.

Related links

Short Code Features on page 993

Call Pickup Any

Pick up the first available ringing call.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *30
- **Programmable Button Control**: ✓ PickA
- **See also**: Call Pickup Extn, Call Pickup Group, Call Pickup Members, Acquire Call, Call Pickup Line, Call Pickup User.
- **Release**: 1.0+.

Example

Below is an example of the short code setup:

- **Short Code**: *30
- **Feature**: CallPickupAny

Related links

Short Code Features on page 993

Call Pickup Extn

Pick up a ringing call from a specific extension.

Details

- **Telephone Number:** ✓ Target extension number.
- **Default Short Code**: ✓ *32*N#
- **Programmable Button Control**: ✓ CpkUp
- **See also**: Call Pickup Any, Call Pickup Group, Call Pickup Members, Acquire Call, Call Pickup Line, Call Pickup User.
- **Release**: 1.0+.

Example

This short code is a default within the system configuration. N represents the specific extension. For example, if a user dials *32*201#, they will pick up the call coming into extension 201.

- **Short Code**: *32*N#
- **Telephone Number**: N
- **Feature**: CallPickupAny

Related links

Short Code Features on page 993

Call Pickup Group

Pick up a call ringing any hunt group of which the user is a member. The user can use this feature even if their membership of the group is currently set as disabled.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *31
- **Programmable Button Control**: ✓ PickG
- **See also**: Call Pickup Any, Call Pickup Extn, Call Pickup Members, Acquire Call, Call Pickup Line, Call Pickup User.
- **Release**: 1.0+.

Example

Below is an example of the short code setup.

- Short Code: *31
- Feature: CallPickupGroup

Related links

Short Code Features on page 993

Call Pickup Line

Pick up an incoming call which is alerting, parked or held. The pickup uses the Line Appearance ID specified in Telephone Number field of the short code. It cannot be used to pickup conferenced calls. The normal user intrusion features are not applied to this pickup feature.

Details

- **Telephone Number**: ✓ Target Line Appearance ID.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **See also**: Call Pickup Any, Call Pickup Extn, Call Pickup Group, Call Pickup Members, Acquire Call, Call Pickup User.
- **Release**: 4.0+ (Added in the Release 4.0 Q2 2007 maintenance release).

Example

This short code is a default within the system configuration. N represents the specific Line Appearance ID.

- **Short Code**: *89*N#
- **Telephone Number**: N
- **Feature**: CallPickupLine

Related links

Short Code Features on page 993

Call Pickup Members

This feature can be used to pick up a ringing or queuing call at an extension that is a member of the Hunt Group specified. The call picked up does not have to be a hunt group call. The function includes group members even if their membership of the group is currently disabled.

Details

- **Telephone Number**: ✓ Group number or "Group name".
- **Default Short Code:** ✓ *53*N#
- **Programmable Button Control**: ✓ PickM
- **See also**: Call Pickup Any, Call Pickup Extn, Call Pickup Group, Acquire Call, Call Pickup Line, Call Pickup User.
- **Release**: 1.0+.

Example

Below is an example of the short code setup. N represents the extension number of the Hunt Group. For example, if a user dials *53*500#, they will pick up the call coming into extension 500 (the hunt group's extension).

- **Short Code:** *53*N#
- **Telephone Number:** N
- **Feature:** CallPickupMembers

Related links

Short Code Features on page 993

Call Pickup User

Pick up an incoming call which is alerting, parked or held. The pickup uses the user extension number specified in Telephone Number field of the short code. If there are multiple calls, priority is given to picking up alerting, then parked and then held in that order of priority. It cannot be used to pickup conferenced calls. The normal user intrusion features are not applied to this pickup feature.

Details

- **Telephone Number**: ✓ Target user extension number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **See also**: Call Pickup Any, Call Pickup Extn, Call Pickup Group, Call Pickup Members, Acquire Call, Call Pickup Line.
- **Release**: 4.0+.

Example

N represents the specific user.

- **Short Code**: *89*N#
- **Telephone Number**: N
- **Feature**: CallPickupUser

Related links

Short Code Features on page 993

Call Queue

Queue the current call to the destination phone, even when the destination phone is busy. This is the same as a transfer except it allows you to transfer to a busy phone.

Details

- **Telephone Number:** ✓ Target extension number.
- **Default Short Code**: ✓ *33*N#
- **Programmable Button Control**: ✓ Queue
- **Release**: 1.0+.

Example

Below is an example of the short code setup. N represents the extension the caller wishes to queue for. For example, if a user dials *33*201# while connected to a caller, this caller will be queued for extension 201.

- **Short Code**: *33*N#
- **Telephone Number**: N
- **Feature**: CallQueue

Related links

Short Code Features on page 993

Call Record

This feature allows you to record a conversation. To use this requires Voicemail Pro. Refer to your local regulations in relation to the recording of calls.

- An advice of recording warning will be given if configured on the voicemail system.
- The recording is placed in the mailbox specified by the user's **Manual Recording Mailbox** setting.
- Intrusion features uses system conference resources during the call. If insufficient conference resource are available, the feature cannot be used.
- Users can use privacy features to set a call cannot be intruded on and recorded.

Details

- **Telephone Number**: ✓ Target extension number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ Recor
- **Release**: 1.0+.

Example: Record your own extension's call

To use this short code, the user should place the call on hold and dial *55. They will automatically be reconnected to the call when recording begins.

- **Short Code**: *55
- **Telephone Number:** None

- **Feature**: CallRecord

Related links

Short Code Features on page 993

Call Steal

This function allows a user to seize a call answered or ringing on another extension. This function can be used with or without a specified user target.

- If the target has multiple alerting calls, the function steals the longest waiting call.
- If the target has a connected call and no altering calls, the function steals the connected call. This is subject to the **Can Intrude** setting of the **Call Steal** user and the **Cannot Be Intruded** setting of the target.
- If no target is specified, the function attempts to reclaim the user's last ringing or transferred call if it has not been answered or gone to voicemail.
- Stealing a video call changes the call to an audio call.
- R11.1 FP2 SP4 and higher: The shortcode for this feature can be used with the user's own extension number. That enables twinned and simultaneous device users to move a connected call from another one of their devices. This usage ignores the user's privacy and intrusion settings.

Details

- **Telephone Number**: ✓
  - Target extension number.
  - User's own extension number to move call from other simultaneous device. This can include using the `U` short code character.
  - Blank for last call transferred.
- **Default Short Code**: ✓ *45*N# and *46
- **Programmable Button Control**: ✓ Aquire
- **Release**: 2.1+

Example: Taking Over a Call

In this example, `N` represents the extension to be taken over. For example, if a user dials `*45*201#`, they will take over the current call on extension 201.

- **Short Code**: *45*N#
- **Telephone Number**: N
- **Feature**: Call Steal

Example: Reclaiming a Call

This short code reclaims the last call from your extension. This function is useful when you want to catch a call you have just missed that has gone off to Voicemail.

- **Short Code**: *46
- **Feature**: Call Steal

Related links

Short Code Features on page 993

Call Waiting On

Enables call waiting on the user's extension. When on, if the user receives a second calls when already on a call, they hear a call waiting tone in the speech path.

Call waiting settings are ignored for users with multiple call appearance buttons. In this case the appearance buttons are used to indicate additional calls. Call waiting is automatically applied for users with 'internal twinned' phones.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *15 (not on Server Edition)
- **Programmable Button Control**: ✓ CWOn
- **See also**: Call Waiting Off, Call Waiting Suspend.
- **Release**: 1.0+.

Example

Below is a sample of the short code setup.

- **Short Code**: *15
- **Feature**: CallWaitingOn

Related links

Short Code Features on page 993

Call Waiting Off

Disables call waiting on the user's extension. Call waiting may be applied for users with internal twinned phones regardless of their call waiting settings.

Details

- **Telephone Number**: ✗

- **Default Short Code**: ✓ *16 (not on Server Edition)
- **Programmable Button Control**: ✓ CWOff
- **See also**: Call Waiting On, Call Waiting Suspend.
- **Release**: 1.0+.

Example

Below is a sample of the short code setup.

- **Short Code**: *16
- **Feature**: Call Waiting Off

Related links

Short Code Features on page 993

Call Waiting Suspend

For phones using call waiting, this feature temporarily disables call waiting for the duration of the user's next call.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *70 (A-Law only)
- **Programmable Button Control**: ✓ CWSus
- **See also**: Call Waiting On, Call Waiting Off.
- **Release**: 1.0+.

Example

Below is a sample of the short code setup. This short code is a default within the system configuration.

- **Short Code**: *70
- **Feature**: CallWaitingSuspend

Related links

Short Code Features on page 993

Cancel All Forwarding

This feature cancels all forms of forwarding on the user's extension including "Follow Me" and "Do Not Disturb".

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *00
- **Programmable Button Control**: ✓ FwdOf
- **See also**: Forward On Busy On, Forward On Busy Off, Forward On No Answer On, Forward On No Answer Off, Forward Unconditional On, Forward Unconditional Off, Do Not Disturb On, Do Not Disturb Off.
- **Release**: 1.0+.

Example

Below is a sample of the short code setup.

- **Short Code**: *00
- **Feature:** CancelCallForwarding

Related links

Short Code Features on page 993

Cancel Ring Back When Free

Cancels any existing ring back (also known as callback) set by the user.

Details

- **Telephone Number:**✗
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ RBak-
- **See also**: Ring Back When Free.
- **Release**: 1.0+.

Example: Cancel Ring Back When Free

This example Short Code will cancel Ring Back When Free on the specified extension. N represents the target extension from which you have set a ring back. For example, if Paul has set a ring back on extension 201, he must dial *84*201# to cancel that ring back request.

- Short Code: *84*N#
- Telephone Number: N
- Feature: CancelRingBackWhenFree

Related links

Short Code Features on page 993

Change Login Code

Allows a user to change their login code. The login code must meet the **Login Code Complexity** requirements defined on the **System | Telephony** tab.

Details

- **Telephone Number**: ✓ The user's current and new log in codes separated by a *, see the examples below.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗

Example

The user has a **Login Code** of **1234** and wants to change it to **5678**. To use the short code below, the user must dial ***60*1234*5678#**.

- **Short Code**: *60*N#
- **Telephone Number**: N
- **Feature**: Change Login Code.

Example

For a user with no login code currently set, they can still use the short code to set a login code. For example using the short code created above to set their login code to 1234 they should dial ***60**1234#**.

Example

System phone users can also use this short code to change the login code of an other user. For example 403 is configured as a system phone with a login code of **1234**. User 410 has forgotten their login code and needs it changed. User 403 can do this by dialing the following:

- ***60*410*1234***<new code>**#**

Related links

Short Code Features on page 993

Clear After Call Work

This feature can be users who have been configured as CCR agents. It allows them to dial a short code to exit the After Call Work (ACW) state as reported by the Customer Call Reporter (CCR) application.

Note:

CCR is not supported in IP Office release 9.1 and later.

Details

- **Telephone Number**: ✗

- **Default Short Code**: ✗
- **Programmable Button Control:** ✓ ACWrk
- **See also**: Start After Call Work.
- **Release:** 4.2 4Q 2008 Maintenance release+.

Related links

Short Code Features on page 993

Clear Call

This feature can be used to end the current call.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *52
- **Programmable Button Control**: ✓ Clear
- **Release**: 1.0+.

Example

Below is a sample of the short code setup. This example could be used in a situation where you are doing a supervised transfer and the party to be transferred to does not want to take the call. In this scenario, you can put the call on hold and dial *52. This will clear the last connected call (for example the party who has just refused the transfer), and retrieve the original call or dial tone.

- **Short Code**: *52
- **Feature**: Deny/ClearCall

Related links

Short Code Features on page 993

Clear CW

This feature is most commonly used to end the user's current call and answer the waiting call.

- Call waiting settings are ignored for users with multiple call appearance buttons.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *26 (A-Law only) (not on Server Edition)
- **Programmable Button Control**: ✓ ClrCW
- **Release:** 1.0+.

Example

Below is a sample of the short code setup.

- **Short Code**: *26
- **Feature:** ClearCW

Related links

Short Code Features on page 993

Clear Hunt Group Night Service

This feature changes the specified hunt group from Night Service mode to In Service mode.

Setting and clearing hunt group night service can be done using either manual controls or using a system time profile. The use of both methods to control the night service status of a particular hunt group is not supported.

This function is currently not supported between systems in a multi-site network. It can only be used by a user currently logged onto the same system as hosting the hunt group.

Details

- **Telephone Number**: ✓
  - Hunt group extension number. If left blank, the short code will affect all hunt groups of which the user is a member.
  - The **Set Hunt Group Night Service** and **Clear Hunt Group Night Service** short code and button features can be used to switch an SSL VPN service off or on respectively. The service is indicated by setting the service name as the telephone number or action data. Do not use quotation marks.
- **Default Short Code**: ✓ *21*N#
- **Programmable Button Control**: ✓ HGNS-
- **See also**: Clear Hunt Group Out Of Service, Set Hunt Group Night Service, Set Hunt Group Out Of Service.
- **Release**: 1.0+.

Example

Below is a sample of the short code setup. N represents the telephone number of the hunt group to be taken out of "Night Service" mode and placed into "In Service" mode. For example, when *21*201# is dialed, the hunt group associated with extension 201 will be taken out of "Night Service" mode.

- **Short Code**: *21*N#
- **Telephone Number**: N
- **Feature**: ClearHuntGroupNightService

Related links

Short Code Features on page 993

Clear Hunt Group Out Of Service

This feature changes the specified hunt group from Out of Service mode to In Service mode. This will not override a hunt group in night service due to a time profile.

Details

- **Telephone Number**: ✓ Hunt group extension number. If left blank, the short code will affect all hunt groups of which the user is a member.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ HGOS-
- **See also**: Clear Hunt Group Night Service, Set Hunt Group Night Service, Set Hunt Group Out Of Service.
- **Release**: 1.0+.

Example

Below is a sample short code using the Clear Hunt Group Out Of Service feature. N represents the telephone number of the hunt group to be taken out of "Out of Service" mode. For example, when *55*201# is dialed, the hunt group associated with extension 201 will be placed into "In Service" mode.

- **Short Code**: *55*N#
- **Telephone Number**: N
- **Feature**: ClearHuntGroupOutOfService

Related links

Short Code Features on page 993

Clear Quota

This feature refreshes the time quota for all services or a specific service.

Details

- **Telephone Number**: ✓ "Service name" or "" (all services).
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ Quota
- **Release**: 1.0+.

Related links

Short Code Features on page 993

Coaching Intrusion

This feature allows the you to intrude on another user's call and to talk to them without being heard by the other call parties to which they can still talk. For example: User A is on a call with user B. When user C intrudes on user A, they can hear users A and B but can only be heard by user A.

- Intrusion features are controlled by the **Can Intrude** setting of the user intruding and the **Cannot Be Intruded** setting of user being intruded on. By default, no users can intrude and all users cannot be intruded.
- Intrusion features uses system conference resources during the call. If insufficient conference resource are available, the feature cannot be used.
- Listening to a call without the other parties being aware is subject to local regulations. You must ensure that you have complied with the local regulations. Failure to do so can result in penalties.

The system support a range of other call intrusion methods in addition to this feature.

Details

- **Telephone Number**: ✓ Target extension number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ Coach.
- **See also**: Call Intrude, Call Listen, Dial Inclusion, Whisper Page.
- **Release:**9.0+

Related links

Short Code Features on page 993

Conference Add

Conference add controls can be used to place the user, their current call and any calls they have on hold into a conference. When used to start a new conference, the system automatically assigns a conference ID to the call. This is termed ad-hoc (impromptu) conferencing.

If the call on hold is an existing conference, the user and any current call are added to that conference. This can be used to add additional calls to an ad-hoc conference or to a meet-me conference. Conference add can be used to connect two parties together. After creating the conference, the user can drop from the conference and the two incoming calls remain connected.

For further details, see Conferencing on page 686.

Details

- **Telephone Number:** ✗
- **Default Short Code**: ✓ *47
- **Programmable Button Control**: ✓ Conf+
- **See also**: Conference Meet Me.
- **Release**: 1.0+.

Example

Below is a sample of the short code setup.

- **Short Code**: *47
- **Feature**: ConferenceAdd

Related links

Short Code Features on page 993

Conference Meet Me

Conference meet-me refers to features that allow a user or caller to join a specific conference by using the conference's ID number (either pre-set in the control or entered at the time of joining the conference).

Non-subscription IP500 V2 systems require a **Preferred Edition** license.

Note:

Conference Meet Me features can create conferences that include only one or two parties. These are still conferences that are using resources from the host system's conference capacity.

Conference ID Numbers

By default, ad hoc conferences are assigned numbers starting from 100 for the first conference in progress. Therefore, for conference Meet Me features specify a number away from this range ensure that the conference joined is not an ad hoc conference started by other users. It is no longer possible to join a conference using conference Meet Me features when the conference ID is in use by an ad-hoc conference.

User Personal Conference Number Each user's own extension number is treated as their own personal conference number. Only that user is able to start a conference using that number as the conference ID. Any one else attempting to start a conference with that number will find themselves in a conference but on hold until the owner also joins. Personal conferences are always hosted on the owner's system.

Note:

When a user calls from their mobile twinned number, the personal conference feature will only work if they access the conference using an FNE 18 service.

Multi-Site Network Conferencing

Meet Me conference IDs are now shared across a multi-site network. For example, if a conference with the ID 500 is started on one system, anyone else joining conference 500 on any system will join the same conference. Each conference still uses the conference resources of the system on which it was started and is limited by the available conference capacity of that system.

Previously separate conferences, each with the same conference ID, could be started on each system in a multi-site network.

Other Features

Transfer to a Conference Button A currently connected caller can be transferred into the conference by pressing **TRANSFER**, then the Conference Meet Me button and **TRANSFER** again to complete the transfer. This allows the user to place callers into the conference specified by the button without being part of the conference call themselves. This option is only support on Avaya phones with a fixed **TRANSFER** button.

Conference Button Status Indication When the conference is active, any buttons associated with the conference ID indicate the active state.

For further details, see Conferencing on page 686.

.

Details

- **Telephone Number:** ✓ Conference number. This can be an alphanumeric value up to 15 characters.
  - The number can be prefixed with **H(*x*)** where ***x*** is the number of the music-on-hold source that should be played to the first caller to enter the conference.
- **Default Short Code**: ✗ / ✓ *66*N# on Server Edition systems.
- **Programmable Button Control**: ✓ CnfMM
- **See also**: Conference Add.
- **Release:** 1.0+.

Related links

Short Code Features on page 993

CW

Pick up the waiting call. This feature provides same functionality as pressing the **Recall** or **Hold** key on the phone. Unlike the Clear CW feature, this feature does not disconnect you from the existing call when the second call is picked up.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **Release:** 1.0+.

Related links

Short Code Features on page 993

Dial

This short code feature allows users to dial the number specified to an outside line.

Details

- **Telephone Number**: ✓ Telephone number.
- **Default Short Code**: ✓ Various depending on locale and system type.
- **Programmable Button Control:** ✓ Dial
- **See also**: Dial Direct, Dial Emergency, Dial Extn, Dial Inclusion, Dial Paging.
- **Release:** 1.0+.

Example: Creating a Speed Dial

In this example, users entering 401 on their telephone key pad will dial the New Jersey Office on 212 555 0000.

- **Short Code**: 401
- **Telephone Number**: 2125550000

Example: Replace Outgoing Caller ID

This short code is useful in a "call center" environment where you do not want customers to have access to the number of your direct line; you want the general office number displayed. The sample short code below will force the outgoing caller ID to display 123.

Use of this feature is dependent upon your local service provider.

- **Short Code**: ?
- **Telephone Number**: .s123

Example: External Dialing Prefix

The short code is for dialing a prefix for an outside line N represents the external number you want to call.

- **Short Code**: 9N
- **Telephone Number**: N

Example: Blocking Caller ID

This is for blocking Caller ID for external calls. This feature can be applied to specific external numbers or to all out going calls. In most situations, the company will choose to block the caller ID for all external calls or leave it available for all external calls.

- **Short Code**: 9N
- **Telephone Number**: NW

Example: Maximum Call Length

The character t can be used in dialing short codes to set the maximum allowed duration of a call. For example, the following short code will dial a number but then disconnect the call after 20 minutes (plus or minus a minute).

- **Short Code**: 9N
- **Telephone Number**: Nt(20)

Related links

Short Code Features on page 993

Dial 3K1

Sets the ISDN bearer capabilities to 3.1Khz audio call.

Details

- **Telephone Number**: ✓ Telephone number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ D3K1
- **Release**: 1.0+.

Related links

Short Code Features on page 993

Dial 56K

Sets the ISDN bearer capabilities to 56Kbps data call.

Details

- **Telephone Number:** ✓ Telephone number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ D56K
- **Release**: 1.0+.

Related links

Short Code Features on page 993

Dial 64K

Sets the ISDN bearer capabilities to 64Kbps data call.

Details

- **Telephone Number:** ✓ Telephone number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ D64K
- **Release**: 1.0+.

Related links

Short Code Features on page 993

Dial CW

Call the specified extension number and force call waiting indication on if the extension is already on a call.

If the user has call appearance buttons programmed, call waiting will not get activated. The next incoming call will appear on an available call appearance button. When there are no available call appearance buttons, the next incoming call will receive busy tone.

Details

- **Telephone Number:** ✓ Extension number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ DCW
- **Release**: 1.0+.

Example

N represents the extension number to be dialed. For example, a user dialing *97*201# will force call waiting indication on at extension 201 if extension 201 is already on a call.

- **Short Code**: *97*N#
- **Telephone Number**: N
- **Feature**: DialCW

Related links

Short Code Features on page 993

Dial Direct

Automatic intercom functions allow you to call an extension and have the call automatically answered on speaker phone after 3 beeps. The extension called must support a handsfree speaker. If the extension does not have a handsfree microphone then the user must use the handset if they want to talk. If the extension is not free when called, the call is presented as a normal call on a call appearance button if available.

Details

- **Telephone Number**: ✓ Extension number
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ Dirct
- **See also**: Dial Paging.
- **Release**: 1.0+.

Example

This allows the extension specified to be automatically answered. N represents the extension that will be forced to automatically answer. For example, when a user dials *83*201#, extension 201 will be forced to automatically answer the call.

- **Short Code**: *83*N#
- **Telephone Number**: N
- **Feature**: DialDirect

Related links

Short Code Features on page 993

Dial Direct Hot Line

When the line appearance button is mapped to a short code using the **Dial Direct Hot Line** short code feature, no secondary dial tone is generated and the number is dialed directly. This feature should not be confused with the hot line feature enabled using **?D** short codes.

Details

- **Telephone Number**: ✓
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **Release**: 3.0 to 4.0, 8.0+

Example

Below is a sample short code using the **Dial Direct Hot Line** feature. The short code *83* should then be set as the prefix for the particular line required.

- **Short Code**: *83*
- **Telephone Number**: .
- **Feature**: DialDirectHotLine

Related links

Short Code Features on page 993

Dial Emergency

Dials the number specified regardless of any call barring applicable to the user.

On all systems, regardless of locale; system short codes using the **Dial Emergency** feature should be created for any required emergency service numbers, with and without any external dialing prefixes. Using a combination of location and emergency ARS entries, calls made matching the emergency short codes should be routed to suitable lines. See Configuration for Emergency Calls on page 772.

- Details of calls made using this function can be viewed using an **Emergency View** button. See Emergency View on page 1142.
- **Telephone Number**: ✓ Telephone number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ Emrgy
- **Release**: 1.0+.

Related links

Short Code Features on page 993

Dial Extn

This feature can be used to dial an internal extension number (user or hunt group).

Details

- **Telephone Number**: ✓ Extension number.
  - **p(x)** can be added as a suffix to the **Telephone Number** to change the priority of a call. Allowable values for **x** are **1**, **2** or **3** for low, medium or high priority respectively. For example **Np(1)**.
- **Default Short Code**: ✗

- **Programmable Button Control**: ✗
- **See also**: Dial Direct, Dial Paging, DialPhysicalExtensionByNumber, DialPhysicalNumberByID.
- **Release**: 1.0+.

Example: Dial on Pick up

The following user short code dials the extension specified the moment the user's handset is picked up.

- **Short Code**: ?D
- **Telephone Number**: 201
- **Line Group ID**: 0
- **Feature**: Dial Extn

Related links

Short Code Features on page 993

Dial Fax

This feature is used to route fax calls via Fax Relay.

Details

- **Telephone Number**: ✓ Fax destination number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **Release**: 5.0+.

Example

In this example, the line group ID matches the URI configured on a SIP line that has been configured for Fax Relay.

- **Short Code**: 6N
- **Telephone Number**: N"@192.16.42.5"
- **Line Group ID**: 17
- **Feature**: Dial Fax

Related links

Short Code Features on page 993

Dial Inclusion

This feature allows you to intrude on another user's call to talk to them. Their current call is put on hold while you talk and automatically reconnected when you end the intrusion. The intruder

and the target extension can then talk but cannot be heard by the other party. This can include intruding into a conference call, where the conference will continue without the intrusion target.

During the intrusion all parties hear a repeated intrusion tone. When the intruder hangs-up the original call parties are reconnected. Attempting to hold a dial inclusion call simply ends the intrusion. The inclusion cannot be parked.

- Intrusion features are controlled by the **Can Intrude** setting of the user intruding and the **Cannot Be Intruded** setting of user being intruded on. By default, no users can intrude and all users cannot be intruded.
- Intrusion features uses system conference resources during the call. If insufficient conference resource are available, the feature cannot be used.

The system support a range of other call intrusion methods in addition to this feature.

Details

- **Release**: 1.4+.
- **See also**: Call Intrude, Call Listen, Coaching Intrusion, Whisper Page.
- **Programmable Button Control**: ✓ Inclu.
- **Default Short Code**: ✗
- **Telephone Number**: ✓ Target extension number.

Example

N represents the extension to be intruded upon. For example, if a user dials *97*201# while extension 201 is on a call, then the user is intruding into extn. 201's current call.

- **Short Code**: *97*N#
- **Telephone Number**: N
- **Feature**: DialInclusion

Related links

Short Code Features on page 993

Dial Paging

This feature makes a page call to an extension or group. The target extension or group members must support page calls (that is be able to auto-answer calls).

- When paging, always use only one codec (the preferred). It is the system administrator's responsibility to ensure all the phones in the paging group support the codec.

Details

- **Telephone Number:** ✓ Extension or group number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ Page

- **See also**: Dial Direct.
- **Release**: 1.0+.

Related links

Short Code Features on page 993

Dial Physical Extension by Number

Dial a specified extension number regardless of the current user logged in at that extension and any forwarding, follow me or do not disturb settings applied by the current extension user. Note that the extension number used is the Base Extension number set against the extension configuration settings.

Details

- **Telephone Number**: ✓ Base Extension number.
- **Default Short Code**: ✓ *70*N# (U-Law only) (not on Server Edition)
- **Programmable Button Control**: ✓ PhyEx
- **See also**: Dial Physical Extension By Id, Priority Call.
- **Release:** 1.4+.

Example

The example below allows the extension with the base extension number 201 to be called regardless of the extension number of the user currently logged in at that extension.

- **Short Code**: *97
- **Telephone Number**: 201
- **Feature**: DialPhysicalExtnByNumber

Related links

Short Code Features on page 993

Dial Physical Extension By ID

Dial a specific extension using its system ID. This may be necessary in hot desking environments where some extensions have been created with no default extension number. Without an extension number, a call can not be made to that extension unless a short code is created.

Details

- **Telephone Number**: ✓ Extension ID
- **Default Short Code**: ✓ *71*N# (U-Law only)

- **Programmable Button Control**: ✓ DialP
- **See also**: DialPhysicalExtensionByNumber, Priority Call.
- **Release**: 1.4+.

Example

In the above example, if the telephone at extension ID 16 is not associated with an extension number, a user can dial *97 to connect to that phone. This may be useful in hot desking environments where some extensions may not have a dedicated base extension number.

- **Short Code**: *97
- **Telephone Number**: 16
- **Feature**: DialPhysicalNumberByID

Related links

Short Code Features on page 993

Dial Speech

This feature allows a short code to be created to force the outgoing call to use the Speech bearer capability.

Details

- **Telephone Number:** ✓ Telephone number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ DSpch
- **Release**: 1.0+.

Related links

Short Code Features on page 993

Dial V110

Sets the ISDN bearer capabilities to V110. The call is presented to local exchange as a "Data Call".

Details

- **Telephone Number**: ✓ Telephone number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ DV110
- **Release**: 1.0+.

Related links

Short Code Features on page 993

Dial V120

Sets the ISDN bear capabilities using V.120.

Details

- **Telephone Number**: ✓ Telephone number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ DV120
- **Release**: 1.0+.

Related links

Short Code Features on page 993

Dial Video

The call is presented to the local exchange as a "Video Call".

Details

- **Telephone Number**: ✓ Telephone number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ Dvide
- **Release**: 1.0+.

Related links

Short Code Features on page 993

Disable ARS Form

This feature can be used to put an ARS form out of service. It can be used with ARS forms for which an Out of Service Route has been configured in Manager. The short code feature Enable ARS Form can be used to return an ARS form to in service.

Details

- **Telephone Number**: ARS form number.

- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **See also**: Enable ARS Form
- **Release**: 4.0+.

Related links

Short Code Features on page 993

Disable Internal Forwards

This feature turns off the forwarding of internal calls for the user. It applies to Forward Unconditional, Forward on Busy and Forward on No Answer.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **See also**: Disable Internal Forwards Unconditional, Disable Internal Forwards Busy or No Answer, Cancel All Forwarding, Enable Internal Forwards, Enable Internal Forwards Unconditional, Enable Internal Forwards Busy or No Answer.
- **Release**: 3.2+.

Related links

Short Code Features on page 993

Disable Internal Forward Unconditional

This feature turns off the forwarding of internal calls for the user. It applies to Forward Unconditional only.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **See also**: Disable Internal Forwards, Disable Internal Forwards Busy or No Answer, Cancel All Forwarding, Enable Internal Forwards, Enable Internal Forwards Unconditional, Enable Internal Forwards Busy or No Answer.
- **Release**: 3.2+.

Related links

Short Code Features on page 993

Disable Internal Forward Busy or No Answer

This feature turns off the forwarding of internal calls for the user. It applies to Forward on Busy and Forward on No Answer.

Details

- **Telephone Number**: No
- **Default Short Code**: No
- **Programmable Button Control**: No
-
- **See also**: Disable Internal Forwards, Disable Internal Forwards Unconditional, Cancel All Forwarding, Enable Internal Forwards, Enable Internal Forwards Unconditional, Enable Internal Forwards Busy or No Answer.

Related links

Short Code Features on page 993

Display Msg

Allows the sending of text messages to digital phones on the local system.

Details

- **Telephone Number**: The telephone number takes the format `N";T"` where:
  - **N** is the target extension.
  - **T** is the text message. Note that the `";` before the text and the `"` after the text are required.
- **Default Short Code**: No
- **Programmable Button Control**: Displ

Example

Below is a sample of the short code setup. When used, the target extension will hear a single ring and then see the message. If the target extension is on a call then may need to scroll the display to a free call appearance in order to see the text message.

- **Telephone Number**: `N";Visitor in Reception"`
- **Feature**: Display Msg

- **Short Code**: `*78*N#`

Example: SIP Extension Message Waiting Indicator

You can use the Display Msg short code to turn an extension's message waiting indicator (MWI) on or off.

- **Telephone Number**: The telephone number takes the format `N";T"` where:
  - **N** is the target extension.
  - **T** is the text message. Note that the `";` before the text and the `"` after the text are required.
    - To turn MWI on, the telephone number must be `N";Mailbox Msgs=1"`
    - To turn MWI off, the telephone number must be `N";Mailbox Msgs=0"`
- **Default Short Code**: No

Example

Below is a sample of the short code setup to turn MWI on. When used, the target extension will receive a message directing it to turn the MWI on.

- **Short Code**: `*99*N#`
- **Feature**: `Display Msg`
- **Telephone Number**: `N";Mailbox Msgs=1"`

Example

Below is a sample of the short code setup to turn MWI off. When used, the target extension will receive a message directing it to turn the MWI off.

- **Short Code**: `*98*N#`
- **Feature**: `Display Msg`
- **Telephone Number**: `N";Mailbox Msgs=0"`

Related links

Short Code Features on page 993

Do Not Disturb Exception Add

This feature adds a number to the user's "Do Not Disturb Exception Numbers List". This can be an internal extension number or external ICLID. Calls from that number, except hunt group calls, will ignore the user's Do Not Disturb setting. For further details see Do Not Disturb (DND).

Details

- **Telephone Number**: Telephone number or ICLID. Up to 31 characters. For ICLID numbers any prefix added by the system must also be included.
- **Default Short Code**: *10*N#

- **Programmable Button Control**: DNDX+
- **See also**: Do Not Disturb Exception Delete, Do Not Disturb On, Do Not Disturb Off.

Example

N represents the number to be added to the user's "Do Not Disturb Exception List". For example, when a user has DND turned on and dials *10*4085551234#, incoming calls from telephone number (408) 555-1234. All other calls, except those numbers on the exception list hear busy tones or are redirected to voicemail if available.

- **Short Code**: *10*N#
- **Telephone Number**: N
- **Feature**: DoNotDisturbExceptionAdd

Example

In this example, the last number received by the user is added to their exception list.

- **Short Code**: *89
- **Telephone Number**: L
- **Feature**: DoNotDisturbExceptionAdd

Related links

Short Code Features on page 993

Do Not Disturb Exception Delete

This feature removes a number from the user's "Do Not Disturb Exception List". For further details see Do Not Disturb (DND).

Details

- **Telephone Number**: ✓ Telephone number or ICLID.
- **Default Short Code**: ✓ *11*N#
- **Programmable Button Control**: ✓ DNDX-
- **See also**: Do Not Disturb Exception Add, Do Not Disturb On, Do Not Disturb Off.
- **Release**: 1.0+.

Example

N represents the number to be deleted from the user's "Do Not Disturb Exception List". For example, when a user has DND turned on and the telephone number (408) 555-1234 in their "Do Not Disturb Exception List", dialing *10*4085551234# will remove this phone number from the list. Incoming calls from (408) 555-1234 will no longer be allowed through; instead they will hear busy tone or be redirected to voicemail if available.

- **Short Code**: *11*N#
- **Telephone Number**: N

- **Feature**: DoNotDisturbExceptionDel

Related links

Short Code Features on page 993

Do Not Disturb On

This feature puts the user into 'Do Not Disturb' mode. When on, all calls, except those from numbers in the user's exception list hear busy tones or are redirected to voicemail if available. For further details, see Do Not Disturb (DND).

- CCR is not supported in IP Office release 9.1 and later.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *08
- **Programmable Button Control**: ✓ DNDOn
- **See also**: Do Not Disturb Off, Do Not Disturb Exception Add, Do Not Disturb Exception Delete.
- **Release**: 1.0+.

Example

Below is a sample of the short code setup.

- **Short Code**: *08
- **Feature**: DoNotDisturbOn

Related links

Short Code Features on page 993

Do Not Disturb Off

Cancels the user's 'do not disturb' mode if set. For further details, see Do Not Disturb (DND).

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *09
- **Programmable Button Control**: ✓ DNDOf
- **See also**: Do Not Disturb On, Do Not Disturb Exception Add, Do Not Disturb Exception Delete.
- **Release**: 1.0+.

Example

This short code is a default within the system configuration. Below is a sample of the short code setup.

- **Short Code**: *09
- **Feature**: DoNotDisturbOff

Related links

Short Code Features on page 993

Enable ARS Form

This feature can be used to put an ARS form in service. It can be used with ARS forms that have been put out of service through Manager or the use of a Disable ARS Form short code.

Details

- **Telephone Number**: ARS form number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **Release**: 4.0+

Related links

Short Code Features on page 993

Enable Internal Forwards

This feature turns on the forwarding of internal calls for the user. It applies to Forward Unconditional, Forward on Busy and Forward on No Answer.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✗
- **Programmable Button Control:**✗
- **See also**: Disable Internal Forwards, Disable Internal Forwards Unconditional, Disable Internal Forwards Busy or No Answer, Cancel All Forwarding, Enable Internal Forwards Unconditional, Enable Internal Forwards Busy or No Answer.
- **Release**: 3.2+.

Related links

Short Code Features on page 993

Enable Internal Forward Unconditional

This feature turns on the forwarding of internal calls for the user. It applies to Forward Unconditional only.

Details

- **Telephone Number**: ✕
- **Default Short Code**: ✕
- **Programmable Button Control**: ✕
- **See also**: Disable Internal Forwards, Disable Internal Forwards Unconditional, Disable Internal Forwards Busy or No Answer, Cancel All Forwarding, Enable Internal Forwards, Enable Internal Forwards Busy or No Answer.
- **Release:** 3.2+.

Related links

Short Code Features on page 993

Enable Internal Forward Busy or No Answer

This feature turns on the forwarding of internal calls for the user. It applies to Forward on Busy and Forward on No Answer.

Details

- **Telephone Number**: ✕
- **Default Short Code**: ✕
- **Programmable Button Control**: ✕
- **See also**: Disable Internal Forwards, Disable Internal Forwards Unconditional, Disable Internal Forwards Busy or No Answer, Cancel All Forwarding, Enable Internal Forwards, Enable Internal Forwards Unconditional.
- **Release**: 3.2+.

Related links

Short Code Features on page 993

Extn Login

Extn Login allows a user who has been configured with a Login Code (User | Telephony | Supervisor Settings) to take over ownership of any extension. That user's extension number

becomes the extension number of the extension while they are logged. This is also known as ‘hot desking’.

- Hot desking is not supported for H175 and J129 telephones.
- When used, the user will be prompted to enter their extension number and then their log in code. Login codes of up to 15 digits are supported with **Extn Login** buttons. Login codes of up to 31 digits are supported with **Extn Login** short codes.
- When a user logs in, as many of their user settings as possible are applied to the extension. The range of settings applied depends on the phone type and on the system configuration.
- By default, on 1400 Series, 1600 Series, 9500 Series and 9600 Series phones, the user's call log and personal directory are accessible while they are logged in. This also applied to M-Series and T-Series telephones.
- On other types of phone, those items such as call logs and speed dials are typically stored locally by the phone and will not change when users log in and log out.
- If the user logging in was already logged in or associated with another phone, they will be automatically logged out that phone.

Details

- **Telephone Number**: ✓ Extension Number*Login Code. If just a single number is dialed containing no * separator, the system assumes that the extension number to use is the physical extension's Base Extension number and that the number dialed is the log in code.
- **Default Short Code**: ✓ *35*N#
- **Programmable Button Control**: ✓ Login
- **See also**: Extn Logout.
- **Release**: 1.0+.

Example: Individual Hot Desking

Based on the above sample short code, Paul (extension 204) can go to another phone (even if it is already logged in by another user) and log in as extension 204 by simply dialing 299. Once Paul has logged into this phone, extension 204 is logged out at Paul's original phone. For Paul to make use of this short code, his log in code must match that configured in the above short code. When Paul logs out of the phone he has "borrowed", his original extension will automatically be logged back in.

- **Short Code**: 299
- **Telephone Number**: 204*1234
- **Feature**: Extnlogin

Example: Log In

The default short code for logging into a phone is configured as shown below. N represents the users extension number followed by a * and then their log in code, for example *35*401*123#.

- **Short Code**: *35*N#
- **Telephone**: N

- **Feature**: ExtnLogin

Related links

Short Code Features on page 993

Extn Logout

This feature logs the user off the phone at which they are logged in. This feature cannot be used by a user who does not have a log in code or by the default associated user of an extension unless they are set to forced log in.

Details

- **Telephone Number**: ✗
- **Default Short Code:** ✓ *36
- **Programmable Button Control**: ✓ Logof
- **See also**: Extn Login.
- **Release**: 1.0+.

Example

Below is a sample short code using the Extn Logout feature. This short code is a default within the system configuration.

- **Short Code**: *36
- **Feature**: ExtnLogout

Related links

Short Code Features on page 993

Flash Hook

This feature sends a hook flash signal to the currently connected line if it is an analog line. Only supported for analog lines on the same system as the short code. See Centrex Transfer on page 909.

Details

- **Telephone Number**: Optional The telephone number field can be used to set the transfer destination number for a Centrex Transfer. In this case the use of the short code Forced Account Code and Forced Authorization Code are not supported and the Line Group Id must match the outgoing line to the Centrex service provider.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ Flash

- **Release**: 1.4+.

Example

Below is a sample short code using the Flash Hook feature.

- **Short Code**: *96
- **Feature**: FlashHook

Related links

Short Code Features on page 993

FNE Service

This short code feature is used for Mobile Call Control and one-X Mobile Client support.

Details

- **Telephone Number**: ✓ This number sets the required FNE function.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **Release**: 4.2+.

Related links

Short Code Features on page 993

Follow Me Here

Causes calls to the extension number specified to be redirected to the extension initiating the 'Follow Me Here'. If the redirected call receives a busy tone or is not answered, then the call behaves as though the User's extension had failed to answer. For further details, see Follow Me on page 865.

Details

Telephone Number: ✓ Extension to redirect to the dialing extension.

Default Short Code: ✓ *12*N#

Programmable Button Control: ✓ Here+

See also: Follow Me Here Cancel, Follow Me To.

Release: 1.0+.

Example

This feature is used at the Follow Me destination. N represents the extension number of the user wanting their calls redirected to that destination. For example, User A's extension is 224. However

they are working at extension 201 and want their calls redirected there. If the following short code is available, they can do this by dialing *12*224# at extension 201.

- **Short Code**: *12*N#
- **Telephone Number**: N
- **Feature**: FollowMeHere

Related links

Short Code Features on page 993

Follow Me Here Cancel

Cancels any Follow Me set on the specified extension. This action can only be performed at the extension to which the Follow Me Here is targetted. For further details, see Follow Me on page 865.

Details

- **Telephone Number**: ✓ Extension being redirected to the dialing extension.
- **Default Short Code**: ✓ *13*N#
- **Programmable Button Control:** ✓ Here-
- **See also**: Follow Me Here, Follow Me To.
- **Release**: 1.0+.

Example

This feature is used at the Follow Me destination. N represents the extension number of the user whose calls are being redirected to that destination. For example, User A's extension is 224. However they are working at extension 201 and so have set a Follow Me on their own extension to redirect their calls to 201. If the following short code is available, they can cancel the Follow Me by dialing *13*224# at extension 201.

Short Code: *13*N#

Telephone Number: N

Feature: FollowMeHereCancel

Related links

Short Code Features on page 993

Follow Me To

Causes calls to the extension to be redirected to the Follow Me destination extension specified. For further details, see Follow Me on page 865.

Details

- **Telephone Number**: ✓ Target extension number or blank (cancel Follow Me To)
- **Default Short Code**: ✓ *14*N#
- **Programmable Button Control**: ✓ FolTo
- **See also**: Follow Me Here, Follow Me Here Cancel.
- **Release:** 1.0+.

Example

This feature is used at the extension that wants to be redirected. N represents the extension number to which the user wants their calls redirected. For example, User A's extension is 224. However they are working at extension 201 and want their calls redirected there. If the following short code is available, they can do this by dialing *14*201# at extension 224.

- **Short Code**: *14*N#
- **Telephone Number**: N
- **Feature**: FollowMeTo

Related links

Short Code Features on page 993

Forward Hunt Group Calls On

Forward the user's hunt group calls (internal and external) to their forward number when the user has Forward Unconditional active. For further details see Forward Unconditional.

This option is only applied for calls to **Sequential** and **Rotary** type hunt groups. Calls from other types of hunt group types are not presented to the user when they have Forward Unconditional active. Note also that hunt group calls cannot be forwarded to another hunt group.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *50
- **Programmable Button Control**: ✓ FwdH+
- **See also**: Forward Hunt Group Calls Off, Forward Unconditional On, Forward Unconditional Off.
- **Release**: 1.0+.

Example

This short code is useful if the hunt group member temporarily uses another workstation and so does not require a permanent extension change.

- **Short Code**: *50
- **Feature**: ForwardHuntgroupCallsOn

Related links

Short Code Features on page 993

Forward Hunt Group Calls Off

This feature cancels the forwarding of the user's hunt group calls. For further details see Forward Unconditional.

Details

- **Telephone Number:** ✗
- **Default Short Code**: ✓ *51
- **Programmable Button Control**: ✓ FwdH-
- **See also**: Forward Hunt Group Calls On, Forward Unconditional On, Forward Unconditional Off.
- **Release**: 1.0+.

Example

Below is a sample of the short code setup.

- **Short Code**: *51
- **Feature**: ForwardHuntgroupCallsOff

Related links

Short Code Features on page 993

Forward Number

Sets the number to which the user's calls are redirected. This can be an internal or external number. The number is still subject to the user's call barring settings. For further details see Forward Unconditional.

This feature does not activate forwarding; it only sets the number for the forwarding destination.

This number is used for all forward types; Forward Unconditional, Forward on Busy and Forward on No Answer, unless the user has a separate Forward on Busy Number set for forward on busy and forward on no answer functions.

Details

- **Telephone Number:** ✓ Telephone number.
- **Default Short Code**: ✓ *07*N#
- **Programmable Button Control**: ✓ FwdNo

- **See also:** Forward On Busy Number.
- **Release**: 1.0+.

Example

N represents the forward destination. For example, if extension 224 wants to set the forwarding number to extension 201, the user can dial *07*201#.

- **Short Code**: *07N*#
- **Telephone Number**: N
- **Feature**: ForwardNumber

Related links

Short Code Features on page 993

Forward On Busy Number

Sets the number to which the user's calls are forwarded when Forward on Busy or Forward on No Answer are on. If no Forward on Busy Number is set, those functions use the Forward Number. For further details, see Forward on Busy on page 869.

This feature does not activate the forwarding, it only sets the number for the forwarding destination.

Details

- **Telephone Number**: ✓ Telephone number.
- **Default Short Code**: ✓ *57*N#
- **Programmable Button Control**: ✓ FwBNo
- **See also**: Forward Number.
- **Release**: 1.0+.

Example

N represents the extension number to be forwarded to. For example, if Paul (whose extension is 224) wants to set the forwarding number for his 'Forward on Busy' and/or 'Forward on No Answer' feature to extension 201, Paul can dial *57*201# followed by the short code for the forwarding function.

- **Short Code:** *57N*#
- **Telephone Number**: N
- **Feature**: ForwardOnBusyNumber

Related links

Short Code Features on page 993

Forward On Busy On

This feature enables forwarding when the user's extension is busy. It uses the Forward Number destination or, if set, the Forward on Busy Number destination. If the user has call appearance buttons programmed, the system will not treat them as busy until all the call appearance buttons are in use. For further details, see Forward on Busy on page 869.

Forward Internal (User | Forwarding) can also be used to control whether internal calls are forwarded.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *03
- **Programmable Button Control**: ✓ FwBOn
- **See also**: Forward On Busy Off, Cancel All Forwarding, Enable Internal Forward Busy or No Answer.
- **Release**: 1.0+.

Example

Below is a sample of the short code setup.

- **Short Code**: *03
- **Feature**: ForwardOnBusyOn

Related links

Short Code Features on page 993

Forward On Busy Off

This feature cancels forwarding when the user's extension is busy.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *04
- **Programmable Button Control**: ✓ FwBOf
- **See also**: Forward On Busy On, Cancel All Forwarding.
- **Release:** 1.0+.

Example

Below is a sample of the short code setup.

- **Short Code**: *04
- **Feature**: ForwardOnBusyOff

Related links

Short Code Features on page 993

Forward On No Answer On

This feature enables forwarding when the user's extension is not answered within the period defined by their No Answer Time. It uses the Forward Number destination or, if set, the Forward on Busy Number destination. For further details, see Forward on No Answer on page 871.

Forward Internal (User | Forwarding) can also be used to control whether internal calls are forwarded.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *05
- **Programmable Button Control**: ✓ FwNOn
- **See also**: Forward On No Answer Off, Cancel All Forwarding.
- **Release**: 1.0+.

Example

Below is a sample of the short code setup. Remember that the forwarding number for this feature uses the 'Forward on Busy Number'.

- **Short Code**: *05
- **Feature**: ForwardOnNoAnswerOn

Related links

Short Code Features on page 993

Forward On No Answer Off

This feature cancels forwarding when the user's extension is not answered.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *06
- **Programmable Button Control**: ✓ FwNOf
- **See also**: Forward On No Answer On.
- **Release**: 1.0+.

Example

Below is a sample of the short code setup.

- **Short Code**: *06
- **Feature**: ForwardOnNoAnswerOff

Related links

Short Code Features on page 993

Forward Unconditional On

This feature enables forwarding of all calls, except group calls, to the Forward Number set for the user's extension. To also forward hunt group calls, Forward Hunt Group Calls On must also be used. For further details, see Forward Unconditional on page 867.

Forward Internal (User | Forwarding) can also be used to control whether internal calls are forwarded.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓
- **Programmable Button Control**: ✓ FwUOn
- **See also**: Forward Unconditional Off.
- **Release**: 1.0+.

Example

Remember that this feature requires having a forward number configured.

- **Short Code**: *01
- **Feature**: ForwardUnconditionalOn

Related links

Short Code Features on page 993

Forward Unconditional Off

This feature cancels forwarding of all calls from the user's extension.

- This does not disable Forward on No Answer and or Forward on Busy if those functions are also on. For further details see Forward Unconditional.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *02
- **Programmable Button Control**: ✓ FwUOf
- **See also**: Forward Unconditional On.
- **Release:** 1.0+.

Example

Below is a sample of the short code setup.

- **Short Code**: *02
- **Feature:** ForwardUnconditionalOff

Related links

Short Code Features on page 993

Group Listen Off

Disables the group listen function on the user's extension. See Group Listen On on page 1046.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ GroupListenOn
- **Release**: 4.1+.

Related links

Short Code Features on page 993

Group Listen On

Using group listen allows callers to be heard through the phone's handsfree speaker but to only hear the phone's handset microphone. When group listen is enabled, it modifies the handsfree functionality of the user's phone in the following manner

- When the user's phone is placed in handsfree/speaker mode, the speech path from the connected party is broadcast on the phone speaker but the phone's base microphone is disabled.
- The connected party can only hear speech delivered through the phone's handset microphone.

- Group listen is not supported for IP phones or when using a phone's **HEADSET** button.
- For T-Series and M- Series phones, this option can be turned on or off during a call. For other phones, currently connected calls are not affected by changes to this setting, instead group listen must be selected before the call is connected.

  Group listen is automatically turned off when the call is ended.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ GroupListenOn
- **Release**: 4.1+.

Related links

Short Code Features on page 993

Headset Toggle

Toggles between the use of a headset and the telephone handset.

Details

- **Telephone Number:**✗
- **Default Short Code:**✗
- **Programmable Button Control**: ✓ HdSet
- **Release**: 1.4+.

Example

Below is a sample short code using the Headset Toggle feature. This short code can be used to toggle the feature on/off. If an Avaya supported headset is connected to your telephone, this short code can be used to toggle between using the headset and the telephone handset.

- **Short Code:** *55
- **Feature**: HeadsetToggle

Related links

Short Code Features on page 993

Hold Call

This uses the Q.931 Hold facility, and "holds" the incoming call at the ISDN exchange, freeing up the ISDN B channel. The Hold Call feature "holds" the current call to a slot. The current call is

always automatically placed into slot 0 if it has not been placed in a specified slot. Only available if supported by the ISDN exchange.

Details

- **Telephone Number**: ✓ Exchange hold slot number or blank (slot 0).
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ Hold
- **See also**: Hold CW, Hold Music, Suspend Call.
- **Release:** 1.0+.

Example

Below is a sample short code using the Hold Call feature. This short code is a default within the system configuration. N represents the exchange hold slot number you want to hold the call on. For example, while connected to a call, dialing *24*3# will hold the call onto slot 3 on the ISDN.

- **Short Code**: *24*N#
- **Telephone Number**: N
- **Feature**: HoldCall

Related links

Short Code Features on page 993

Hold CW

This uses the Q.931 Hold facility, and "holds" the incoming call at the ISDN exchange, freeing up the ISDN B channel. The Hold CW feature "holds" the current call to an exchange slot and answers the call waiting. The current call is always automatically placed into slot 0 if it has not been placed in a specified slot. Only available if supported by the ISDN exchange.

Details

- **Telephone Number**: ✓ Exchange slot number or blank (slot 0).
- **Default Short Code**: ✓ *27*N# (A-Law only) (not on Server Edition)
- **Programmable Button Control**: ✓ HoldCW
- **See also**: Hold Call, Suspend Call.
- **Release**: 1.0+.

Example

Below is a sample short code using the Hold CW feature.

- **Short Code**: *27*N#
- **Feature**: HoldCW

Related links

Short Code Features on page 993

Hold Music

This feature allows the user to check the system's music on hold. See Music On Hold for more information.

Details

- **Telephone Number**: Optional. If no number is specified, the default system source is assumed. The system supports up to 4 hold music sources, numbered 1 to 4. 1 represents the System Source. 2 to 4 represent the Alternate Sources.
- **Default Short Code**: ✓
- ***34N;** where N is the number of the hold music source required.
- **Programmable Button Control**: ✓ Music
- **Release**: 1.0+.

Example

Below is a sample short code using the Hold Music feature. This short code is a default within the configuration.

- **Short Code**: *34N;
- **Feature**: HoldMusic

Related links

Short Code Features on page 993

Hunt Group Disable

This feature disables the user's membership of the specified hunt group. They will no longer receive call to that hunt group until their membership is enabled again. To use this feature, you must already belong to the hunt group. See also Hunt Group Enable.

Details

- **Telephone Number**: ✓ Group number.
- **Default Short Code:** ✗
- **Programmable Button Control**: ✓ HGDis
- **See also**: Hunt Group Enable.
- **Release:** 1.0+.

Example

N represents the hunt group number from which the user wants to be disabled from. For example, if Paul wants to be disabled from the Sales hunt group (extn. 500), he needs to dial *90*500#.

- **Short Code:** *90*N#
- **Telephone Number**: N

- **Feature**: HuntGroupDisable

Related links

Short Code Features on page 993

Hunt Group Enable

This feature enables the user's membership of a hunt group so they can begin to receive calls to the specified hunt group. To use this feature, the user must already belong to the hunt group. This short code can not be used to add someone to a hunt group, that must be done within Manager's Hunt Group form.

Details

- **Telephone Number:** ✓ Group number.
- **Default Short Code:** ✗
- **Programmable Button Control**: ✓ HGEna
- **See also**: Hunt Group Disable.
- **Release**: 1.0+. Previously in Release 3.2 the **Set Hunt Group Night Service**, **Set Hunt Group Out of Service** and **Hunt Group Enable** short code features toggled. That behaviour is not supported in 4.0 and higher.

Example

This short code can be used to turn the feature on. N represents the hunt group number for which the user wants to start receiving calls. For example, if Paul is already a member of the sales hunt group (extn. 500) but has changed his availability status for that hunt group using hunt group disable, he can make himself available for receiving calls to the Sales hunt group again by dialing *91*500#.

- **Short Code:** *91*N#
- **Telephone Number**: N
- **Feature:** HuntGroupEnable

Related links

Short Code Features on page 993

Last Number Redial

This feature allows an extension to redial the last number they dialed.

Details

- **Telephone Number**: ✗

- **Default Short Code**: ✕
- **Programmable Button Control**: ✕
- **Release:** 3.0+.

Related links

Short Code Features on page 993

MCID Activate

This feature should only be used in agreement with the ISDN service provider and the appropriate local legal authorities. It allows users with **Can Trace Calls** (**User | Telephony | Supervisor Settings**) set to trigger a malicious call trace of their previous call at the ISDN exchange. Refer to Telephone Features Malicious Call Tracing for further details.

- Currently, in Server Edition network, MCID is only supported for users using an MCID button and registered on the same IP500 V2 Expansion system as the MCID trunks.

Details

- **Telephone Number**: ✕
- **Default Short Code**: ✕
- **Programmable Button Control:** Advanced | Miscellaneous | MCID Activate.
- **Release**: 4.0+.

Related links

Short Code Features on page 993

Mobile Twinned Call Pickup

This short code feature allows the user to pickup a call ringing or connected at the destination of their mobile twinning number. This short code can only be used from the primary extension which is being used for the twinning operation.

Note that the use of mobile twinning requires entry of a Mobile Twinning license and may be subject to a time profile.

Details

- **Telephone Number**: ✕
- **Default Short Code:**✕
- **Programmable Button Control:**✕
- **See also**: Set Mobile Twinning Number, Set Mobile Twinning On, Set Mobile Twinning Off.

- **Release**: 3.2+.

Related links

Short Code Features on page 993

Off Hook Station

Enables or disables whether the user's extension acts as a fully handsfree unit. Typically this is used when the answering and clearing of calls is done through an application. For more details see Off Hook Station (User | Telephony | Call Settings).

Details

- **Telephone Number**: ✓ "Y" for on or "N" for off.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ OHStn
- **Release**: 1.0+.

Example: Turning the off hook station off

- **Short Code**: *89
- **Telephone Number**: N
- **Feature**: OffHookStation

Example: Turning the off hook station on

- **Short Code**: *98
- **Telephone Number**: Y
- **Feature**: OffHookStation

Related links

Short Code Features on page 993

Outgoing Call Bar Off

Allows a user to switch off their outgoing call bar status. The short code user must enter their log in code, if set, in order to be successful.

If you add a short code using this feature to a system it is recommended that you also assign a login code to the No User user to prevent the short code being used to change the status of that user.

Details

- **Telephone Number**: ✓ The user's log in code.
  - System phone users can use *<target user>*<system phone user's login code>*.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **Release**: 4.1+ (Added to Release 4.1 2008Q2 Maintenance release).

Example

The user has a **Login Code** of **1234**. To use the short code below, the user must dial ***59*1234#**.

- **Short Code**: *59*N#
- **Telephone Number**: N
- **Feature**: Outgoing Call Bar Off.

Example

A user set as a system phone can also switch off the Outgoing Call Bar status of another user. This is done using their own login code. For example the system phone 401 with login code 1234 can switch off the outgoing call bar status of extension 403 as follows:

- ***59*403*1234**

Related links

Short Code Features on page 993

Outgoing Call Bar On

Allows a user to switch on their outgoing call bar status.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **Release**: 4.1+ (Added to Release 4.1 2008Q2 Maintenance release).

Example

To use the short code below, the user must dial ***58**.

- **Short Code**: *58
- **Telephone Number**: <blank>
- **Feature**: Outgoing Call Bar On.

Related links

Short Code Features on page 993

Private Call Off

Short codes using this feature turn off private call status for the user if set. The short code features Private Call and Private Call On can be used to turn private call on.

- When on, any subsequent calls cannot be intruded on until the user's private call status is switched off. The exception is Whisper Page which can be used to talk to a user on a private call.
- Note that use of private calls is separate from the user's intrusion settings. If the user's **Cannot be Intruded** (User | Telephony | Supervisor Settings) setting is enabled, switching private calls off does not affect that status. To allow private calls to be used to fully control the user status, **Cannot be Intruded** (User | Telephony | Supervisor Settings) should be disabled for the user.

Details

- **Telephone Number:** ✕
- **Default Short Code**: ✕
- **Programmable Button Control**: Advanced | Call | Private Call.
- **Release**: 4.0+.

Related links

Short Code Features on page 993

Private Call On

Short codes using this feature turn on the private call settings for the user regardless.

- When on, any subsequent calls cannot be intruded on until the user's private call status is switched off. The exception is Whisper Page which can be used to talk to a user on a private call.
- Note that use of private calls is separate from the user's intrusion settings. If the user's **Cannot be Intruded** (User | Telephony | Supervisor Settings) setting is enabled, switching private calls off does not affect that status. To allow private calls to be used to fully control the user status, **Cannot be Intruded** (User | Telephony | Supervisor Settings) should be disabled for the user.
- Private call status can be switched off using a short code with the Private Call Off feature or a programmed button set to the Private Call action. To enable private call status for a single following call only the Private Call short code feature should be used.

Details

- **Telephone Number**: ✕
- **Default Short Code**: ✕

- **Programmable Button Control**: Advanced | Call | Private Call.
- **Release:** 4.0+.

Related links

Short Code Features on page 993

Priority Call

This feature allows the user to call another user even if they are set to 'do not disturb'. Priority calls to a user without DND will follow forwarding and follow me settings but will not go to voicemail.

Details

- **Telephone Number:** ✓ Extension number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ PCall
- **See also**: DialPhysicalExtensionByNumber, DialPhysicalNumberByID.
- **Release**: 1.0+.

Example

N represents the extension number to be called, despite the extension being set to 'do not disturb'. For example, if extension 201 has 'do not disturb' enabled, a user can dial *71*201# and still get through. This short code is useful for companies that frequently use the 'do not disturb' feature and can be given to Managing Directors or people who may need to get through to people regardless of their 'do not disturb' status.

- **Short Code:** *71*N#
- **Telephone Number**: N
- **Feature**: PriorityCall

Related links

Short Code Features on page 993

Record Message

This short code feature is used to record hunt group announcements on Embedded Voicemail, see Hunt Group | Announcements. Release 5.0+: It is also used to record mailbox user name prompts for the auto attendant **Dial by Name** function.

Details

- **Telephone Number**: ✓
  - For a hunt group queue announcement, use the hunt group extension number followed by **".1"**.

- For a hunt group still queue announcement, use the hunt group extension number followed by **".2"**.
- For a mailbox user name prompt, use the user extension number followed by **".3"**.

- **Default Short Code**: ✓ *91N; and *92N; (not on Server Edition)
- **Programmable Button Control**: ✗
- **Release**: 4.0+.

Example

For a hunt group with extension number 300, the default short codes ***91N;/Record Message/N".1"** and ***92N;/Record Message/N".2"** can be used to allow recording of the announcements by dialing ***91300#** and ***92300#**.

To allow users to record their own name prompt, the short code ***89#/Record Message/E."3"** can be used. The **E** is replace by the extension number of the dialing user.

Related links

Short Code Features on page 993

Relay On

This feature closes the specified switch in the system's external output (EXT O/P) port.

This feature is not supported on Linux based systems. For Server Edition, this option is only supported on Expansion System (V2) units.

Details

- **Telephone Number**: ✓ Switch number (1 or 2).
- **Default Short Code**: ✓ *39 (Switch 1), *42 (Switch 2), *9000*.
- **Programmable Button Control:** ✓ Rely+
- **See also:** Relay Off, Relay Pulse.
- **Release**: 1.0+.

Example

This short code is a default within the system configuration. This short code is useful for companies that have external devices, such as door controls, connected to the system. Based on this sample short code, a user dialing *42 is closing switch number 2 to activate an external device.

- **Short Code**: *42
- **Telephone Number**: 2
- **Feature**: RelayOn

Analog Modem Control

On systems with an analog trunk card in the control unit, the first analog trunk can be set to answer V.32 modem calls. This is done by either selecting the Modem Enabled option on the

analog line settings or using the default short code *9000* to toggle this service on or off. This short code uses the **RelayOn** feature with the Telephone Number set to "MAINTENANCE". Note that the short code method is always returned to off following a reboot or if used for accessing the system date and time menu.

IP500 ATM4 Uni Trunk Card Modem Support It is not required to switch the card's modem port on/off. The trunk card's V32 modem function can be accessed simply by routing a modem call to the RAS service's extension number. The modem call does not have to use the first analog trunk, instead the port remains available for voice calls.

Related links

Short Code Features on page 993

Relay Off

This feature opens the specified switch in the system's external output (EXT O/P) port.

Details

- **Telephone Number**: ✓ Switch number (1 or 2).
- **Default Short Code**: ✓ *40 (Switch 1), *43 (Switch 2)
- **Programmable Button Control:** ✓ Rely-
- **See also**: Relay On, Relay Pulse.
- **Release:** 1.0+.

Example

This short code is a default within the system configuration. This short code is useful for companies that have external devices, such as door controls, connected to the system. Based on this sample short code, a user dialing *43 is opening switch number 2 to activate an external device.

- **Short Code**: *43
- **Telephone Number**: 2
- **Feature**: RelayOff

Related links

Short Code Features on page 993

Relay Pulse

This feature closes the specified switch in the system's external output (EXT O/P) port for 5 seconds and then opens the switch.

Details

- **Telephone Number**: ✓ Switch number (1 or 2).
- **Default Short Code**: ✓ *41 (Switch 1), *44 (Switch 2)
- **Programmable Button Control**: ✓ Relay
- **See also**: Relay On, Relay Off.
- **Release**: 1.0+.

Example

This short code is a default within the system configuration. This short code is useful for companies that have external devices, such as door controls, connected to the system. Based on this sample short code, a user dialing *44 is opening switch number 2 to activate an external device.

- **Short Code**: *44
- **Telephone Number**: 2
- **Feature**: RelayPulse

Related links

Short Code Features on page 993

Resume Call

Resume a call previously suspended to the specified ISDN exchange slot. The suspended call may be resumed from another phone/ISDN Control Unit on the same line.

Details

- **Telephone Number**: ✓ Exchange suspend slot number.
- **Default Short Code**: ✓ *23*N# (A-Law only) (not on Server Edition)
- **Programmable Button Control**: ✓ Resum
- **See also**: Suspend Call.
- **Release**: 1.0+.

Example

Below is sample short code using the Resume Call feature. N represents the exchange slot number from which the call has been suspended. For example, if a user has suspended a call on slot number 4, this user can resume that call by dialing *23*4#.

- **Short Code:** *23*N#
- **Telephone Number**: N
- **Feature:** ResumeCall

Related links

Short Code Features on page 993

Retrieve Call

Retrieves a call previously held to a specific ISDN exchange slot.

Details

- **Telephone Number**: ✓ Exchange hold slot number.
- **Default Short Code:** ✓ *25*N# (A-Law only) (not on Server Edition)
- **Programmable Button Control**: ✓ Retriv
- **See also**: Hold Call.
- **Release**: 1.0+.

Example

Below is sample short code using the Retrieve Call feature. N represents the exchange slot number from which the call has been placed on hold. For example, if a user has placed a call hold on slot number 4, the user can resume that call by dialing *25*4#.

- **Short Code**: *25*N#
- **Telephone Number**: N
- **Feature**: RetrieveCall

Related links

Short Code Features on page 993

Ring Back When Free

This feature sets a ringback on the specified extension. This sets a 'ringback when free' on an extension currently on a call or a 'ringback when next used' for an extension that is free but does not answer.

When the target extension is next used or ends its current call, the users is rung and when they answer a call is made to the target extension.

Details

- **Telephone Number**: ✓ Target extension number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ RBak+
- **See also**: Cancel Ring Back When Free.
- **Release**: 1.0+.

Example

N represents the target extension from which you want to receive the callback. For example, if you call extension 201 but the line is busy, hang up and then dial *71*201#. When extension 201

disconnects from its current call, your phone will ring. Once you pick up the phone, extension 201's line will start ringing to indicate an incoming call.

- **Short Code**: *71*N#
- **Telephone Number:** N
- **Feature**: RingBackWhenFree

Related links

Short Code Features on page 993

Secondary Dial Tone

Secondary dial tone is a system feature to generate a secondary dial tone after the user has begun dialing an external number. This dial tone is then played until the number dialing and an external trunk seized.

- Pre-Release 4.0: Secondary dial tone is triggered through the use of the secondary dial tone short code feature.
- Release 4.0+: The use of this short code feature has been replaced by the Secondary Dial Tone check box option on ARS forms.

Details

- **Telephone Number**: ✓ Digit which triggers secondary dial tone.
- **Default Short Code**: ✓ 9 (U-Law only)
- **Programmable Button Control**: ✗
- **Release**: 1.0+.

Example

For pre-4.0 systems secondary dial tone works in two parts. The following system short code will trigger secondary dial tone. To use it to trigger secondary dial tone and then continue dialing, other user, user rights and system short codes should begin with [9].

- **Short Code:** 9
- **Telephone Number**: .
- **Feature**: Secondary Dial Tone

Related links

Short Code Features on page 993

Set Absent Text

This feature can be used to select the user's current absence text. This text is then displayed to internal callers who have suitable display phones or applications. It doesn't changes the users

status. The absence text message is limited to 128 characters. Note however that the amount displayed will depend on the caller's device or application.

The text is displayed to callers even if the user has forwarded their calls or is using follow me. Absence text is supported across a multi-site network.

Details

- **Telephone Number**: ✓ The telephone number should take the format **"y,n,text"** where:
  - **y** = 0 or 1 to turn this feature on or off.
  - **n** = the number of the absent statement to use, see the list below:

0 = None.	4 = Meeting until.	8 = With cust. til.
1 = On vacation until.	5 = Please call.	9 = Back soon.
2 = Will be back.	6 = Don't disturb until.	10 = Back tomorrow.
3 = At lunch until.	7 = With visitors until.	11 = Custom.

  - **text** = any text to follow the absent statement.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ Absnt
- **Release**: 1.0+.

Example

The following short code can be used to turn an absent text message on:

- **Short Code**: *88
- **Telephone Number**: "1,5,me on 208"
- **Line Group ID**: 0
- **Feature**: SetAbsentText

Example

The following short code could be used to turn this facility off. In the Telephone Number the first 0 is used to turn this facility off and the second 0 is used to select the absent statement "None".

- **Short Code:** *89
- **Telephone Number**: "0,0"
- **Line Group ID**: 0
- **Feature**: SetAbsentText

Related links

Short Code Features on page 993

Set Account Code

This short code feature is used to allow system users to enter a valid account code prior to making a phone call. Once this short code is set up, any existing account code in the system configuration can be used in conjunction with it.

This short code feature is essential for allowing analog phone users to enter account codes as they cannot enter account code through the phone during a call or after dial a number.

Details

- **Telephone Number**: ✓ A valid account code.
- **Default Short Code:**✗
- **Programmable Button Control**: ✓ Acct.
- **Release:** 2.1+.

Example

In this example, N represents any valid account code. For the purpose of this example, we will imagine the account code to be 1234. Once this short code is created, a user can dial 11*1234# to get a dial tone for dialing the restricted telephone number or the phone number needing to be tracked for billing purposes.

- **Short code**: 11*N#
- **Telephone Number**: N
- **Feature**: SetAccountCode

Related links

Short Code Features on page 993

Set Authorization Code

This short code feature is only available on systems configured to use authorization codes. See Authorization Codes. The feature is used to allow a user to enter a valid authorization code prior to making a phone call.

This short code feature is essential for allowing analog phone users to enter authorization codes. Note that the authorization code must be associated with the user or the user rights to which the user belongs.

Details

- **Telephone Number**: ✓ A valid authorization code.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **Release:** 3.2+.

Related links

Short Code Features on page 993

Set Fallback Twinning Off

This feature can be used by users to disable fallback twinning operation. This feature requires the user to have a mobile twinning number set.

Fallback twinning redirects calls to the user's configured mobile twinning number when the system cannot detect a connection to the user's normal registered extension. This feature can be used without mobile twinning itself being enabled.

Details

- **Telephone Number:** ✕
- **Default Short Code:** ✕
- **Programmable Button Control:** ✕

Related links

Short Code Features on page 993

Set Fallback Twinning On

This feature can be used by users to enable fallback twinning operation. This feature requires the user to have a mobile twinning number set.

Fallback twinning redirects calls to the user's configured mobile twinning number when the system cannot detect a connection to the user's normal registered extension. This feature can be used without mobile twinning itself being enabled.

Details

- **Telephone Number:** ✕
- **Default Short Code:** ✕
- **Programmable Button Control:** ✕

Related links

Short Code Features on page 993

Set Hunt Group Night Service

This feature puts the specified hunt group into Night Service mode.

Setting and clearing hunt group night service can be done using either manual controls or using a system time profile. The use of both methods to control the night service status of a particular hunt group is not supported.

This function is not supported between systems in a multi-site network. It can only be used by a user currently logged onto the same system as hosting the hunt group.

Details

- **Telephone Number:** ✓ Hunt group extension number. If left blank, the short code will affect all hunt groups of which the user is a member.
  - The **Set Hunt Group Night Service** and **Clear Hunt Group Night Service** short code and button features can be used to switch an SSL VPN service off or on respectively. The service is indicated by setting the service name as the telephone number or action data. Do not use quotation marks.
- **Default Short Code**: ✓ *20*N#
- **Programmable Button Control:** ✓ HGNS+
- **See also**: Set Hunt Group Out Of Service, Clear Hunt Group Night Service, Clear Hunt Group Out Of Service.
- **Release**: 1.0+.

Example

This short code is a default within the system configuration. N represents the telephone number of the hunt group to be placed into "Night Service" mode. For example, when *20*201# is dialed, the hunt group associated with extension 201 will be placed into "Night Service" mode.

- **Short Code**: *20*N#
- **Telephone Number**: N
- **Feature**: SetHuntGroupNightService

Related links

Short Code Features on page 993

Set Hunt Group Out Of Service

This feature manually puts the specified hunt group into Out of Service mode. If a time profile has also been defined to control hunt group night service, the action may vary:

- **Set Hunt Group Out of Service** can be used to override a time profile and change a hunt group from night service to out of service.

Details

- **Telephone Number**: ✓ Hunt group extension number. For Release 4.0+, if left blank, the short code will affect all hunt groups of which the user is a member.
- **Default Short Code**: ✗

- **Programmable Button Control**: ✓ HGOS+
- **Release**: 1.0+.

Example

Below is a sample short code using the **Set Hunt Group Out Of Service** feature. N represents the telephone number of the hunt group to be placed into "Out of Service" mode. For example, when *56*201# is dialed, the hunt group associated with extension 201 will be placed into "Out of Service" mode.

- **Short Code**: *56*N#
- **Telephone Number:** N
- **Feature**: SetHuntGroupOutOfService

Related links

Short Code Features on page 993

Set Inside Call Seq

This feature allows the user to select the ringing used on their analog extension for internal calls.

Details

- **Telephone Number:** ✓ 0 to 10.
  - The number sets to the required ring pattern. See Ring Tones on page 775.
  - The numbering starts at 0 for Default Ring, 1 for Ring Normal, 2 for RingType1, and so on.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ ICSeq
- **See also**: Set Ringback Seq, Set Inside Call Seq.
- **Release**: 1.0+.

Example

This Short Code allows a user to change their inside call pattern. N represents the number corresponding to the Call Sequence the user wishes to choose.

- **Short Code:** *80*N#
- **Telephone Number**: N
- **Feature**: SetInsideCallSeq

Related links

Short Code Features on page 993

Set Mobile Twinning Number

This short code feature can be used to set a mobile twinning number. The destination can be any external number the user is able to dial normally. It should include any prefix if necessary.

Details

- **Telephone Number**: ✓ Twinning destination.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **See also**: Set Mobile Twinning On, Set Mobile Twinning Off, Mobile Twinned Call Pickup.
- **Release**: 3.2+.

Related links

Short Code Features on page 993

Set Mobile Twinning On

This short code feature turns on the user's mobile twinning. It requires a mobile twinning number to have been set for the user. That can be done through using the Set Mobile Twinning Number short code feature or through the User | Twinning tab within Manager.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **See also**: Set Mobile Twinning Off, Set Mobile Twinning Number, Mobile Twinned Call Pickup.
- **Release**: 3.2+.

Related links

Short Code Features on page 993

Set Mobile Twinning Off

This short code feature turns off the user's mobile twinning.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✗

- **Programmable Button Control**: ✗
- **See also**: Set Mobile Twinning On, Set Mobile Twinning Number, Mobile Twinned Call Pickup.
- **Release:** 3.2+.

Related links

Short Code Features on page 993

Set No Answer Time

This short code feature allows the user to change their No Answer Time (User | Telephony | Call Settings).

Details

- **Telephone Number**: ✓ Time in seconds.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ NATim
- **See also**: Set Wrap Up Time.
- **Release**: 1.0+.

Example

This short code allows a user to change the length of time they have to answer the phone before it goes to divert or voicemail. N represents the number of seconds. For example, if a user wants to set the no answer time to 15 seconds, the following information needs to be entered: *81*15#.

- **Short Code**: *81*N#
- **Telephone Number**: N
- **Feature**: SetNoAnswerTime

Related links

Short Code Features on page 993

Set Outside Call Seq

This feature allows the user to select the ringing used on their analog extension for external calls.

Details

- **Telephone Number**: ✓ 0 to 10.
  - The number sets to the required ring pattern. See Ring Tones on page 775.
  - The numbering starts at 0 for Default Ring, 1 for Ring Normal, 2 for RingType1, and so on.

- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ OCSeq
- **See also**: Set Ringback Seq, Set Outside Call Seq.
- **Release**: 1.0+.

Example

This short code allows a user to change the ringing tone for an external call. N represents the number corresponding to the Call Sequence the user wishes to choose.

- **Short Code**: *81*N#
- **Telephone Number**: N
- **Feature**: SetOutsideCallSeq

Related links

Short Code Features on page 993

Set Ringback Seq

This feature allows the user to select the ringing used on their analog extension for ringback calls.

Details

- **Telephone Number**: ✓ 0 to 10.
  - The number sets to the required ring pattern. See Ring Tones on page 775.
  - The numbering starts at 0 for Default Ring, 1 for Ring Normal, 2 for RingType1, and so on.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ RBSeq
- **See also:** Set Outside Call Seq, Set Inside Call Seq.

Example

This short code allows a user to change the ringing tone for a ringback call. N represents the number corresponding to the ring tone the user wishes to choose.

- **Short Code**: *81*N#
- **Telephone Number**: N
- **Feature:** SetRingbackSeq

Related links

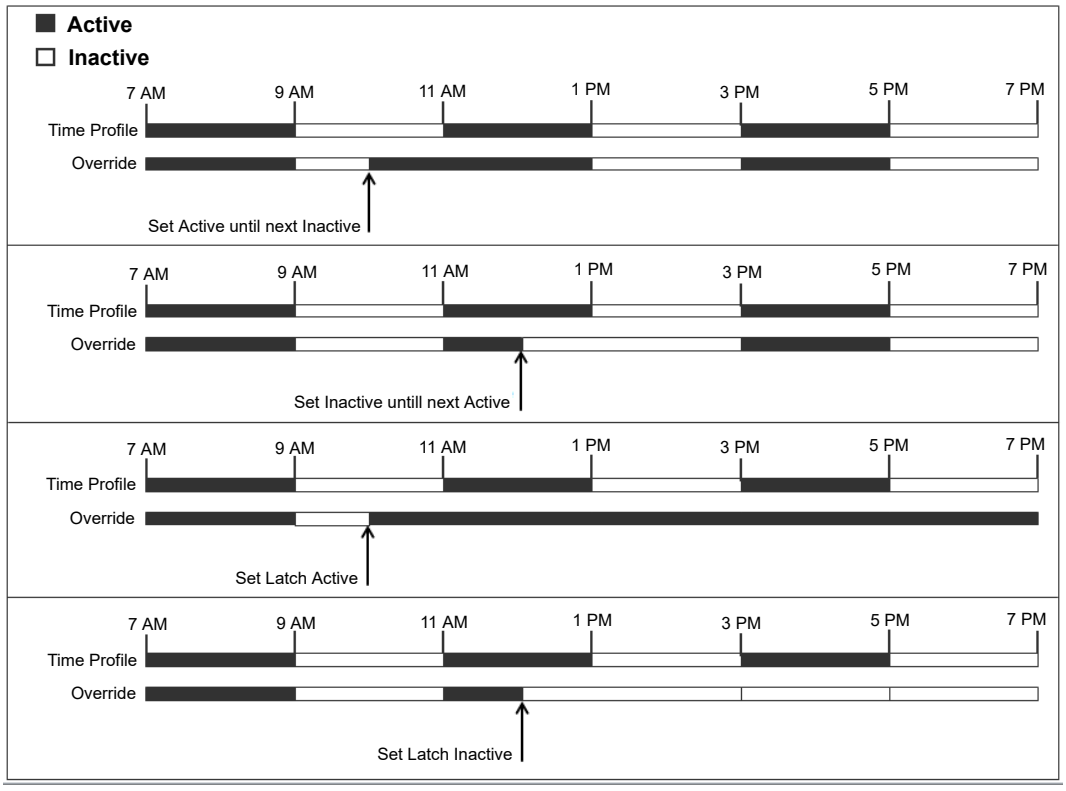
Short Code Features on page 993

Set Time Profile

You can manually override a time profile. The override settings allow you to mix timed and manual settings.

Five short codes can be configured.

Short Code Name	Description
Set Time Profile Timed Operation	No override. The time profile operates as configured.
Set Time Profile Active Until Next Timed Inactive	Use for time profiles with multiple intervals. Select to make the current timed interval active until the next inactive interval.
Set Time Profile Inactive Until Next Timed Active	Use for time profiles with multiple intervals. Select to make the current active timed interval inactive until the next active interval.
Set Time Profile Latch Active	Set the time profile to active. Timed inactive periods are overridden and remain active.
Set Time Profile Latch Inactive	Set the time profile to inactive. Timed active periods are overridden and remain active.



Details

- **Telephone Number**: Time profile name.
-
- **Default Short Code**: No.
- **Programmable Button Control**: Yes: Time Profile

Related links

Short Code Features on page 993

Set Wrap Up Time

Allows users to change their Wrap-up Time (User | Telephony | Call Settings) setting.

- Other phones or applications monitoring the user's status will indicate the user as still being busy (on a call).
- Hunt group calls will not be presented to the user.
- If the user is using a single line set, direct calls also receive busy treatment. If the user is using a mutli-line set (multiple call appearances), direct calls to them will ring as normal.
- It is recommended that this option is not set to less than the default of 2 seconds. 0 is used to allow immediate ringing.
- For users set as an CCR Agent, the After Call Work Time (User | Telephony | Supervisor Settings) setting should be used.

Details

- **Telephone Number**: ✓ Time in seconds.
- **Default Short Code**: ✗
- **Programmable Button Control:** ✓ WUTim
- **See also**: Set No Answer Time.
- **Release:** 1.0+.

Example

N represents the number of seconds. For example, if a user wants to set her/his wrap up time to 8 seconds, this user would dial *82*5#. This short code is useful in a "call center" environment where users may need time to log call details before taking the next call. If set to 0 the user does not receive any calls. It is recommended that this option is not set to less than the default of 2 seconds.

- **Short Code**: *82*N#
- **Telephone Number**: N
- **Feature**: SetWrapUpTime

Related links

Short Code Features on page 993

Speed Dial

Each system directory and personal directory number stored in the configuration can be optionally assigned an index number. That index number can then be used by M-Series and T-Series phone users to dial the directory number. This short code feature allows the creation of short codes to perform the same function. However, the short code is diallable from any type of telephone extension on the system.

For example:

- If **Feature 0** is followed by a 3-digit index number in the range 000 to 999, the system directory record with the matching index number is dialed.
- If **Feature 0** is followed by ***** and a 2-digit index number in the range 00 to 99, the personal directory record with the matching index number is dialed. Alternatively Feature 0 can be followed by 00# to 99#. Note: Release 10.0 allows users to have up to 250 personal directory entries. However, only 100 of those can be assigned index numbers.

Details

- **Telephone Number**: ✓ System directory entry index number (000 to 999) or personal directory entry index number (00 to 99).
- **Default Short Code**: ✗
- **Programmable Button Control:** ✗
- **Release**: 8.1.

Example

Using the example below, a user is able to dial *0 and then either a 2 digit code for an indexed personal directory entry or a 3 digit code for an indexed system directory entry.

- **Short Code**: *0N#
- **Telephone Number**: N
- **Feature**: Speed Dial

Related links

Short Code Features on page 993

Shutdown Embedded Voicemail

Allows the Embedded Voicemail service provided by an Avaya memory card in a control unit to be shut down. To restart the service, a **Startup Embedded Voicemail** short code should be used.

The short code has the following effects:

1. Immediately disconnect all current users within Embedded Voicemail. This is not a polite shutdown.
2. Mark the Embedded Voicemail as inactive so that it will not receive any new calls.

Details

- **Telephone Number**: ✗
- **Default Short Code:**✗
- **Programmable Button Control:**✗
- **Release**: 4.0+ (Added in the Release 4.0 Q2 2007 maintenance release).

Related links

Short Code Features on page 993

Stamp Log

The stamp log function is used to insert a line into any System Monitor trace that is running. The line in the trace indicates the date, time, user name and extension plus additional information. The line is prefixed with **LSTMP: Log Stamped** and a log stamp number. When invoked from a Avaya phone with a display, **Log Stamped#** is also briefly displayed on the phone. This allows users to indicate when they have experienced a particular problem that the system maintainer want them to report and allows the maintainer to more easily locate the relevant section in the monitor trace.

The log stamp number is set to 000 when the system is restarted. The number is then incremented after each time the function is used in a cycle between 000 and 999. Alternately if required, a specific stamp number can be assigned to the button or short code being used for the feature.

Details

- **Telephone Number:** Optional. If not set, a number in the sequence 000 to 999 is automatically used. If set, the number set is used.
- **Default Short Code**: ✓ *55
- **Programmable Button Control:** ✓ Stamp Log
- **Release:** 8.1+

Related links

Short Code Features on page 993

Startup Embedded Voicemail

Restarts the Embedded Voicemail service provided by an Avaya Memory in a control unit.

Details

- **Telephone Number**: ✗
- **Default Short Code:**✗
- **Programmable Button Control:**✗
- **Release**: 6.0+

Related links

Short Code Features on page 993

Suspend Call

This feature uses the Q.931 Suspend facility. It suspends the incoming call at the ISDN exchange, freeing up the ISDN B channel. The call is placed in exchange slot 0 if a slot number is not specified.

Details

- **Telephone Number:** ✓ Exchange slot number or blank (slot 0).
- **Default Short Code**: ✗
- **Programmable Button Control:** ✓ Suspe
- **See also**: Resume Call.
- **Release**: 1.0+.

Related links

Short Code Features on page 993

Suspend CW

This feature uses the Q.931 Suspend facility. Suspends the incoming call at the ISDN exchange and answer the call waiting. The call is placed in exchange slot 0 if a slot number is not specified. Only available when supported by the ISDN exchange.

Details

- **Telephone Number**: ✓ Exchange slot number or blank (slot 0).
- **Default Short Code**: ✓ *28*N# (A-Law only) (not on Server Edition)
- **Programmable Button Control:** ✓ SusCW
- **See also**: Resume Call.
- **Release:** 1.0+.

Example

Sample short code using the Suspend CW feature.

- **Short Code**: *28*N#
- **Feature**: Suspend CW

Related links

Short Code Features on page 993

Start After Call Work

This feature can be used by users who have been configured as CCR agents. It allows them to dial a short code to enter the After Call Work (ACW) state as reported by the Customer Call Reporter (CCR) application.

- CCR is not supported in IP Office release 9.1 and later.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✗
- **Programmable Button Control:** ✓ ACWrk
- **See also**: Clear After Call Work.
- **Release:** 4.2 4Q 2008 Maintenance release+.

Related links

Short Code Features on page 993

Toggle Calls

This feature cycles through each call that the user has on hold on the system. This feature is useful when a user with a single-line telephone has several calls on hold and needs to respond to each one in turn.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *29
- **Programmable Button Control**: ✓ Toggl
- **Release**: 1.0+.

Example

Below is sample short code using the Toggle Calls feature.

- **Short Code**: *29
- **Feature:** ToggleCalls

Related links

Short Code Features on page 993

Unpark Call

Retrieve a parked call from a specified system park slot.

Details

- **Telephone Number**: ✓ System park slot number.
- **Default Short Code**: ✓ *38*N#
- **Programmable Button Control**: ✓ Ride
- **See also**: Call Park.
- **Release:** 1.0+.

Example

Below is a sample short code using the Unpark Call feature. N represents the park slot number in which the call you want to retrieve was parked. For example, if a user parked a call to slot number 9, you can retrieve that call by dialing *38*9#.

- **Short Code**: *38*N#
- **Telephone Number:** N
- **Feature**: Unpark Call

Related links

Short Code Features on page 993

Voicemail Collect

This feature connects to the voicemail system. The telephone number field is used to indicate the name of the mailbox to be accessed, for example "?Extn201" or "#Extn201".

- **?** indicates 'collect messages'.
- **#** indicates 'leave a message'. It also instructs the voicemail server to give a brief period of ringing before connecting the caller. This is useful if the short code is used for functions such as call transfers as otherwise the voicemail server can start playing prompts before the transfer is completed. However, the # can be omitted for immediate connection if required.

- **" "** quotation marks must be used to enclose any information that needs to be sent to the voicemail server as is. Any text not enclosed by quote marks is checked by the telephone system for short code character matches which will be replaced before being sent to the voicemail server.
  - Manager automatically adds quotation marks to the **Telephone Number** field if they are not added manually. Care should be taken to ensure that special characters that you want replaced by the telephone system, such as **U**, **N** or **X**, are not enclosed by the quotation marks. For scenarios where the telephone number only contains short code characters, add an empty pair of quotation marks, for example **""N**.

When using Voicemail Pro, names of specific call flow start points can directly access those start points via a short code. In these cases, **?** is not used and **#** is only needed if ringing is required before the start point's call flow begins.

Short codes using the **Voicemail Collect** feature, with either `"Short Codes.name"` and `"#Short Codes.name"` records in the **Telephone Number** field are automatically converted to the **Voicemail Node** feature and name.

CallPilot voicemail is used for IP Office Branch deployments with CS 1000. Users can access their CallPilot voicemail by dialing the **Voicemail Collect** short code. For access to CallPilot voicemail from an Auto Attendant, set a **Normal Transfer** action to point to the CallPilot number.

Details

- **Telephone Number:** ✓ See the notes above.
- **Default Short Code**: ✓ *17
- **Programmable Button Control**: ✓ VMCol
- **See also**: Voicemail On, Voicemail Off, Voicemail Node.
- **Release**: 1.0+.

Example: Retrieve Messages from Specific Mailbox

This short code allows a user to retrieve messages from the mailbox of the hunt group 'Sales'. This usage is not supported on Voicemail Pro running in Intuity emulation mode unless a custom call flow has been created for the hunt group, refer to the Voicemail Pro help.

- **Short Code**: *89
- **Telephone Number**: "?Sales"
- **Feature**: VoicemailCollect

Example: Record Message to Specific Mailbox

To allow users to deposit a message directly to Extn201's Voicemail box. This short code is useful when you know the person is not at her/his desk and you want to immediately leave a message rather than call the person and wait to be redirected to voicemail.

- **Short Code**: *201
- **Telephone Number**: "#Extn201"
- **Feature**: VoicemailCollect

Example: Accessing a Specific Voicemail Pro Module

This short code can be used in instances where you have a conference bridge set up on the system and a module has been created via Voicemail Pro to access this conference bridge. A short code can be created for internal access to the module. In the sample short code below, the telephone number field contains the name of the module. In this example, if a short burst of ringing is required before connecting the module, "#conferenc" would be used as the telephone number.

- **Short Code**: *100
- **Telephone Number**: "conferenc"
- **Feature**: VoicemailCollect

Related links

Short Code Features on page 993

Voicemail Node

Similar to Voicemail Collect but used for calls being directed to a Voicemail Pro Short Codes start point. Useful if you have set up a short code start point with Voicemail Pro and want to give direct internal access to it.

Details

- **Telephone Number**: ✓ Voicemail Pro Short Code start point name without quotation marks.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✗
- **See also**: Voicemail Collect.
- **Release**: 2.0+.

Example

Having created a short codes start point call flow called Sales, the following system short code can be used to route calls to that call flow:

- **Short Code:** *96
- **Telephone Number:** Sales
- **Feature**: VoicemailNode

Related links

Short Code Features on page 993

Voicemail On

This feature enables the user's voicemail mailbox to answer calls which ring unanswered or arrive when the user is busy.

Details

- **Telephone Number**: ✗ None.
- **Default Short Code:** ✓ *18
- **Programmable Button Control:** ✓ VMOn
- **See also**: Voicemail Off.
- **Release**: 1.0+.

Example

This short code can be used to toggle the feature on.

- **Short Code**: *18
- **Feature**: VoicemailOn

Related links

Short Code Features on page 993

Voicemail Off

This feature disables the user's voicemail mailbox box from being used to answer calls. It does not disable the voicemail mailbox being used as the target for other functions such as call recording or messages forwarded from other mailboxes.

Details

- **Telephone Number**: ✗ None.
- **Default Short Code**: ✓ *19
- **Programmable Button Control**: ✓ VMOff
- **See also:** Voicemail On.
- **Release:** 1.0+.

Example

Below is a sample of the short code setup.

- **Short Code**: *19
- **Feature**: VoicemailOff

Related links

Short Code Features on page 993

Voicemail Ringback On

This feature enables voicemail ringback to the user's extension. Voicemail ringback is used to call the user when they have new voicemail messages. The ringback takes place each time the

extension is used. This feature is useful for users who do not have voicemail light/button indicators on their telephone.

If the user has been configured to receive message waiting indication for any hunt groups, a separate voicemail ringback will occur for each such group and for the users own mailbox.

Details

- **Telephone Number**: ✗
- **Default Short Code:** ✓ *48
- **Programmable Button Control**: ✓ VMRB+
- **See also**: Voicemail Ringback Off.
- **Release**: 1.0+. For Release 3.2, the Voicemail On and Voicemail Ringback On short code features toggled. For Release 4.0 and higher, they no longer toggle.

Example

This short code can be used to turn the feature on.

- **Short Code**: *48
- **Feature**: VoicemailRingbackOn

Related links

Short Code Features on page 993

Voicemail Ringback Off

This feature disables voicemail ringback to the user's extension.

Details

- **Telephone Number**: ✗
- **Default Short Code**: ✓ *49
- **Programmable Button Control**: ✓ VMRB-
- **See also:** Voicemail Ringback On.
- **Release**: 1.0+.

Example

Below is a sample of the short code setup.

- **Short Code**: *49
- **Feature**: VoicemailRingbackOff

Related links

Short Code Features on page 993

Whisper Page

This feature allows you to intrude on another user and be heard by them without being able to hear the user's existing call which is not interrupted.

For example: User A is on a call with user B. When user C intrudes on user A, they can be heard by user A but not by user B who can still hear user A. Whisper page can be used to talk to a user who has enabled private call.

- Intrusion features are controlled by the **Can Intrude** setting of the user intruding and the **Cannot Be Intruded** setting of user being intruded on. By default, no users can intrude and all users cannot be intruded.

The system support a range of other call intrusion methods in addition to this feature.

Details

- **Telephone Number**: ✓ Target extension number.
- **Default Short Code**: ✗
- **Programmable Button Control**: ✓ Whisp.
- **See also**: Call Intrude, Call Listen, Coaching Intrusion, Dial Inclusion.
- **Release**: 8.0+.

Related links

Short Code Features on page 993

Part 14: Button Programming

Chapter 104: Button Programming Overview

This section provides an overview of system actions that can be assigned to programmable buttons on Avaya phones.

Button assignment can be done through the system configuration using IP Office Manager and IP Office Web Manager. If only button programming changes are required, the configuration changes can be merged back to the system without requiring a reboot.

Users can also do their own button programming using the user portal application or, on some phones, through the phone's menu. However, users can only program a limited set of functions and cannot override appearance buttons and buttons set through user rights templates.

- **Appearance Functions**

  The functions **Call Appearance**, **Bridged Appearance**, **Coverage** and **Line Appearance** are collectively known as "appearance functions". For full details of their operation and usage, see Appearance Buttons on page 1198.

- **Phone Support**

  Note that not all functions are supported on all phones with programmable buttons. Where possible exceptions, have been indicated. Those buttons will typically play an error tone when used on that phone. Programming of those features however is not restricted as users may hot desk between different types of phones, including some where the feature is supported.

- **Status Indication**

  Actions that use status feedback are only supported on buttons that provide that feedback through lamps or icons.

Related links

Programming Buttons with IP Office Web Manager on page 1083
Interactive Button Menus on page 1083
Label Templates on page 1084

Programming Buttons with IP Office Web Manager

This process edits the programmable buttons for individual users.

- You can also use user rights to create a set of programmable buttons that are simultaneously applied to multiple users. See Configuring User Rights on page 858.

Procedure

1. Use **Call Management** > **Users** to display the list of users.
2. Click the icon next to the user you want to edit.
3. Select **Button Programming**.
4. The number of buttons displayed is based on the **Select Phone** settings. This defaults to matches the phone currently associated with the user. You can change the value or set it to **None** to display all the possible buttons. This may be necessary for users who switch between different phones using hot desking or have an expansion unit attached to their phone.
5. For the required button, click the icon.
6. Add a label and select the required action. Additional options may appear depending on the action selected.
7. When completed, click **OK**.
8. Repeat for any other buttons.
9. Click **Update**.

Related links

Button Programming Overview on page 1082

Interactive Button Menus

For certain functions, on display phones where a button has been configured without a specific number, a menu for number entry is displayed. The menu includes a **Dir** option for selecting a number from the directories held by the system.

Functions that use the interactive menu are:

Feature	Directory lists...		Feature	Directory lists...
Automatic Intercom	Users		Follow Me Here Cancel	Users
Acquire Call/Call Steal	Users		Follow Me Here	Users
Call Forwarding All	Users		Follow Me To	Users
Call Intrude	Users		Forward Number	Users/Groups

Table continues…

Call Park To Other Extension	Users		Forward Busy Number	Users/Groups
Dial Inclusion	Users		Group Paging	Users/Groups
Dial Intercom	Users		Leave Word Calling	Users/Groups
Directed Call Pickup	Users/Groups		Priority Calling	Users/Groups

User and Group buttons can be used to indicate the required user or hunt group only if those buttons are on an associated button module. **User** and **Group** buttons on the users extension are not accessible while the interactive button menu is being displayed.

For functions supported across a multi-site network, the directory will include remote users and advertised hunt groups.

For M-Series and T-Series phone, the volume buttons are used to scroll through the list of matching names. If this is done during a call or while a call is alerting, this will also adjust the call or ring volume.

Related links

Button Programming Overview on page 1082

Label Templates

A zip file is available containing Word document templates for the paper programmable key labels used on various phones supported by the system. Two templates are provided, one for A4 size paper, the other for US Letter sized paper. See https://ipofficekb.avaya.com/businesspartner/ipoffice/user/dsstemplate/index.htm.

For 1400 and 1600 phones, a number of tools and perforated printable labels are available. For further details visit http://support.avaya.com and search for information on DESI. Alternatively, visit http://www.desi.com.

Related links

Button Programming Overview on page 1082

Chapter 105: Button Programming Actions

The following sections provide details for each of the button actions supported by system. Note that this does not include buttons on phones on a system running in Partner Edition mode.

For each, the following details are listed:

- **Action** - Indicates the selection path to the action from within the list of actions displayed in Manager.
- **Action Data** - Indicates the type of data required by the action. For some actions no data is required while for others action data may be optional. The option to enter the data after pressing the button is not available for all phones, see Interactive Button Menus.
- **Default Label** - This is the default text label displayed on phones which provide a display area next to programmable buttons. Alternate labels can be specified in the system configuration or entered by the phone user (refer to the telephone user guide). Note that for buttons with action data set, the action data may also be displayed as part of the default label. Depending on the display capacity of the particular phone, either a short or long label is displayed.
- **Toggles** - Indicates whether the action toggles between two states, typically on or off.
- **Status Indication** - Indicates whether the button provides status indication relevant to the feature if the button has status lamps or display. If the **Status Indication** is listed as **Required** it indicates that the button action is only supported on programmable buttons that can provide status indication.
- **User Admin** - This item indicates that users with a Self-Administer button can assign the action to other buttons themselves.
- **Phone Support** - This is only a general indication of support or otherwise of an action by phones within particular series. On phones with 3 or less programmable buttons those button can only be used for the Call Appearance action. In addition some actions are only supported on phones where the programmable buttons provide status indication and or a display for data entry once the feature is invoked.

Button Programming Actions Summary

The following tables list the actions available for programmable buttons on system.

- **Login Code Required** Some function may require the user to enter their log in code. This typically applies when the action data is left blank for entry when the button is pressed.

General

Action	Action Data	Default Label
Dial	Any number.	Dial
Group	"Group name" in quote marks.	<Group name>
User	"User name" in quote marks.	<User name>

Appearance

Action	Action Data	Default Label
Appearance	None.	**a=**
Bridged Appearance	User name and call appearance button number.	<user name><appearance label>
Coverage Appearance	User name.	<user name>
Line Appearance	Line appearance ID.	**Line**

Emulation

Action	Action Data	Short Label	Long Label
Abbreviated Dial	Any number.	**AD**	**Abbreviate Dial**
Abbreviated Dial Pause	None.	**Pause**	**–**
Abbreviated Dial Program	None.	**Prog**	**–**
Abbreviated Dial Stop	None.	**Stop**	**–**
Absent Message	None.	None.	None.
Account Code Entry	Account code or blank for entry when pressed.	**Acct**	**Account Code**
ACD Agent Statistics	None.	**Stats**	**–**
ACD Stroke Count	None.	**Count**	**–**
AD Special Function Mark	None.	**Mark**	**–**
AD Special Function Wait	None.	**Wait**	**–**
AD Special Functions	None.	**Sfunc**	**–**
AD Suppress	None.	**Spres**	**Suppress Digits**
Automatic Callback	None.	**AutCB**	**Auto Callback**
Automatic Intercom	User number or name.	**Iauto**	**Auto Intercom**
Call Forwarding All	Any number or blank for entry when pressed.	**CFrwd**	**Call Forward All**
Call Park	Park slot ID (alphanumeric) or blank for menu of slots in use.	**CPark**	**Call Park**

Table continues…

Action	Action Data	Short Label	Long Label
Call Park To Other Extension	User number.	**RPark**	**Call Park to Other**
Call Pickup	None.	**CpkUp**	**Call Pickup Any**
Cancel Leave Word Calling	None.	**CnLWC**	**–**
Consult	None.	**CnsIt**	**–**
Dial Intercom	User number or name or blank for entry when pressed.	**Idial**	**Auto Intercom**
Directed Call Pickup	User number or name or group number or name or or blank for entry when pressed..	**DpkUp**	**Call Pickup**
Directory	None.	**Dir**	**–**
Drop	None.	**Drop**	**Drop Call**
Emergency View	None.	**911–View** or **EView**	
Group Paging	User or group number or name or blank for entry when pressed.	**GrpPg**	**Page**
Headset Toggle	None or FF	**HdSet**	**–**
Inspect	None.	**Inspt**	**–**
Internal Auto-Answer	None.	**HFAns**	**Auto Answer**
Leave Word Calling	None.	**LWC**	**–**
Manual Exclude	None.	**Excl**	**–**
Priority Calling	None.	**Pcall**	**–**
Ringer Off	None.	**RngOf**	**Ringer Off**
Self-Administer	Blank or 1 or 2	**Admin**	**Self Administer**
Send All Calls	None.	**SAC**	**Send All Calls**
Stored Number View	None.	**BtnVu**	**–**
Time of Day	None.	**TmDay**	**–**
Timer	None.	**Timer**	**–**
Twinning	None.	**Twinning**	**Twinning**
Visual Voice	None.	**Voice**	**Voice**

Advanced

Action	Action Data	Category	Short Label	Long Label
Acquire Call	User number or blank for last call transferred.	Call	**Acquir**	**Acquire**
Break Out	System name or IP address or blank for selection when pressed.	Dial	**BkOut**	**Breakout**
Busy	None.	Busy	**Busy**	**–**
Busy On Held	0 (off) or 1 (on).	Busy	**BusyH**	**–**
Call Intrude	User number or blank for entry when pressed.	Call	**Intru**	**Call Intrude**
Call List	None.	Call	**LIST**	**–**
Call Listen	User number.	Call	**Listn**	**Listen**
Call Log	None.	Call		**Call Log**
Call Pickup Any	None.	Call	**PickA**	**Pickup Any**
Call Pickup Group	Group number or name.	Call	**PickG**	**Pickup Group**
Call Pickup Members	Group number or name.	Call	**PickM**	**Pickup Members**
Call Queue	User number.	Call	**Queue**	**Queue**
Call Record	None.	Call	**Recor**	**Record**
Call Screening	None.	Call	**CallScreen**	**Call Screening**
Call Steal	User number or blank for last call transferred.	Call	**Steal**	**–**
Call Waiting Off	None.	Call	**CWOff**	**–**
Call Waiting On	None.	Call	**CWOn**	**–**
Call Waiting Suspend	None.	Call	**CWSus**	**–**
Cancel All Forwarding	None.	Call	**FwdOf**	**Call Forward Off**
Cancel Ring Back When Free	None.	Miscellaneous	**RBak-**	**–**
Channel Monitor	Channel number.	Call	**ChMon**	**–**
Clear Call	None.	Call	**Clear**	**Clear**
Clear CW	None.	Call	**ClrCW**	**–**

Table continues…

Action	Action Data	Category	Short Label	Long Label
Clear Hunt Group Night Service	Group number.	Call	**HGNS-**	**–**
Clear Hunt Group Out Of Service	Group number.	Call	**HNOS-**	**–**
Clear Quota	"Service name" within quote marks or "" for all services.	Call	**Quota**	**–**
Coaching Intrusion	User number or name or blank for entry when pressed.	Call	**Coach**	**Coaching Intrusion**
Conference	Invoke the conference process. (M and T-Series phones only)	Call	**Conf**	**–**
Conference Add	None.	Call	**Conf+**	**Conference Add**
Conference Meet Me	Conference name or number.	Call	**CnfMM**	**Conf. Meet Me**
Dial 3K1	Any number.	Dial	**D3K1**	**Dial 3K1**
Dial 56K	Any number.	Dial	**D56K**	**Dial 56K**
Dial 64K	Any number.	Dial	**D64K**	**Dial 64K**
Dial CW	User number.	Dial	**DCW**	**Dial Call Waiting**
Dial Direct	User number or name or blank for entry when pressed.	Dial	**Dirct**	**Auto Intercom**
Dial Emergency	Any number.	Dial	**Emrgy**	**Dial Emergency**
Dial Inclusion	User number or name or blank for entry when pressed.	Dial	**Inclu**	**Dial Inclusion**
Dial Paging	User or group number or name or blank for entry when pressed.	Dial	**Page**	**Page**
Dial Physical Extn by Number	Extension port Base Extension number.	Dial	**PhyEx**	**Dial Physical Extn**

Table continues…

Action	Action Data	Category	Short Label	Long Label
Dial Physical Extn by Id	Extension port ID number. (Release 1.4+)	Dial	**DialP**	**Dial Extn by Id**
Dial Speech	Any number.	Dial	**DSpch**	**Dial Speech**
Dial V110	Any number.	Dial	**DV110**	**Dial V110**
Dial V120	Any number.	Dial	**DV120**	**Dial V120**
Dial Video	Any number.	Dial	**Dvide**	**Dial Video**
Display Msg	Command string.	Dial	**Displ**	**–**
Do Not Disturb Auto-Intercom Deny	None	Do Not Disturb	**NoAI**	**No Auto Int Calls**
Do Not Disturb Exception Add	Any number.	Do Not Disturb	**DNDX+**	**–**
Do Not Disturb Exception Delete	Any number.	Do Not Disturb	**DNDX-**	**–**
Do Not Disturb Off	None.	Do Not Disturb	**DNDOf**	**–**
Do Not Disturb On	None.	Do Not Disturb	**DNDOn**	**Do Not Disturb**
Extn Login	None.	Extension	**Login**	**Login**
Extn Logout	None.	Extension	**Logof**	**Logout**
Flash Hook	None.	Miscellaneous	**Flash**	**Flash Hook**
Follow Me Here	User number.	Follow Me	**Here+**	**Follow Me Here**
Follow Me Here Cancel	User number or blank for entry when pressed.	Follow Me	**Here-**	**Follow Me Here-**
Follow Me To	User name or user number or blank for entry when pressed.	Follow Me	**FolTo**	**Follow Me To**
Forward Hunt Group Calls On	None.	Forward	**FwdH+**	**–**
Forward Hunt Group Calls Off	None.	Forward	**FwdH-**	**Fwd HG Calls**
Forward Number	Any number or blank for entry when pressed.	Forward	**FwdNo**	**Fwd Number**
Forward On Busy Number	Any number or blank for entry when pressed.	Forward	**FwBNo**	**Fwd Busy Number**
Forward On Busy Off	None.	Forward	**FwBOf**	**–**

Table continues…

Action	Action Data	Category	Short Label	Long Label
Forward On Busy On	None.	Forward	**FwBOn**	**Fwd Busy**
Forward On No Answer Off	None.	Forward	**FwNOf**	**–**
Forward On No Answer On	None.	Forward	**FwNOn**	**Fwd No Answer**
Forward Unconditional Off	None.	Forward	**FwUOf**	**–**
Forward Unconditional On	None.	Forward	**FwUOn**	**Fwd Unconditional**
Group Listen On	None.	Extension	**GroupListenOn**	**–**
Hold Call	ISDN Exchange slot number.	Hold	**Hold**	**–**
Hold CW	None.	Hold	**HoldCW**	**–**
Hold Music	None.	Hold	**Music**	**Hold Music**
Hunt Group Disable	Group number or name or blank for all groups.	Hunt Group	**HGDis**	
Hunt Group Enable	Group number or name or blank for all groups.	Hunt Group	**HGEna**	**HG Enable**
Last Number Redial	Redial the last number dialed. (M and T-Series phones only)	Call	**Again**	**–**
MCID Activate	None.	Miscellaneous	**MCID**	**Malicious Call**
Monitor Analogue Trunk MWI	Line appearance ID.	Voicemail	**TrkMW**	**Trunk MWI**
Off Hook Station	None.	Miscellaneous	**OHStn**	**–**
Pause Recording	None.	Call	**PauseRec**	**Pause Recording**
Priority Call	User number or name.	Call	**PCall**	**Priority Call**
Private Call	None. (Release 4.0+)	Call	**PrivC**	**Private Call**
Relay Off	1 or 2.	Relay	**Rely-**	**–**
Relay On	1 or 2.	Relay	**Rely+**	**Relay On**
Relay Pulse	1 or 2.	Relay	**Relay**	**Relay Pulse**
Resume Call	ISDN Exchange slot number.	Call	**Resum**	**–**

Table continues…

Action	Action Data	Category	Short Label	Long Label
Retrieve Call	ISDN Exchange slot number.	Call	**Retriv**	**–**
Ring Back When Free	None.	Miscellaneous	**RBak+**	**Auto Callback**
Set Absent Text	String for selected message and custom text.	Set	**Absnt**	**Absence Text**
Set Account Code	Blank or valid account code. (Release 2.1+)	Set	**Acct**	**Account Code**
Set Hunt Group Night Service	Group number.	Set	**HGNS+**	**HG Night Service**
Set Hunt Group Out Of Service	Group number.	Set	**HGOS+**	**HG Out of Service**
Set Inside Call Seq	Value 0 to 10.	Set	**ICSeq**	**–**
Set Night Service Group	Group number. (Release 4.2+)	Set	**SetNSG**	**HG NS Group**
Set No Answer Time	Time in seconds (range 6 to 99999).	Set	**NATim**	**No Answer Time**
Set Outside Call Seq	Value 0 to 10.	Set	**OCSeq**	**–**
Set Out of Service Group	Group number. (Release 4.2+)	Set	**SetOOSG**	**HG OS Group**
Set Ringback Seq	Value 0 to 10.	Set	**RBSeq**	**–**
Set Wrap Up Time	Time in seconds (range 0 to 99999).	Set	**WUTim**	**Wrap-up Time**
Speed Dial	Initiate the speed dial selection process. (M and T-Series phones only)	Dial	**SpdDial**	**–**
Stamp Log	None.	Miscellaneous	**StmpL**	**Stamp Log**
Suspend Call	ISDN Exchange slot number.	Suspend	**Suspe**	**–**
Suspend CW	ISDN Exchange slot number.	Suspend	**SusCW**	**–**
Toggle Calls	None.	Call	**Toggl**	**–**
Transfer	Initiate the call transfer process. (M and T-Series phones only)	Call	**Xfer**	**–**

Table continues…

Action	Action Data	Category	Short Label	Long Label
Unpark Call	Park slot ID (alphanumeric).	Call	**Ride**	**–**
Voicemail Collect	See notes.	Voicemail	**VMCol**	**VMail Collect**
Voicemail Off	None.	Voicemail	**VMOff**	**–**
Voicemail On	None.	Voicemail	**VMOn**	**VMail On**
Voicemail Ringback Off	None.	Voicemail	**VMRB-**	**–**
Voicemail Ringback On	None.	Voicemail	**VMRB+**	**VMail Ringback**
Whisper Page	User number or name or blank for entry when pressed.	Call	**Whisp**	**Whisper Page**
Channel Monitor	Channel	Call	**ChMon**	-

911-View

See Emergency View on page 1142.

Abbreviated Dial

This function allows quick dialing of a stored number.

Details

- **Action**: Emulation | Abbreviated Dial.
- **Action Data**:
  - **Full Number** The number is dialed.
  - **Partial Number** The partial number is dialed and the user can then complete dialing the full number.
- **Default Label**: AD or Abbreviate Dial.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: Yes.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.

    - 1400 Series and 1600 Series.
    - M-Series and T-Series.

Abbreviated Dial Pause

Supported for CTI emulation only.

Allows a user to enter a pause character when programming an abbreviated dial.

Details

- **Action**: Emulation | Abbreviated Dial Pause.
- **Action Data**: None.
- **Default Label**: Pause.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
    - 1400 Series and 1600 Series.

Abbreviated Dial Program

Supported for CTI emulation only.

Allows a user to program abbreviated dialing numbers against other programmable buttons. This function cannot be used to overwrite call appearance buttons.

Details

- **Action**: Emulation | Abbreviated Dial Program.
- **Action Data**: None.
- **Default Label**: Prog.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: Yes.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
    - 1400 Series and 1600 Series.

Abbreviated Dial Stop

Supported for CTI emulation only.

Allows a user to enter a stop character when programming an abbreviated dial.

Details

- **Action**: Emulation | Abbreviated Dial Stop.
- **Action Data**: None.
- **Default Label**: Stop.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Absent Message

This feature allows to select the user's current absence text. See Set Absent Text on page 1174.

Account Code Entry

Enter an account code for a call. This button can be used before dialing a number or during a call.

Details

- **Action**: Emulation | Account Code Entry.
- **Action Data**: Optional. If an code is set it must match an account code set in the account codes list. If no account code is set, the phone display will request entry of a valid code. This option is not supported on XX02 phones and the T7000 phone.
- **Default Label**: Acct or Account Code.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: Yes.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.

- 1400 Series and 1600 Series.
- M-Series and T-Series.
- 1100 Series and 1200 Series.

ACD Agent Statistics

Supported for CTI emulation only.

Details

- **Action**: Emulation | ACD Agent Statistics.
- **Action Data**: None.
- **Default Label**: Stats.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

ACD Stroke Count

Supported for CTI emulation only.

Details

- **Action**: Emulation | ACD Stroke Count.
- **Action Data**: None.
- **Default Label**: Count.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: Yes.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Acquire Call

See Call Steal on page 1117.

AD Special Functions

Supported for CTI emulation only.

Allows a user to enter a special character (mark, pause suppress, wait) when entering an abbreviated dial.

Details

- **Action**: Emulation | AD Special Functions.
- **Action Data**: None.
- **Default Label**: Sfunc.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

AD Special Function Mark

Supported for CTI emulation only.

Allows a user to enter a mark character when programming abbreviated dial.

Details

- **Action**: Emulation | AD Special Function Mark.
- **Action Data**: None.
- **Default Label**: Mark.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** No.

- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

AD Special Function Wait

Supported for CTI emulation only.

Allows a user to enter a Wait for Dial Tone character when programming an abbreviated dial.

Details

- **Action**: Emulation | AD Special Function Wait.
- **Action Data**: None.
- **Default Label**: Wait.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

AD Suppress

Suppresses the display of dialed digits on the telephone display. Dialed digits are replaced with an **s** character.

Details

- **Action**: Emulation | AD Suppress.
- **Action Data**: None.
- **Default Label**: Spres or Suppress Digits.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin:** No.

- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.

After Call Work

This button is used by users configured as a Customer Call Reporter (CCR) Agent (**User | Telephony | Supervisor Settings**) and working with the CCR application. It shows the CCR agent their current After Call Work (ACW) status and allow them to manually change status. While in ACW state, the agent will not receive hunt group calls.

CCR Agents can be automatically put into and taken out of ACW by the system if the user is configured for Automatic After Call Work (User | Telephony | Supervisor Settings). Those users must have an **After Call Work** button.

Note:

CCR is not supported in IP Office release 9.1 and later.

Details

- **Action**: Advanced | Miscellaneous | After Call Work
- **Action Data**: None.
- **Default Label**: ACWrk or After Call Work.
- **Toggles**: Yes.
- **Status Indication**: Yes. Required.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Appearance

Creates a call appearance button. This can be used to answer and make calls. Users with multiple call appearance buttons can handle multiple calls. For details, see Call Appearance Buttons on page 1200.

Call appearance functions, assigned to buttons that do not have status lamps or icons, are automatically disabled until the user logs in at a phone with suitable buttons.

Appearance buttons can be set with a ring delay if required or to not ring. This does not affect the visual alerting displayed next to the button. The delay uses the user's **Ring Delay** (**User** > **Telephony** > **Multi-line Options**) setting.

Details

- **Action**: Appearance | Appearance.
- **Action Data**: Optional text label.
- **Default Label**: a=.
- **Toggles**: No.
- **Status Indication**: Yes, required.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Virtual Call Appearances

T7000, T7100, M7100 and M7100N phones support virtual call appearance button operation. Virtual call appearance operation is similar to an analog phone with call waiting enabled. However, it does not use the call waiting on/off settings, instead it uses call appearance buttons.

The number of virtual call appearances is set by the call appearance buttons programmed in the user's settings. These must be programmed as a single block start from button 1. It is recommended that only a maximum of 3 call appearances are used, however the user must have at least 1 call appearance programmed in order to make and receive calls.

Virtual Call Appearance Usability

If the user goes off-hook, they are connected to the alerting call if any, else to dial tone in order to make an outgoing call. This uses one of their virtual call appearance buttons.

With a call connected:

- If another call arrives on another virtual call appearance, the user will hear a call waiting tone on the set. The display, if the phone has one, will switch between details of the current and the waiting caller.
- If the user presses **Hold**, the connected call is placed on hold and:

If there are any available virtual call appearances, dial tone is heard. This allows the user to make a call or to use short codes that may affect the held or waiting calls. The following are some of the default short codes that can be used:

- ***26: Clear CW** Drop the previous call and answer the waiting call.
- ***52: Clear Call** Drop the previous call.
- ***47: Conference Add** Start a conference between the user and any held calls.
- Else, if there is a call waiting, that call is answered.
- Else, if there is a call on hold, that call is reconnected.

If the user presses **Release** or **Drop** or goes on-hook during a call, the current call is ended and the user's phone returns to idle. If there is a waiting call, it starts ringing. The user can answer the call by going off hook or pressing **Hold**.

With the phone idle:

If the user goes off hook:

- The first alerting call appearance is answered if any.
- Else, the first idle call appearance is seized and the user hears dial tone.
- The user can press `Hold`to switch between virtual call appearances. This will answer or retrieve any call on next virtual call appearance or else hear dial tone to make a call.

With the phone idle but a call alerting:

Going off-hook or pressing Hold will answer the call.

When all the users virtual call appearances are in use, they are busy to any further calls. Calls will follow forward on busy if set, else go to voicemail is available or else get busy indication.

The only other appearance button controls applied and supported are

Reserve Last CA This setting can be enabled for the extension user. When selected, the last available call appearance is reserved for outgoing calls only. For example, for a user with 3 call appearances, they return busy to any further calls when 2 virtual appearances are in use. The extension user can press hold to get dial tone on the reserved call appearance. An available call appearance is also required when using **Feature 70** to initiate a call transfer.

Coverage Appearances Other users can have Coverage Appearance buttons set to provided coverage to the virtual call appearance user. The virtual appearance users **Individual Coverage Time** setting is applied.

Automatic Callback

Sets a ringback on the extension being called. When the target extension ends its current call, the ringback user is rung (for their set **No Answer Time**) and if they answer, a new call is made to the target extension.

Ringback can also be cleared using the Cancel Ring Back When Free function.

Details

- **Action**: Emulation | Automatic Callback.
- **Action Data**: None.
- **Default Label**: AutCB or Auto Callback.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin:** Yes.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Auto-Intercom Deny

Use the Auto-Intercom Deny function to block automatic intercom calls.

Details

- **Action**: Advanced | Do Not Disturb | Auto Intercom Deny.
- **Action Data**: Blank.
- **Default Label**: NoAI or No Auto Int Calls.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.

- M-Series and T-Series.

Automatic Intercom

Automatic intercom functions allow you to call an extension and have the call automatically answered on speaker phone after 3 beeps. The extension called must support a handsfree speaker. If the extension does not have a handsfree microphone then the user must use the handset if they want to talk. If the extension is not free when called, the call is presented as a normal call on a call appearance button if available.

This feature can be used as part of handsfree announced transfers.

Details

- **Action**: Emulation | Automatic Intercom.
- **Action Data**: User number or name. This field can be left blank for number entry when pressed. On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.
- **Default Label**: Iauto or Auto Intercom.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Break Out

This feature is usable within a system multi-site network. It allows a user on one system in the network to specify that the following dialing be processed by another system on the network as if the user dialed it locally on that other system.

On phones with a multi-line display, if the target system is not specified in the button settings, a menu of the available systems in the network is displayed from which a selection can be made.

Details

- **Action**: Advanced | Dial | Break Out.
- **Action Data**: Optional. The system name or IP address of the required system can be specified. If no system name or IP address is set, on display phones a list of systems within the network is displayed when the button is pressed.

- **Default Label**: BkOut or Breakout.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.

Bridged Appearance

Creates an appearance button that follows the state of another user's call appearance button. The bridged appearance can be used to make and answer calls on behalf of the call appearance user. For details, see Bridged Appearance Buttons on page 1205.

The bridged appearance button user must also have at least one call appearance button programmed.

Bridged appearance functions, assigned to buttons that do not have status lamps or icons, are automatically disabled until the user logs in at a phone with suitable buttons.

Appearance buttons can be set with a ring delay if required or to not ring. This does not affect the visual alerting displayed next to the button. The delay uses the user's **Ring Delay** (**User** > **Telephony** > **Multi-line Options**) setting.

Details

- **Action**: Appearance | Bridged Appearance.
- **Action Data**: User name and call appearance button number.
- **Default Label**: <user name><call appearance label>.
- **Toggles**: No.
- **Status Indication**: Yes. Required.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
    1. Not supported on T7000, T7100, M7100 and M7100N.

Busy

Not used.

Busy On Held

When on, busy on held returns busy to new calls while the user has an existing call on hold. While this feature can be used by users with appearance keys, it is not recommended as this overrides the basic call handling intent of appearance keys.

Details

- **Action**: Advanced | Busy | Busy on Held.
- **Action Data**: 1 for on, 0 for off.
- **Default Label**: BusyH.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Call Forwarding All

Switches forward unconditional on and sets the forward number to the number specified or prompts the user to enter a number if none is specified.

Details

- **Action**: Emulation | Call Forwarding All.
- **Action Data**: Telephone number or blank for entry when pressed.
  - If blank, user's with a log in code will be prompted to enter that code to use this function.
  - On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.
- **Default Label**: CFrwd or Call Forward All.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Call Intrude

This feature allows you to intrude on the existing connected call of the specified target user. All call parties are put into a conference and can talk to and hear each other. A **Call Intrude** attempt to a user who is idle becomes a Priority Call.

- Intrusion features are controlled by the **Can Intrude** setting of the user intruding and the **Cannot Be Intruded** setting of user being intruded on. By default, no users can intrude and all users cannot be intruded.
- Intrusion features uses system conference resources during the call. If insufficient conference resource are available, the feature cannot be used.
- Users can use privacy features to set a call cannot be intruded on and recorded.
- Intruding onto a user doing silent monitoring (see Call Listen on page 1000) is turned into a silent monitoring call.

The system support a range of other call intrusion methods in addition to this feature.

Details

- **Action**: Advanced | Call | Call Intrude.
- **Action Data**: User number or blank for entry when pressed. On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.
- **Default Label**: Intru or Intrude.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.

- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Call Listen

This feature allows you to monitor another user's call without being heard.

- By default, monitoring is accompanied by a tone heard by all parties. Use of the tone is controlled by the **Beep on Listen** setting on the **System** > **Telephony** > **Tones and Music** tab.

Warning:

- Listening to a call without the other parties being aware is subject to local regulations. You must ensure that you have complied with the local regulations. Failure to do so can result in penalties.

The use of call listen is dependent on:

- The target being a member of the group set as the user's **Monitor Group** (**User** > **Telephony** > **Supervisor Settings**). The user does not have to be a member of the group.
- Intrusion features are controlled by the **Can Intrude** setting of the user intruding and the **Cannot Be Intruded** setting of user being intruded on. By default, no users can intrude and all users cannot be intruded.
- Intrusion features uses system conference resources during the call. If insufficient conference resource are available, the feature cannot be used.

A number of features are supported for call listening:

- Users can use privacy features to set a call cannot be intruded on and recorded.
- IP extensions can be monitored including those using direct media.
- The monitoring call can be initiated even if the target user is not currently on a call and remains active until the monitoring user clears the monitoring call.
- The user who initiated the call listen can also record the call.

Intruding onto an a user doing silent monitoring (Call Listen) is turned into a silent monitoring call.

1400, 1600, 9500 and 9600 Series phones with a user button can initiate listening using that button if the target user meets the criteria for listening.

The system support a range of other call intrusion methods in addition to this feature.

Details

- **Action:** Advanced | Call | Call Listen.
- **Action Data**: User number.

- **Default Label**: Listn or Listen.
- **Toggles:** No.
- **Status Indication**: No.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Call Log

This function provides access to a list of received calls.

Details

- **Action**: Advanced | Call | Call Log.
- **Action Data**: None.
- **Default Label**: Call Log.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - M-Series and T-Series.

Call Park

Users can use a button set to this action to park and unpark calls.

- Pressing the button whilst on a call will park that call.
  - Whilst parked, the caller hears music-on-hold if available.
  - The system **Park Timeout (secs)** setting (**System** > **System** > **Telephony**) controls how long calls remain parked. When this expires, the call recalls to the user who parked it if they are idle or when they next become idle. The recall call rings continuously and does follow any forwards or go to voicemail.
- Pressing the button whilst not on a call displays details of any other calls the user has parked and allows call retrieval.

You can configure a call park button with or without a park slot number:

- **When associated with a specific park slot number:**

  The button will park and unpark a call from that park slot only. The button indicates when someone has parked a call using that park slot number.

- **When not associated with a specific park slot number:**

  The button can park up to 10 calls by assigning each parked call a park slot number based on the user's extension number. For example, for extension *XXX*, the first parked call is assigned to park slot *XXX*0, the next to *XXX*1 and so on up to *XXX*9. The button will indicate when there are parked calls in any of those slots.

Park buttons on other phones and in applications (for example IP Office SoftConsole and Avaya one-X Portal) with the same park slot number as a parked call will indicate the park call and can be used to retrieve it.

Details

- **Action**: **Emulation** > **Call Park**
- **Action Data**: Either blank or a specific park slot number.
  - Park slot IDs can be up to 15 digits in length.
  - You can use names for application park slots.
- **Default Label**: CPark or Call Park.
- **Toggles**: ✓.
- **Status Indication**: ✓.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series, M-Series
- Calls parked by extension	Green flash	Green flash	Blue	Slow flash
- Call Parked by other extension	Red flash	Red flash	**Green**	Slow flash
- No parked calls	Off	Off	Gray	Off

- **User Admin:** Yes.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
    1. The button is equivalent to **Feature 74**.

Call Park and Page

Parks the user's current call into the park slot number specified on the **System | Telephony | Park & Page** tab, in the **Central Park Range** field.

On M/T-series phones, 14xx/16xx phones, and the 9504 phone, the user is presented with up to three Page Target Groups. On other 95xx/96xx phones, the Page action displays a scrolling list of possible Page Target Groups. The user may also directly enter a Page target number, or use the system Directory to find a Page target.

A call Parked within the Central Park Range (regardless of the origin of the Park action) can be retrieved by directly dialing the desired Central Park Range slot on which that call is Parked.

Details

- **Action**: Emulation | Call Park and Page.
- **Action Data:** None.
- **Default Label**: ParkPage
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** Yes.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
    1. **Feature 74** is equivalent to this button when a Central Park Range is defined. On an M7000 phone, if this feature is invoked, the call always attempts to Park on the highest defined Central Park Range slot. See the Call Park and Page short code description for details.
  - 1100 Series and 1200 Series.

Call Park To Other Extension

Allows the user to park their current call against another user's extension. The parked call indication on that extension is then activated according to the telephone type.

If the target extension has a Call Park button with no specific park slot number, the parked call will be indicated by that button and can be unparked from the list of parked calls shown when that button is pressed.

The park slot number assigned to the parked call is based on the number of the extension parking the call. For example, calls parked by extension 201 are assigned the park slot ID 2010, 2011 and so on up to 2019 depending on the number of calls parked.

Details

- **Action**: Emulation | Call Park To Other Extension.
- **Action Data**: User number. This field can be left blank for number entry when pressed. On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.
- **Default Label**: RPark or Call Park to Other.
- **Toggles**: Yes .
- **Status Indication**: Yes. This is the status indication on the extension parking the call.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series, M-Series
Parked call	Green flash	Green flash	Blue	Slow flash
No parked call	Off	Off	Grey	Off

- **User Admin:** Yes.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Call Pickup

Answer an alerting call on the system.

Details

- **Action**: Emulation | Call Pickup.
- **Action Data**: None.
- **Default Label**: CpkUp or Call Pickup Any.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** Yes.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Call Pickup Any

Pick up the first available ringing call on the system.

Details

- **Action**: Advanced | Call | Call Pickup Any.
- **Action Data**: None.
- **Default Label**: PickA or Pickup Any.
- **Toggles**: No.
- **Status Indication**: No.
- User Admin: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Call Pickup Group

Pick up a call ringing any hunt group of which the user is a member or set to pick up calls from a specific group.

The user can use this feature even if their membership of the group is currently set as disabled.

Details

- **Action**: Advanced | Call | Call Pickup Group.
- **Action Data**: Optional. To pick up calls from a specific group, use the group number or name.
- **Default Label**: PickG or Pickup Group.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.

- M-Series and T-Series.
    1. The button is equivalent to **Feature 75**.

Call Pickup Members

This feature can be used to pick up any call to an extension that is a member of the hunt group specified. The call picked up does not have to be a hunt group call. The function includes group members even if their membership of the group is currently disabled.

Details

- **Action**: Advanced | Call | Call Pickup Members.
- **Action Data**: Group number or name.
- **Default Label**: PickM or Pickup Members.
- **Toggles**: No.
- **Status Indication**: Yes *(11.1 SP1)*
    - On suitable phones, pressing the button displays a list of any group member with a call waiting to be answered. Pressing the button next to the user name answers their call.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
    - 9500 Series, 9600 Series and J100 Series.
    - 1400 Series and 1600 Series.
    - M-Series and T-Series.

Call Queue

Transfer the call to the target extension if free or busy. If busy, the call is queued to wait for the phone to become free. This is similar to transfer except it allows you to transfer calls to a busy phone.

Details

- **Action**: Advanced | Call | Call Queue.
- **Action Data**: User number.
- **Default Label**: Queue.
- **Toggles**: No.
- **Status Indication**: No.

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Call Record

This feature allows you to record a conversation and requires Voicemail Pro to be installed.

- An advice of recording warning will be given if configured on the voicemail system.
- The recording is placed in the mailbox specified by the user's **Manual Recording Mailbox** setting.
- Intrusion features uses system conference resources during the call. If insufficient conference resource are available, the feature cannot be used.
- Users can use privacy features to set a call cannot be intruded on and recorded.

Details

- **Action**: Advanced | Call | Call Record.
- **Action Data**: None.
- **Default Label**: Recor or Record.
- **Toggles**: Yes.
- **Status Indication**: Yes.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.
  - This button action is also supported by the Vantage Connect Expansion application.

Call Screening

This function is used to enable or disable call screening. While enabled, when a caller is presented to the user's voicemail mailbox, if the user's phone is idle they will hear through the

phone's handsfree speaker the caller leaving the message and can select to answer or ignore the call.

This feature can be used with both Embedded Voicemail and Voicemail Pro. Call screening is only applied as follows:

- It is only applied to calls that have audible alerted at the user's extension before going to voicemail. This requires the user to have both voicemail coverage and call screening enabled and the phone's ringer not set to silent. However it is not applied if the user transfers the call to voicemail.
- It is only applied if the user's phone is idle. That is, not on a call or with a call held pending transfer or conference.
- Calls that ring the user, are then rerouted (for example follow a forward on busy setting) and then return to the user's mailbox are screened.

While a call is being screened, the phone can be used to either answer or ignore the screened call. Auto answer options are ignored.

Answering a screened call

A screened call can be answered by pressing the **Answer** soft key (if displayed) or lifting the handset. Pressing the call appearance or line button on which the call is indicated will also answer the call.

When answered:

- The phone's microphone is unmuted and a normal call between the user and caller now exists.
- The voicemail recording stops but that portion of the call already recorded is left as a new message in the user's mailbox.

Ignoring a screened call

A screened call can be ignored by pressing the Ignore soft key if displayed. On 1400, 1600, 9500 and 9600 Series phones, pressing the **SPEAKER** button will ignore the call. On M-Series and T-Series phones, pressing the **Release** key will ignore the call.

When ignored:

- The call continues to be recorded until the caller hangs up or transfers out of the mailbox.
- The user's phone returns to idle with call screening still enabled. However any other call that has already gone to voicemail is not screened.

Screened call operation

While a call is being screened:

- The mailbox greeting played and the caller can be heard on the phone's speakerphone. The caller cannot hear the user.
- The user is regarded as being active on a call. They will not be presented with hunt group calls and additional personal calls use abbreviated ringing.
- 1400/1600/9500/9600 Series phones: If the phone's default audio path is set to headset or the phone is idle on headset, then the screened call is heard through the headset.
- Any additional calls that go to the user's mailbox when they are already screening a call, remain at the mailbox and are not screened even if the existing call being screened is ended.

- Making or answering another call while listening to a screened call is treated as ignoring the screened call. For users with **Answer Pre-Select** enabled (User | Telephony | Multi-line Options), pressing an appearance button to display details of a call is also treated as ignoring the screened call.
- Other users cannot access a call that is being screened. For example they cannot use call pickup, bridged appearance or line appearance buttons, call intrude or call acquire functions.
- Phone based administration cannot be accessed and the hold, transfer and conference buttons are ignored.
- The screened caller using DTMF breakout ends the call screening.

Enabling do not disturb overrides call screening except for calls from numbers in the user's do not disturb exceptions list.

Locking the phone overrides call screening.

Manual call recording cannot be applied to a call being screened.

While a call is being screened, it uses one of the available voicemail channels. If no voicemail channels are available, call screening does not occur.

Warning:

The use of features to listen to a call without the other call parties being aware of that monitoring may be subject to local laws and regulations. Before enabling the feature you must ensure that you have complied with all applicable local laws and regulations. Failure to do so may result in severe penalties.

Details

- **Action:** Advanced | Call | Call Screening.
- **Action Data**: None.
- **Default Label**: CallScreen or Call Screening.
- **Toggles:** Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
    1. Not T7406E.

Call Steal

This function allows a user to seize a call answered or ringing on another extension. This function can be used with or without a specified user target.

- If the target has multiple alerting calls, the function steals the longest waiting call.
- If the target has a connected call and no altering calls, the function steals the connected call. This is subject to the **Can Intrude** setting of the **Call Steal** user and the **Cannot Be Intruded** setting of the target.
- If no target is specified, the function attempts to reclaim the user's last ringing or transferred call if it has not been answered or gone to voicemail.
- Stealing a video call changes the call to an audio call.
- R11.1 FP2 SP4 and higher: The shortcode for this feature can be used with the user's own extension number. That enables twinned and simultaneous device users to move a connected call from another one of their devices. This usage ignores the user's privacy and intrusion settings.

Details

- **Action**: Advanced | Call | Call Steal.
- **Action Data**:
  - User number or blank for last call transferred.
- **Default Label**: Aquir or Aquire.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Call Waiting Off

Switches call waiting off for the user. This button function is obsolete. The Call Waiting On button function toggles on/off and indicates current status.

Details

- **Action**: Advanced | Call | Call Waiting Off.
- **Action Data**: None.

- **Default Label**: CWOff.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Call Waiting On

Enables call waiting on the user's extension. When the user is on a call and another call arrives, they will hear a call waiting tone.

Note:

Call waiting does not operate for user's with call appearance buttons. See Call Waiting.

Details

- **Action:** Advanced | Call | Call Waiting On.
- **Action Data**: None.
- **Default Label**: CWOn or Call Waiting On.
- **Toggles:** Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Call Waiting Suspend

Disables call waiting, if on, for the duration of the extension's next call.

Details

- **Action**: Advanced | Call | Call Waiting Suspend.

- **Action Data**: None.
- **Default Label**: CWSus.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Cancel All Forwarding

Cancels forward unconditional, forward on busy, forward on no answer, follow me and do not disturb if any of those are active on the user's extension.

- **Action**: Advanced | Call | Cancel All Forwarding.
- **Action Data**: None.
- **Default Label**: FwdOf or Call Forward Off.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.

Details

- 9500 Series, 9600 Series and J100 Series.
- 1400 Series and 1600 Series.
- M-Series and T-Series.
- This button action is also supported by the Vantage Connect Expansion application.

Cancel Leave Word Calling

Supported for CTI emulation only.

Cancels the last Leave Word Calling message originated by the user.

Details

- **Action**: Emulation | Cancel Leave Word Calling.

- **Action Data**: None.
- **Default Label**: CnLWC.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Cancel Ring Back When Free

Cancels any existing ring back set by the user, see Ring Back When Free. Note that the Ring Back When Free button toggles to set or cancel ring back when free and also indicates the current status.

Details

- **Action**: Advanced | Miscellaneous | Cancel Ring Back When Free.
- **Action Data**: None.
- **Default Label**: RBak-.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

1. M-Series/T-Series: The button is equivalent to **Feature #2**.

Channel Monitor

For Avaya use only. Configurable through web manager only.

Clear Call

This feature can be used to end the last call put on hold. This can be used in scenarios where a first call is already on hold and simply ending the second call will cause an unsupervised transfer of the first call.

Details

- **Action**: Advanced | Call | Clear Call.
- **Action Data**: None.
- **Default Label**: Clear.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Clear CW

End the user's current call and answer any call waiting. Requires the user to also have call waiting indication on. This function does not work for users with multiple call appearance buttons.

Details

- **Action**: Advanced | Call **|** Clear CW.
- **Action Data**: None.
- **Default Label**: ClrCW.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Clear Hunt Group Night Service

Changes the specified hunt group from Night Service mode to 'In Service' mode. This button function is obsolete. The Set Hunt Group Night Service function can be used to toggle a group in/out of service and provides lamp status indication.

Setting and clearing hunt group night service can be done using either manual controls or using a system time profile. The use of both methods to control the night service status of a particular hunt group is not supported.

This function is not supported between systems in a multi-site network. It can only be used by a user currently logged onto the same system as hosting the hunt group.

Details

- **Action**: Advanced | Call | Clear Hunt Group Night Service.
- **Action Data**: Group number. If left blank, the button will affect all hunt groups of which the user is a member.
  - The **Set Hunt Group Night Service** and **Clear Hunt Group Night Service** short code and button features can be used to switch an SSL VPN service off or on respectively. The service is indicated by setting the service name as the telephone number or action data. Do not use quotation marks.
- **Default Label**: HGNS-.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Clear Hunt Group Out Of Service

Changes the specified hunt groups status from Out of Service mode to 'In Service' mode. This button function is obsolete. The Set Hunt Group Out Of Service function can be used to toggle a group in/out of service and provides lamp status indication.

This function is not supported between systems in a multi-site network. It can only be used by a user currently logged onto the same system as hosting the hunt group.

Details

- **Action**: Advanced | Call | Clear Hunt Group Out of Service.
- **Action Data**: Group number. If left blank, the button will affect all hunt groups of which the user is a member.

- **Default Label**: HGOS-.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Clear Quota

Quotas can be assigned on outgoing calls to data services such as internet connections. The quota defines the number of minutes available for the service within a time frame set within the service, for example each day, each week or each month.

The Clear Quota function can be used to reset the quota for a specific service or for all services.

Details

- **Action**: Advanced | Call | Clear Quota.
- **Action Data**: Service name" or "" (all services).
- **Default Label**: Quota.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Coaching Intrusion

This feature allows the you to intrude on another user's call and to talk to them without being heard by the other call parties to which they can still talk. For example: User A is on a call with user B. When user C intrudes on user A, they can hear users A and B but can only be heard by user A.

- Intrusion features are controlled by the **Can Intrude** setting of the user intruding and the **Cannot Be Intruded** setting of user being intruded on. By default, no users can intrude and all users cannot be intruded.
- Intrusion features uses system conference resources during the call. If insufficient conference resource are available, the feature cannot be used.

- Listening to a call without the other parties being aware is subject to local regulations. You must ensure that you have complied with the local regulations. Failure to do so can result in penalties.

The system support a range of other call intrusion methods in addition to this feature.

Details

- **Action:** Advanced | Call | Coaching Intrusion.
- **Action Data**: User number or name or blank for entry when pressed.
- **Default Label**: Coach or Coaching Intrusion.
- **Toggles:** No.
- **Status Indication**: No.
- **User Admin:** No feedback provided..
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - Not supported on non-IP telephones when using a headset.

Conference

This function is intend for use with Avaya M-Series and T-Series phones only. When pressed, the button invokes the same conference process as dialing **Feature 3**.

Details

- **Action**: Advanced | Call | Conference.
- **Action Data**: None.
- **Default Label**: Conf or Conference Add.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - M-Series and T-Series.
    - The button is equivalent to **Feature 3**.

Conference Add

Conference add controls can be used to place the user, their current call and any calls they have on hold into a conference. When used to start a new conference, the system automatically assigns a conference ID to the call. This is termed ad-hoc (impromptu) conferencing.

If the call on hold is an existing conference, the user and any current call are added to that conference. This can be used to add additional calls to an ad-hoc conference or to a meet-me conference. Conference add can be used to connect two parties together. After creating the conference, the user can drop from the conference and the two incoming calls remain connected.

For R11.0 and higher, the button has additional features:

- When pressed during a normal two-party call, that call is turned into a two-party conference call. This then provides access to the phone's other conference control, such as to add other parties, without interrupting the call.
- During an existing conference, pressing the button (on 1400, 1600, 9500, 9600 and J100 Series phones) provides a menu to enter the number of an additional party to add to the conference without put the conference on hold. The other parties in the conference can hear the call progress and if answered the other party is immediately in the conference.

For further details, see Conferencing on page 686.

Details

- **Action**: Advanced | Call | Conference Add.
- **Action Data**: None.
- **Default Label**: Conf+ or Conference Add.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Conference Meet Me

Conference meet-me refers to features that allow a user or caller to join a specific conference by using the conference's ID number (either preset in the button's configuration or entered at the time of joining the conference).

Note:

- Conference Meet Me features can create conferences that include only one or two parties. These are still conferences that are using resources from the host system's conference capacity.

Conference ID Numbers

Each conference has a conference ID number:

- **Ad-Hoc Conferences** - By default, ad-hoc conferences are assigned numbers starting from 100 for the first conference in progress. Therefore, for conference Meet-Me features, you should always specify a number away from this range ensure that the conference joined is not an ad-hoc conference started by other users. It is not possible to join a conference using conference Meet-Me features when the conference ID is in use by an ad-hoc conference.
- **User Personal Meet-Me Conferences** - Each user's own extension number is treated as their own personal conference number. Only that user is able to start a conference using that number as the conference ID. Any one else attempting to start a conference with that number will find themselves in a conference but on hold until the owner also joins. Personal conferences are always hosted on the owner's system.
- **System Meet-Me Conferences** - Each of these is assigned a conference ID number when the conference settings are configured.

For further details, see Conferencing on page 686.

Note:

When a user calls from their mobile twinned number, the personal conference feature will only work if they access the conference using an FNE 18 service.

Multi-Site Network Conferencing

Meet Me conference IDs are now shared across a multi-site network. For example, if a conference with the ID 500 is started on one system, anyone else joining conference 500 on any system will join the same conference. Each conference still uses the conference resources of the system on which it was started and is limited by the available conference capacity of that system.

Previously separate conferences, each with the same conference ID, could be started on each system in a multi-site network.

Other Features

- **Transfer to a Conference Button** - A currently connected caller can be transferred into the conference by pressing **TRANSFER**, then the Conference Meet Me button and **TRANSFER** again to complete the transfer. This allows the user to place callers into the conference specified by the button without being part of the conference call themselves. This option is only support on Avaya phones with a fixed **TRANSFER** button.
- **Conference Button Status Indication** - When the conference is active, any buttons associated with the conference ID indicate the active state.

Details

- **Action:** Advanced | Call | Conference Meet Me.

- **Action Data**: Conference number. This can be an alphanumeric value up to 15 characters.
  - **User Personal Conference Number** Each user's own extension number is treated as their own personal conference number. Only that user is able to start a conference using that number as the conference ID. Any one else attempting to start a conference with that number will find themselves in a conference but on hold until the owner also joins. Personal conferences are always hosted on the owner's system.
  - When a user calls from their mobile twinned number, the personal conference feature will only work if they access the conference using an FNE18 service.
- **Default Label**: CnfMM <conference number> or Conf. Meet Me <conference number>.
- **Toggles:** No.
- **Status Indication**: Yes

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

For a Conference Meet Me configured to the user's own extension number, the indicator flashes red when the conference is in use but the user has not joined. There is also an abbreviated ring when the indicator changes to flashing red. It changes to solid red when the user joins.

- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Consult

Supported for CTI emulation only.

Details

- **Action**: Emulation | Consult.
- **Action Data**: None.
- **Default Label**: Cnslt.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.

- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Coverage Appearance

Creates a button that alerts when a call to the specified covered user is unanswered after that users **Individual Coverage Timer** expires. For details, see Call Coverage Buttons on page 1210.

The call coverage appearance button user must also have at least one call appearance button programmed. The covered user does not need to be using call appearance buttons.

Coverage appearance functions, assigned to buttons that do not have status lamps or icons, are automatically disabled until the user logs in at a phone with suitable buttons.

Appearance buttons can be set with a ring delay if required or to not ring. This does not affect the visual alerting displayed next to the button. The delay uses the user's **Ring Delay** (**User** > **Telephony** > **Multi-line Options**) setting.

Details

- **Action**: Appearance | Coverage Appearance.
- **Action Data**: User name.
- **Default Label**: <user name>.
- **Toggles**: No.
- **Status Indication**: Yes.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Dial

This action is used to dial the number contained in the Telephone Number field. A partial number can be enter for the user to complete. On buttons with a text label area, **Dial** followed by the number is shown.

Details

- **Action Data**: Telephone number or partial telephone number.

- **Default Label**: Dial.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - This button action is also supported by the Vantage Connect Expansion application.
    - 9500 Series, 9600 Series and J100 Series.
    - 1400 Series and 1600 Series.
    - M-Series and T-Series.

Dial 3K1

The call is presented to local exchange as a "3K1 Speech Call". Useful in some where voice calls cost less than data calls.

Details

- **Action**: Advanced | Dial | Dial 3K1.
- **Action Data**: Telephone number.
- **Default Label**: D3K1 or Dial 3K1.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Dial 56K

The call presented to local exchange as a "Data Call".

Details

- **Action**: Advanced | Dial | Dial 56K.

- **Action Data**: Telephone number.
- **Default Label**: D56K or Dial 56K.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Dial 64K

The call is presented to local exchange as a "Data Call".

Details

- **Action**: Advanced | Dial | Dial 64K.
- **Action Data**: Telephone number.
- **Default Label**: D64K or Dial 64K.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Dial CW

Call the specified extension number and force call waiting indication on if the extension is already on a call. The call waiting indication will not work if the extension called has multiple call appearance buttons in use.

Details

- **Action**: Advanced | Dial | Dial CW.

- **Action Data**: User number.
- **Default Label**: DCW or Dial Call Waiting.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Dial Direct

Automatic intercom functions allow you to call an extension and have the call automatically answered on speaker phone after 3 beeps. The extension called must support a handsfree speaker. If the extension does not have a handsfree microphone then the user must use the handset if they want to talk. If the extension is not free when called, the call is presented as a normal call on a call appearance button if available.

This feature can be used as part of handsfree announced transfers.

Details

- **Action**: Advanced | Dial | Dial Direct.
- **Action Data**: User number or name or blank for entry when pressed. If left blank, the **Dial Direct** button can be used with User buttons to specify the target.
- **Default Label**: Dirct or Auto Intercom.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - This button action is also supported by the Vantage Connect Expansion application.

Dial Emergency

Dials the number specified regardless of any outgoing call barring applicable to the user. See Configuration for Emergency Calls on page 772.

- Details of calls made using this function can be viewed using an **Emergency View** button. See Emergency View on page 1142.

Details

- **Action**: Advanced | Dial | Dial Emergency.
- **Action Data**: Telephone number. This must match the emergency call routing configured for the system or for the extension location.
- **Default Label**: Emrgy or Dial Emergency.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Dial Inclusion

This feature allows you to intrude on another user's call to talk to them. Their current call is put on hold while you talk and automatically reconnected when you end the intrusion. The intruder and the target extension can then talk but cannot be heard by the other party. This can include intruding into a conference call, where the conference will continue without the intrusion target.

During the intrusion all parties hear a repeated intrusion tone. When the intruder hangs-up the original call parties are reconnected. Attempting to hold a dial inclusion call simply ends the intrusion. The inclusion cannot be parked.

- Intrusion features are controlled by the **Can Intrude** setting of the user intruding and the **Cannot Be Intruded** setting of user being intruded on. By default, no users can intrude and all users cannot be intruded.
- Intrusion features uses system conference resources during the call. If insufficient conference resource are available, the feature cannot be used.

The system support a range of other call intrusion methods in addition to this feature.

Details

- **Action**: Advanced | Dial | Dial Inclusion.

- **Action Data**: User number or name or blank for user selection when pressed. On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.
- **Default Label**: Inclu or Dial Inclusion.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Dial Intercom

Automatic intercom functions allow you to call an extension and have the call automatically answered on speaker phone after 3 beeps. The extension called must support a handsfree speaker. If the extension does not have a handsfree microphone then the user must use the handset if they want to talk. If the extension is not free when called, the call is presented as a normal call on a call appearance button if available.

This feature can be used as part of handsfree announced transfers.

Details

- **Action**: Emulation | Dial Intercom.
- **Action Data**: User number or name or blank for number entry when pressed. On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.
- **Default Label**: Idial or Auto Intercom.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
    1. The button is equivalent to **Feature 66 <number>**.

Dial Paging

Makes a paging call to an extension or group specified. If no number is specified, this can be dialed after pressing the button. The target extension or group members must be free and must support handsfree auto-answer in order to hear the page.

On Avaya phones with a **CONFERENCE** button, a paged user can convert the page call into a normal call by pressing that button.

Details

- **Action**: Advanced | Dial | Dial Paging.
- **Action Data**: User number or name or group number or name or blank for number entry when pressed.
- **Default Label**: Page.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - This button action is also supported by the Vantage Connect Expansion application.
    - 9500 Series, 9600 Series and J100 Series.
    - 1400 Series and 1600 Series.
    - M-Series and T-Series.
    - 1100 Series and 1200 Series.

Dial Physical Extn by Number

Call the specified extension using its Base Extension number setting. This is regardless of the current user logged in at that extension and any forwarding, follow me or do not disturb settings applied by the extension user. This function requires the extension to be assigned a default extension number in the system configuration. If the extension does not have a default extension number, Dial Physical Extn by Id should be used.

Details

- **Action**: Advanced | Dial | Dial Physical Extn by Number.
- **Action Data**: Extension port base extension number.
- **Default Label**: PhyEx or Dial Physical Extn.
- **Toggles**: No.
- **Status Indication**: No.

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Dial Physical Number by ID

Call the specified extension, if free, regardless of the current user logged in at that extension and any forwarding, follow me or do not disturb settings applied by the extension user. This function uses the port ID shown in the system configuration.

Details

- **Action**: Advanced | Dial | Dial Physical Extn by Id.
- **Action Data**: Extension port ID number.
- **Default Label**: DialP or Dial Extn by Id.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Dial Speech

This feature allows a short code to be created to force the outgoing call to use the Speech bearer capability.

Details

- **Action**: Advanced | Dial | Dial Speech.
- **Action Data**: Telephone number.
- **Default Label**: DSpch or Dial Speech.
- **Toggles**: No.

- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Dial V110

The call is presented to local exchange as a "Data Call".

Details

- **Action**: Advanced | Dial | Dial V110.
- **Action Data**: Telephone number.
- **Default Label**: DV110 or Dial V110.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Dial V120

The call is presented to local exchange as a "Data Call".

Details

- **Action**: Advanced | Dial | Dial V120.
- **Action Data**: Telephone number.
- **Default Label**: DV120 or Dial V120.
- **Toggles**: No.
- **Status Indication**: No.

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Dial Video

The call is presented to the local exchange as a "Video Call".

Details

- **Action**: Advanced | Dial | Dial Video.
- **Action Data**: Telephone number.
- **Default Label**: Dvide or Dial Video.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Directed Call Pickup

Pickup a call ringing at a specific extension or hunt group.

Details

- **Action**: Emulation | Directed Pickup.
- **Action Data**: User number or name or group number or name or blank for number entry when pressed. On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.
- **Default Label**: DpkUp or Call Pickup.
- **Toggles**: No.
- **Status Indication**: No.

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
    1. The button is equivalent to **Feature 76**.
  - 1100 Series and 1200 Series.

Directory

A **Dir** button provides access to various directories and allows telephone number selection by dialed name matching. The directories available for searching depend on the phone type, see User Directory Access. Once they user has selected a directory, dialing on the dial pad letter keys is used to filter the display of matching names, with controls for scrolling through the matching names and for calling the currently displayed name.

Details

- **Action**: Emulation | Directory.
- **Action Data**: None.
- **Default Label**: Dir.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Display Msg

Allows the sending of text messages to digital phones on the local system.

Details

- **Action**: Advanced | Dial | Display Msg.

- **Action Data**: The telephone number takes the format N";T" where:
  - **N** is the target extension.
  - **T** is the text message. Note that the **";** before the text and the **"** after the text are required.
- **Default Label**: Displ.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Do Not Disturb Exception Add

Adds a number to the user's "Do Not Disturb Exception List". This can be the number of an internal user or a number to match the CLI of a particular external caller. Calls from that number, except hunt group calls, will ignore the user's Do Not Disturb setting. For further details see Do Not Disturb (DND).

Details

- **Action**: Advanced | Do Not Disturb | Do Not Disturb Exception Add.
- **Action Data**: Telephone number or CLI. Up to 31 characters. For CLI numbers any prefix added by the system must also be included.
- **Default Label**: DNDX+.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Do Not Disturb Exception Delete

Removes a number from the user's "Do Not Disturb Exception List". This can be the number of an internal user or a number to match the CLI of a particular external caller.

Details

- **Action**: Advanced | Do Not Disturb | Do Not Disturb Exception Delete.
- **Action Data**: Telephone number or CLI.
- **Default Label**: DNDX-.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Do Not Disturb Off

Cancels the user's 'do not disturb' mode if set. This button function is obsolete as the do not disturb on function toggles on/off and indicates the button status.

Details

- **Action**: Advanced | Do Not Disturb | Do Not Disturb Off.
- **Action Data**: None.
- **Default Label**: DNDOf.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.
  - 1100 Series and 1200 Series.

Do Not Disturb On

Enables the user's 'do not disturb' mode.

Details

- **Action**: Advanced | Do Not Disturb | Do Not Disturb On.
- **Action Data**: None.
- **Default Label**: DNDOn or Do Not Disturb.
- **Toggles**: Yes.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
    1. The button is equivalent to **Feature 85**.
  - 1100 Series and 1200 Series.
  - This button action is also supported by the Vantage Connect Expansion application.

Drop

This action is supported on phones which do not have a permanent **Drop** button.

- For a currently connected call, pressing **Drop** disconnects the call. When drop is used to end a call, silence is returned to the user rather than dial tone. This is intended operation, reflecting that **Drop** is mainly intended for use by call center headset users.
- If the user has no currently connected call, pressing **Drop** will redirect a ringing call using the user's **Forward on No Answer** setting if set or otherwise to voicemail if available.
- For a conference call, on phones with a suitable display, **Drop** can be used to display the conference parties and allow selection of which party to drop from the conference.

Details

- **Action**: Emulation | Drop.
- **Action Data**: None.
- **Default Label**: Drop or Drop Call.
- **Toggles**: No.
- **Status Indication**: No.

- **User Admin**: ✓.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.

Emergency View

A button set to this function indicates when a call has been made from the system to which the user's extension is registered. The definition of an emergency call is one using a number routed by a **Dial Emergency** button or short code.

- Pressing the button displays details of currently connected emergency calls (the first 10).
- After pressing the button, the **History** option displays details of any previously connected emergency calls (the first 30) and allows deletion those call details.
- The emergency call history for a system is shared by all users on the same system. Therefore updates to or deleting the history affects the details shown on all user phones on the same system.
- The time shown in the call details, is the UTC time of the alarm calls. On J189 phones, it also includes the location name if an IP Office **Location** entry was used to route the call.
- Note that the button only works for an extension registered to the same system as the outgoing trunk used for the emergency call.

Details

- **Action**: Emulation | Emergency View.
- **Action Data**: None
- **Default Label**: 911–View or EView
- **Toggles**: No.
- **Status Indication**: Yes
  - The button gives a single ring and then flashes when there is a connected emergency call in progress.
  - The button remains on when there are previous emergency calls in the alarm history.
  - Note that there is a delay of a few seconds in changes of the lamp state.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Extn Login

Extn Login allows a user who has been configured with a **Login Code** (User | Telephony | Supervisor Settings) to take over ownership of any extension. That user's extension number becomes the extension number of the extension while they are logged. This is also called ‘hot desking’.

Hot desking is not supported for H175, E129 and J129 telephones.

When used, the user is prompted to enter their extension number and then their log in code. Login codes of up to 15 digits are supported with **Extn Login** buttons. Login codes of up to 31 digits are supported with **Extn Login** short codes.

When a user logs in, as many of their user settings as possible are applied to the extension. The range of settings applied depends on the phone type and on the system configuration.

By default, on 1400 Series, 1600 Series, 9500 Series and 9600 Series phones, the user's call log and personal directory are accessible while they are logged in. This also applied to M-Series and T-Series telephones.

On other types of phone, those items such as call logs and speed dials are typically stored locally by the phone and will not change when users log in and log out.

If the user logging in was already logged in or associated with another phone, they will be automatically logged out that phone.

Details

- **Action**: Advanced | Extension | Extn Login.
- **Action Data**: None.
- **Default Label**: Login.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Extn Logout

Logs out a user from the phone. The phone will return to its normal default user, if an extension number is set against the physical extension settings in the configuration. Otherwise it takes the setting of the **NoUser** user. This action is obsolete as Extn Login can be used to log out an existing logged in user.

- If the user who logged out was the default user for an extension, dialing *36 will associate the extension with the user unless they are set to forced log in.
- This feature cannot be used by a user who does not have a log in code.

Details

- **Action**: Advanced | Extension | Extn Logout.
- **Action Data**: None.
- **Default Label**: Logof or Logout.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.
  - This button action is also supported by the Vantage Connect Expansion application.

Flash Hook

Sends a hook flash signal to the currently connected line if that line is an analog line.

Details

- **Action**: Advanced | Miscellaneous | Flash Hook.
- **Action Data:** Optional. Normally this field is left blank. It can contain the destination number for a Centrex Transfer for external calls on a local analog line from a Centrex service provider. See Centrex Transfer on page 909.
- **Default Label**: Flash or Flash Hook.
- **Toggles**: No.
- **Status Indication**: No.

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Follow Me Here

Causes calls to the extension number specified, to be redirected to this user's extension. User's with a log in code will be prompted to enter that code when using this function. For further details, see Follow Me on page 865.

Details

- **Action**: Advanced | Follow Me | Follow Me Here.
- **Action Data**: User name or user number.
  - If a user name or user number has been entered in the **Action Data** field, when the interactive menu opens, press `Enter` to activate Follow Me Here for the number displayed on the screen.
  - This field can be left blank for number entry when pressed.
  - On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.
- **Default Label**: Here+ or Follow Me Here.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Follow Me Here Cancel

Cancels any 'Follow Me Here' set on the specified extension. Only works if entered at the extension to which the extension's calls are being sent by the follow me action. For further details, see Follow Me on page 865.

Details

- **Action**: Advanced | Follow Me | Follow Me Here Cancel.
- **Action Data**: User number or blank for number entry when pressed.
  - If a user name or user number has been entered in the **Action Data** field, when the interactive menu opens, press `Enter` to deactivate Follow Me Here for the number displayed on the screen.
  - On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.
- **Default Label**: Here- or Follow Me Here-.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Follow Me To

Leaving the extension blank prompts the user to enter the extension to which their calls should be redirected. User's with a log in code will be prompted to enter that code when using this function. For further details, see Follow Me on page 865.

Details

- **Action**: Advanced | Follow Me | Follow Me To.
- **Action Data**: User name or user number or blank for number entry when pressed.
  - If a user name or user number has been entered in the **Action Data** field, when the interactive menu opens, press `Enter` to activate Follow Me To for the number displayed on the screen.
  - On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.

- **Default Label**: FolTo or Follow Me To.
- **Toggles**: Yes.
- **Status Indication**: Yes. On/off status indication is provided if the button is programmed with a user name or number.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Forward Hunt Group Calls Off

Cancels the forwarding of the user's hunt group calls. This function is obsolete since the button function Forward Hunt Group Calls On toggles on/off and indicates status.

Details

- **Action**: Advanced | Forward | Forward Hunt Group Calls Off.
- **Action Data**: None.
- **Default Label**: FwdH-.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Forward Hunt Group Calls On

Forward the user's hunt group calls (internal and external). This function only works when forward unconditional is also on and uses the same forwarding number as forward unconditional.

This option is only applied for calls to **Sequential** and **Rotary** type hunt groups. Calls from other hunt group types are not presented to the user when they have Forward Unconditional active. Note also that hunt group calls cannot be forwarded to another hunt group.

Details

- **Action**: Advanced | Forward | Forward Hunt Group Calls On.
- **Action Data**: None.
- **Default Label**: FwdH+ or Fwd HG Calls.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Forward Number

Sets the number to which calls are forwarded when the user has forwarding on. Used for all forwarding options unless a separate **Forward On Busy Number** is also set. Forwarding to an external number is blocked if **Inhibit Off-Switch Transfers** is selected within the system configuration.

Details

- **Action**: Advanced | Forward | Forward Number.
- **Action Data**: Telephone number.
- The field to be left blank to prompt the user for entry when the button is pressed. If blank, users with a log in code will be prompted to enter that code.
- On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.
- **Default Label**: FwdNo or Fwd Number.
- **Toggles**: No.
- **Status Indication**: Yes. For a button with a prefixed number, status indication will indicate when that number matches the users current set number. For a button with a no number, status indication will show when a number has been set.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - This button action is also supported by the Vantage Connect Expansion application.

Forward On Busy Number

Sets the number to which calls are forwarded when using 'Forward on Busy' and/or 'Forward on No Answer'. Forwarding to an external number is blocked if **Inhibit Off-Switch Transfers** is selected within the system configuration.

For further details, see Forward on Busy on page 869.

Details

- **Action**: Advanced | Forward | Forward on Busy Number.
- **Action Data**: Telephone number.
  - The field to be left blank to prompt the user for entry when the button is pressed. If blank, users with a log in code will be prompted to enter that code.
  - On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.
- **Default Label**: FwBNo or Fwd Busy Number.
- **Toggles**: No.
- **Status Indication**: Yes. For a button with a prefixed number, status indication indicates when that number matches the user's current set number. For a button with a no number, status indication shows when a number has been set.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.

- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - This button action is also supported by the Vantage Connect Expansion application.

Forward On Busy Off

Switches forward on busy off. This button function is obsolete, as Forward On Busy On can be used to switch forward on busy on/off and provides status indication.

Details

- **Action**: Advanced | Forward | Forward on Busy Off.
- **Action Data**: None.
- **Default Label**: FwBOf.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Forward On Busy On

Enables forwarding when the user's extension is busy. For users with call appearance buttons, they will only return busy when all call appearance buttons are in use. Uses the **Forward Number** as its destination unless a separate **Forward on Busy Number** is set. For further details, see Forward on Busy on page 869.

Details

- **Forward Internal** (**User | Forwarding**) can also be used to control whether internal calls are forwarded.
- **Action**: Advanced | Forward | Forward on Busy On.
- **Action Data**: None.
- **Default Label**: FwBOn or Fwd Busy.
- **Toggles**: Yes.

- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - This button action is also supported by the Vantage Connect Expansion application.

Forward On No Answer Off

Switches forward on no answer off. This button function is obsolete, as Forward On No Answer On can be used to switch forward on no answer on/off and provides status indication.

Details

- **Action**: Advanced | Forward | Forward on No Answer Off.
- **Action Data**: None.
- **Default Label**: FwNOf.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Forward On No Answer On

Switches forward on no answer on/off. The time used to determine the call as unanswered is the user's no answer time. Uses the **Forward Number** as its destination unless a separate **Forward on Busy Number** is set.

For further details, see Forward on No Answer on page 871.

Details

- **Forward Internal** (**User | Forwarding**) can also be used to control whether internal calls are forwarded.
- **Action**: Advanced | Forward | Forward on No Answer On.
- **Action Data**: None.
- **Default Label**: FwNOn or Fwd No Answer.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - This button action is also supported by the Vantage Connect Expansion application.

Forward Unconditional Off

Switch 'forward all calls' off. This does not affect 'Forward on No Answer' and/or 'Forward on Busy' if also on. This function is obsolete as a button set to Forward Unconditional On toggles on/off and indicates when on.

Details

- **Action**: Advanced | Forward | Forward Unconditional Off.
- **Action Data**: None.
- **Default Label**: FwUOf.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Forward Unconditional On

This function is also known as 'divert all' and 'forward all'. It forwards all calls, except hunt group and page calls, to the forward number set for the user's extension. To also forward hunt group calls to the same number 'Forward Hunt Group Calls On' must also be used.

For further details, see Forward Unconditional on page 867.

Details

- **Forward Internal** (**User | Forwarding**) can also be used to control whether internal calls are forwarded.
  - In addition to the lamp indication shown below, some phones display **D** when forward unconditional is on.
- **Action**: Advanced | Forward | Forward Unconditional On.
- **Action Data**: None.
- **Default Label**: FwUOn or Fwd Unconditional.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
    1. The button is equivalent to **Feature 4 <number>**.
  - This button action is also supported by the Vantage Connect Expansion application.

Group

Monitors the status of a hunt group queue. This option is only supported for hunt groups with queuing enabled. The user does not have to be a member of the group.

Depending on the users button type, indication is given for when the group has alerting calls and queued calls (queued in this case is defined as more calls waiting than there are available group members).

Pressing a **Group** button answers the longest waiting call.

The definition of queued calls include group calls that are ringing. However, for operation of the **Group** button, ringing calls are separate from other queued calls.

Details

- **Action**: Group.
- **Action Data**: Group name enclosed in " " double-quotes or group number.
- **Default Label**: <group name>.
- **Toggles**: No.
- **Status Indication**: Required.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series, M-Series
- No calls	Off	Off	Grey	Off
- Call alerting	Green flash	Green flash	Blue	Slow flash
- Calls queued	Red flash	Red flash	**Green**	Slow flash

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Group Listen On

Using group listen allows callers to be heard through the phone's handsfree speaker but to only hear the phone's handset microphone. When group listen is enabled, it modifies the handsfree functionality of the user’s phone in the following manner

- When the user’s phone is placed in handsfree/speaker mode, the speech path from the connected party is broadcast on the phone speaker but the phone's base microphone is disabled.
- The connected party can only hear speech delivered through the phone's handset microphone.
- Group listen is not supported for IP phones or when using a phone's **HEADSET** button.
- For T-Series and M- Series phones, this option can be turned on or off during a call. For other phones, currently connected calls are not affected by changes to this setting, instead group listen must be selected before the call is connected.

  Group listen is automatically turned off when the call is ended.

Details

- **Action**: Advanced | Extension | Group Listen On.
- **Action Data**: None.
- **Default Label**: Group Listen On.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 9500	T-Series,
On.	Green on	▲ On
Off.	Off	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series, 9500 Series.
  - M-Series and T-Series.
    1. The button is equivalent to **Feature 802** (On) and **Feature #802** (Off).

Group Paging

Makes a paging call to an extension or group specified. If no number is specified, this can be dialed after pressing the button. The target extension or group members must be free and must support handsfree auto-answer in order to hear the page.

On Avaya phones, a paged user can convert the page call into a normal call by pressing the **Conference** button.

Details

- **Action**: Emulation | Group Paging.
- **Action Data**: User number or name or group number or name. On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.
- **Default Label**: GrpPg.
- **Toggles**: No.
- **Status Indication**: Yes.
- **User Admin**: Yes.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.

- 1400 Series and 1600 Series.
- M-Series and T-Series.
    1. The button is equivalent to **Feature 60 <number>**.
- 1100 Series and 1200 Series.

Headset Toggle

This function is intended for use with Avaya phones that have separate handset and headset sockets but do not provide a dedicated Headset button. On phones without a headset socket or with a dedicated headset button this control will have no effect.

Details

- **Action**: Miscellaneous | Headset Toggle.
- **Action Data**: None.
- **Default Label**: HdSet.
- **Toggles**: Yes.
- **Status Indication**: Yes.
- **User Admin**: No.

Hold Call

This uses the Q.931 Hold facility, and "holds" the incoming call at the ISDN exchange, freeing up the ISDN B channel. The Hold Call feature "holds" the current call to a slot. The current call is always automatically placed into slot 0 if it has not been placed in a specified slot. Only available if supported by the ISDN exchange.

Details

- **Action**: Advanced | Hold | Hold Call.
- **Action Data**: ISDN Exchange hold slot number or blank (slot 0).
- **Default Label**: Hold.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
    - 1400 Series and 1600 Series.

Hold CW

Place the user's current call on hold and answers the waiting call. This function is not supported on phones which have multiple call appearance buttons set.

Details

- **Action**: Advanced | Hold | Hold CW.
- **Action Data**: None.
- **Default Label**: HoldCW.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Hold Music

This feature allows the user to listen to the system's music on hold. See Music On Hold for more information.

Details

- **Action**: Advanced | Hold | Hold Music.
- **Action Data**: Optional. Systems can support multiple hold music sources. However only the system source is supported for **Hold Music** buttons.
- **Default Label**: Music or Hold Music.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Hunt Group Enable

An individual users membership of any particular hunt groups is programmed through the system configuration. This control allows the user to enable or disable that membership. While enabled, the user can receive hunt group calls when logged in.

Details

- In addition to the lamp indication below, phones display **G** when any group membership is enabled.
- **Action**: Advanced | Hunt Group | Hunt Group Enable.
- **Action Data**: Group number or name or blank for all groups of which the user is a member.
- **Default Label**: HGEna or HG Enable.
- **Toggles**: Yes.
- **Status Indication**: Required.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - This button action is also supported by the Vantage Connect Expansion application.

Hunt Group Disable

This function is obsolete, the Hunt Group Enable function being able to toggle membership between enabled and disabled and providing lamp indication of when membership is enabled.

An individual user's membership of any particular hunt groups is programmed through the system configuration. This control allows the user to disable that membership. They will no longer receive calls to that hunt group until their membership is enabled again.

Details

- **Action**: Advanced | Hunt Group | Hunt Group Disable.
- **Action Data**: Group number or blank for all groups of which the user is a member.
- **Default Label**: HGDis.

- **Toggles**: No.
- **Status Indication:** No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Inspect

Supported for CTI emulation only.

Allows users on display phones to determine the identification of held calls. Allows users on an active call to display the identification of incoming calls.

Details

- **Action**: Emulation | Inspect.
- **Action Data**: None.
- **Default Label**: Inspt.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Internal Auto-Answer

This function is also known as handsfree auto-answer. It sets the user's extension to automatically connect internal calls after a single tone. This function should only be used on phones that support handsfree operation.

Details

- **Action**: Emulation | Internal Auto-Answer.
- **Action Data**: Optional.
  - If left blank this function acts as described above for internal auto-answer.
  - **FF** can be entered. In that case the button will enable/disable headset force feed operation for external calls. In this mode, when headset mode is selected but the phone is idle, an incoming external call will cause a single tone and then be automatically connected. This

operation is only supported on Avaya phones with a fixed **HEADSET** button. Ring delay is applied if set on the appearance button receiving the call before the call is auto-connected.

- **Default Label**: HFAns or Auto Answer.
- **Toggles**: Yes.
- **Status Indication**: Required.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: Yes.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Last Number Redial

This function is intend for use with Avaya M-Series and T-Series phones only. When pressed, the button invokes the same last number redial process as dialing **Feature 5**.

Details

- **Action**: Advanced | Call | Last Number Redial.
- **Action Data**: None.
- **Default Label**: Again.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - M-Series and T-Series.
    - The button is equivalent to **Feature 5**.

Leave Word Calling

Supported for CTI emulation only.

Leaves a message for the user associated with the last number dialed to call the originator.

Details

- **Action**: Emulation | Leave Word Calling.
- **Action Data**: None.
- **Default Label**: LWC.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Line Appearance

Creates an line appearance button linked to the activity of a specified line appearance ID number. The button can then be used to answer and make calls on that line. For details, see Line Appearance Buttons on page 1215.

The line appearance button user must also have at least one call appearance button programmed before line appearance buttons can be programmed.

Line appearance functions, assigned to buttons that do not have status lamps or icons, are automatically disabled until the user logs in at a phone with suitable buttons.

Details

- **Action**: Appearance | Line Appearance.
- **Action Data**: Line ID number.
- **Default Label**: Line <Line ID number>.
- **Toggles**: No.
- **Status Indication**: Yes.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
    1. Not supported on T7000, T7100, M7100 and M7100N phones.

MADN Call Appearance

Multiple Appearance Directory Number (MADN) emulates an Avaya Communication Server 1000 key and lamp style feature.

When using normal appearance buttons to answer or make calls, the information (name and number) presented to the other end of the call is that of the button user (subject to any other line and short code settings). When using a MADN call appearance button, the information presented is that of the user to which the button is associated rather than that of the button user.

The user associated with a MADN button does not need to have a license or an active extension. However, they must have an extension number. The system considers the user's records when the user makes a call using the MADN buttons. You can have up to 30 MADN buttons associated with the same user.

MADN can operate in two modes:

- **MADN Single Call Appearance (SCA)**

  The button is configured with the user name of the associated user and one of their call appearances. This provides the following behaviors:

  - Incoming extension calls: The button acts like a Bridged Appearance button to the associated user.
  - Incoming group calls: The button alerts if associated user is a member of the hunt group and alerting.
  - Outgoing calls: The button acts like a Call Appearance. It presents the call as originating from the button user but with the number and name of the associated user in the calling party information.

- **MADN Multiple Call Appearance (MCA)**

  The button is configured with just the user name of the associated user. This provides the following behaviors:

  - Incoming extension calls: The button acts like a Coverage Appearance to the associated user.
  - Incoming groups calls: The button does not alert.
  - Outgoing calls: The button acts like a Call Appearance. It presents the call as originating from the button user but with the number of the associated user in the calling party information.

Details

- **Action** Either:
  - Appearance | MADN Single Call Appearance
  - Appearance | MADN Multiple Call Appearance
- **Action Data**:
  - MADN Single Call Appearance: User Name, Call Appearance button number and Ring Delay.

  - MADN Multiple Call Appearance: User Name and Ring Delay.
- **Default Label**:
  - MADN SCA: <MADN number S=>
  - MADN MCA: <MADN number M=>
- **Toggles**: No.
- **Status Indication**:
  - MADN SCA: Yes. See Bridge Appearance Button Indication.
  - MADN MCA: Yes. See Coverage Button Indication.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.

Manual Exclude

Supported for CTI emulation only.

Details

- **Action**: Emulation | Manual Exclude
- **Action Data**: None.
- **Default Label**: Excl.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

MCID Activate

This action is used with ISDN Malicious Caller ID call tracing. It is used to trigger a call trace at the ISDN exchange. The call trace information is then provided to the appropriate legal authorities.

This option requires the line to the ISDN to have MCID enabled at both the ISDN exchange and on the system. The user must also be configured with **Can Trace Calls** (**User | Telephony | Supervisor Settings**) enabled.

Currently, in Server Edition network, MCID is only supported for users using an MCID button and registered on the same IP500 V2 Expansion system as the MCID trunks.

Details

- **Action**: Advanced | Miscellaneous | MCID Activate.
- **Action Data**: None.
- **Default Label**: MCID or Malicious Call.
- **Toggles**: No.
- **Status Indication**: Yes.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Monitor Analog Trunk MWI

Enables a user to receive message waiting indicator (MWI) signals from analog trunks terminating on the ATM4U-V2 card. MWI is a telephone feature that turns on a visual indicator on a telephone when there are recorded messages.

Details

- **Action**: Advanced | Voicemail | Monitor Analog Trunk MWI.
- **Action Data**: The line appearance ID of the analog line for which MWI will be received.
- **Default Label**: Trunk MWI.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.

Off Hook Station

Enables the user's extension to be controlled by an application, for example SoftConsole. Calls can then be answered and cleared through the application without having to manually go off or on hook. Requires the phone to support full handsfree operation.

Details

- **Action**: Advanced | Miscellaneous | Off Hook Station.
- **Action Data**: None.
- **Default Label**: OHStn.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Pause Recording

This feature can be used to pause any call recording. It can be used during a call that is being recorded to omit sensitive information such as customer credit card information. This feature can be used with calls that are recorded both manually or calls that are recorded automatically.

The button status indicates when call recording has been paused. The button can be used to restart call recording. The system **Auto Restart Paused Recording** (System | Voicemail) setting can be used to set a delay after which recording is automatically resumed.

If the voicemail system is configured to provide advice of call recording warnings, then pausing the recording will trigger a "Recording paused" prompt and a repeat of the advice of call recording warning when recording is resumed.

Details

- **Action**: Advanced | Call | Pause Recording.
- **Action Data**: None.
- **Default Label**: PauseRec or Pause Recording.
- **Toggles**: Yes.
- **Status Indication**: Yes.
- **User Admin**: No.

- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.

Priority Call

This feature allows the user to call another user even if they are set to 'do not disturb'. A priority call will follow forward and follow me settings but will not go to voicemail.

Details

- **Action**: Advanced | Call | Priority Call.
- **Action Data**: User number or name.
- **Default Label**: PCall or Priority Call.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - This button action is also supported by the Vantage Connect Expansion application.

Priority Calling

Supported for CTI emulation only.

Details

- **Action**: Emulation | Priority Calling.
- **Action Data**: None.
- **Default Label**: Pcall.
- **Toggles**: No.
- **Status Indication**: No.

- **Phone Support**: The following table indicates phones which support the programmable button:
  - 1400 Series and 1600 Series.

Private Call

When on, any subsequent calls cannot be intruded on until the user's private call status is switched off. The exception is Whisper Page which can be used to talk to a user on a private call.

Note that use of private calls is separate from the user's intrusion settings. If the user's **Cannot be Intruded** (User | Telephony | Supervisor Settings) setting is enabled, switching private calls off does not affect that status. To allow private calls to be used to fully control the user status, **Cannot be Intruded** (User | Telephony | Supervisor Settings) should be disabled for the user.

If enabled during a call, any current recording, intrusion or monitoring is ended.

Details

- **Action**: Advanced | Call | Private Call.
- **Action Data**: None.
- **Default Label**: PrivC or Private Call.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Relay Off

Opens the specified switch in the system's external output port (**EXT O/P**).

This feature is not supported on Linux based systems. For Server Edition, this option is only supported on Expansion System (V2) units.

Details

- **Action**: Advanced | Relay | Relay Off.
- **Action Data**: Switch number (1 or 2).
- **Default Label**: Rely-.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Relay On

Closes the specified switch in the system's external output port (**EXT O/P**).

This feature is not supported on Linux based systems. For Server Edition, this option is only supported on Expansion System (V2) units.

Details

- **Action**: Advanced | Relay | Relay On.
- **Action Data**: Switch number (1 or 2).
- **Default Label**: Rely+ or Relay On.
- **Toggles**: Yes.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Relay Pulse

Closes the specified switch in the system's external output port (**EXT O/P**) for 5 seconds and then opens the switch.

This feature is not supported on Linux based systems. For Server Edition, this option is only supported on Expansion System (V2) units.

Details

- **Action**: Advanced | Relay | Relay Pulse.
- **Action Data**: Switch number (1 or 2).
- **Default Label**: Relay or Relay Pulse.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Resume Call

Resume a call previously suspended to the specified ISDN exchange slot. The suspended call may be resumed from another phone/ISDN Control Unit on the same line.

Details

- **Action**: Advanced | Call | Resume Call.
- **Action Data**: ISDN Exchange suspend slot number.
- **Default Label**: Resum.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Request Coaching Intrusion

This feature allows a user to request that another user intrude on a call and talk to them without being heard by the other call parties to which they can still talk.

- Intrusion features are controlled by the **Can Intrude** setting of the user intruding and the **Cannot Be Intruded** setting of user being intruded on. By default, no users can intrude and all users cannot be intruded.
- Intrusion features uses system conference resources during the call. If insufficient conference resource are available, the feature cannot be used.

Warning:

- Listening to a call without the other parties being aware is subject to local regulations. You must ensure that you have complied with the local regulations. Failure to do so can result in penalties.
-

The system support a range of other call intrusion methods in addition to this feature. The Request Coaching Intrusion feature exhibits the following behavior:

- A coaching request can be sent to a user or a group.
- While the request is pending, the user can cancel the request by pressing the **Request Coach** button again.
- Once a coaching session is established, the user that initiated the request can include the coach in the call, transfer the call to the coach, or drop the coach from the call.
- Once a coaching session is established, the coach can join the call or steal the call. The coach cannot transfer or conference the call.
- Once the primary call ends, the coaching call continues.

Details

Details

- **Action:** Advanced | Call | Request Coaching Intrusion.
- **Action Data**: None.
- **Default Label**: Request Coach or Request Coaching Intrusion.
- **Toggles:** Yes.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.

Retrieve Call

Retrieves a call previously held to a specific ISDN exchange slot. Only available when supported by the ISDN exchange.

Details

- **Action**: Advanced | Call | Retrieve Call.
- **Action Data**: Exchange hold slot number.
- **Default Label**: Retriv.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Ring Back When Free

Sets a ringback on the extension being called. When the target extension ends its current call, the ringback users is rung (for their set No Answer Time) and if they answer, a new call is made to the target extension.

Ringback can be cleared using the Cancel Ring Back When Free function.

Details

- **Action**: Advanced | Miscellaneous | Ring Back When Free.
- **Action Data**: None.
- **Default Label**: AutCB or Auto Callback.
- **Toggles**: No.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.

- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
    1. The button is equivalent to **Feature 2**.
  - This button action is also supported by the Vantage Connect Expansion application.

Ringer Off

Switches the phone's call alerting ring on/off.

Details

- **Action**: Emulation | Ringer Off.
- **Action Data**: None.
- **Default Label**: RngOf or Ringer Off.
- **Toggles**: Yes.
- **Status Indication**: Yes Required.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: Yes.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Self-Administer

Allows a user to program features against other programmable buttons themselves.

Appearance can no longer be used to create call appearance buttons. Similarly, existing call appearance button cannot be overwritten using any of the other Admin button functions.

User's with a log in code will be prompted to enter that code when they use this button action.

On 4412D+, 4424D+, 6408D, 6416D, 6424D phones:

- **Admin** can be permanently accessed via **Menu** , , , Admin. See Using a Menu Key.
- **Admin1** can be permanently accessed via **Menu** , Menu , , **ProgA**, , , **DSS**.

Details

- **Action**: Emulation | Self-Administer.
- **Action Data**: See below.

Value	T-Series and M-Series phones	Other Phones
None	The **Feature *3** process is started with an alternate set of possible functions.	If no value is set, the button allows user programming of the following emulation actions: - **Abbreviated Dial**, **Abbreviated Dial Program**, **Account Code Entry**, **AD Suppress**, **Automatic Callback**, **Break Out**, **Call Forwarding All**, **Call Park**, **Call Park and Page**, **Call Park To Other Extension**, **Call Pickup**, **Call Pickup Any**, **Conference Meet Me**, **Dial Paging**, **Directed Call Pickup**, **Directory**, **Drop**, **Group Paging**, **Headset Toggle**, **Hook Flash**, **Internal Auto-Answer**, **Ringer Off**, **Self-Administer**, **Send All Calls**, **Set Absent Text**, **Set Hunt Group Night Service**, **Time of Day**, **Timer**, **Twinning**.
1	The **Feature *1** process is started for assigning **Abbreviated Dial** button.	If **1** is entered as the telephone number, allows user programming of the following system functions. - **Abbreviated Dial**, **Group**, **CPark**, **User**, **Flash Hook**.
2	The **Feature *6** process is started for setting the ring type.	If **2** is entered, the button can be used for viewing details of the control unit type and its software version. This option is available. If the user has a log in code set, they will be prompted to enter that code. System phone users (see System Phone Features on page 846) can also use the button to manually set the system's date and time.
3	The option **3** is used with M-Series and T-Series sets to enable display contrast control.	Not used.

- **Default Label**: Admin or Self Administer.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: Yes.

- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Send All Calls

Sets the user's extension into 'Do Not Disturb' mode. Callers, other than those on the user's do not disturb exception list, receive busy or are diverted to the users voicemail mailbox. Note that with a call already connected and other calls already alerting, enabling Do Not Disturb will not affect those calls already existing. For full details of see Do Not Disturb.

When on, most phones display an **N** on the display. This function and the Do Not Disturb On function work in parallel, ie. setting one sets the other.

Details

- **Action**: Emulation | Send All Call.
- **Action Data**: None.
- **Default Label**: SAC or Send All Calls.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: Yes.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Set Absent Text

This feature can be used to select the user's current absence text. This text is then displayed to internal callers who have suitable display phones or applications. It doesn't changes the users

status. The absence text message is limited to 128 characters. Note however that the amount displayed will depend on the caller's device or application.

The text is displayed to callers even if the user has forwarded their calls or is using follow me. Absence text is supported across a multi-site network.

The user still has to select **Set** or **Clear** on their phone to display or hide the text.

Details

- **Action:** Advanced | Set | Set Absent Text.
- **Action Data**: Optional. On certain phones, if the button is set without any Action Data, the user is prompted to select their absence text and switch it on/off through a menu shown on the phone display.

  The telephone number should take the format "**y,n,text**" where:

  - **y** = 0 or 1 to turn this feature off or on respectively.
  - **n** = the number of the absent statement to use:

0 = None.	4 = Meeting until.	8 = With cust. til.
1 = On vacation until.	5 = Please call.	9 = Back soon.
2 = Will be back.	6 = Don't disturb until.	10 = Back tomorrow.
3 = At lunch until.	7 = With visitors until.	11 = Custom.

  text = any text to follow the absent statement..
- **Default Label**: Absnt or Absence Text.
- **Toggles:** No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Set Account Code

Dials an account code and then returns dial tone for the user to dial a number. Can also be used to enter an account code after a call has been connected.

Details

- **Action**: Advanced | Set | Set Account Code..
- **Action Data**: Account code or blank. If blank, the user is prompted to dial an account code after pressing the button. This option is not supported on XX02 phone modules.

- **Default Label**: Acct or Account Code.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Set Hunt Group Night Service

Puts the specified hunt group into Night Service mode. Calls to a group set to night service, receive busy or are diverted to voicemail if available or are diverted to the group's night service fallback group if set.

Setting and clearing hunt group night service can be done using either manual controls or using a system time profile. The use of both methods to control the night service status of a particular hunt group is not supported.

This function is not supported between systems in a multi-site network. It can only be used by a user currently logged onto the same system as hosting the hunt group.

Details

- **Action**: Advanced | Set | Set Hunt Group Night Service.
- **Action Data**: Hunt group extension number.
  - If left blank, the button will affect all hunt groups of which the user is a member.
  - The **Set Hunt Group Night Service** and **Clear Hunt Group Night Service** short code and button features can be used to switch an SSL VPN service off or on respectively. The service is indicated by setting the service name as the telephone number or action data. Do not use quotation marks.
- **Default Label**: HGNS+ or HG Night Service.
- **Toggles**: Yes.
- **Status Indication**: Required. If the button is blank (no specific hunt group) it will indicate on if any one of the hunt groups of which the user is a member is set to night service. If the button is set for multiple hunt groups it will indicate on if any one of those groups is set to night service.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Set Hunt Group Out Of Service

Puts the specified hunt group into Out of Service mode. Calls to a group set to out of service receive busy or are diverted to voicemail if available or are diverted to the group's out of service fallback group if set.

This function can be used to used to override hunt groups already set to night service mode by an associated time profile.

Details

- **Action**: Advanced | Set | Set Hunt Group Out of Service.
- **Action Data**: Hunt group extension number. If left blank, the button will affect all hunt groups of which the user is a member.
- **Default Label**: HGOS+ or HG Out of Service.
- **Toggles**: Yes.
- **Status Indication**: Required. If the button is blank (no specific hunt group) it will indicate on if any one of the hunt groups of which the user is a member is set out of service. If the button is set for multiple hunt groups it will indicate on if any one of those groups is set out of service.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Set Inside Call Seq

This feature allows the user to select the ringing used on their analog extension for internal calls.

Details

- **Action**: Advanced | Set | Set Inside Call Seq.
- **Action Data**: 0 to 10.
  - The number sets to the required ring pattern. See Ring Tones on page 775.
  - The numbering starts at 0 for Default Ring, 1 for Ring Normal, 2 for RingType1, and so on.
- **Default Label**: ICSeq.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.

Set Night Service Destination

This button allows the user to change the Night Service target of a hunt group. The button user does not have to be a member of the hunt group. In a multi-site network this function can be used for hunt groups on remote systems.

Changing the destination does not affect calls already ringing at the hunt groups previous night service destination.

Details

- **Action**: Advanced | Set | Set Night Service Group.
- **Action Data**: Hunt group extension number. This is the group for which the night service destination is being set.
- **Default Label**: SetNSG or HG NS Group.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Set No Answer Time

Allows the user to change their no answer time setting. This is the time calls ring before going to voicemail or following the user's divert on no answer setting if set on.

In situations where call coverage is also being used, the user's no answer time must be greater than their individual coverage time for coverage to occur.

Details

- **Action**: Advanced | Set | Set No Answer Time.
- **Action Data**: Time in seconds.
- **Default Label**: NATim or No Answer Time.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Set Out of Service Destination

This button allows the user to change the Out of Service target of a hunt group. The button user does not have to be a member of the hunt group. In a multi-site network this function can be used for hunt groups on remote systems.

Changing the destination does not affect calls already ringing at the hunt groups previous Out of Service destination.

Details

- **Action**: Advanced | Set | Set Out of Service Group.
- **Action Data**: Hunt group extension number. This is the group for which the night service destination is being set.
- **Default Label**: SetOOSG or HG OS Group.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.

- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Set Outside Call Seq

This feature allows the user to select the ringing used on their analog extension for external calls.

Details

- **Action**: Advanced | Set | Set Outside Call Seq.
- **Action Data**: 0 to 10.
  - The number sets to the required ring pattern. See Ring Tones on page 775.
  - The numbering starts at 0 for Default Ring, 1 for Ring Normal, 2 for RingType1, and so on.
- **Default Label**: OCSeq.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.

Set Ringback Seq

This feature allows the user to select the ringing used on their analog extension for ringback calls.

Details

- **Action**: Advanced | Set | Set Ringback Seq.
- **Action Data**: 0 to 10.
  - The number sets to the required ring pattern. See Ring Tones on page 775.
  - The numbering starts at 0 for Default Ring, 1 for Ring Normal, 2 for RingType1, and so on.
- **Default Label**: RBSeq.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.

Set Wrap Up Time

Allows users to change their Wrap-up Time (User | Telephony | Call Settings) setting. Other phones or applications monitoring the user's status will indicate the user as still being busy (on a call). Hunt group calls will not be presented to the user.

If the user is using a single line set, direct calls also receive busy treatment. If the user is using a mutli-line set (multiple call appearances), direct calls to them will ring as normal.

It is recommended that this option is not set to less than the default of 2 seconds. 0 is used to allow immediate ringing.

Details

- **Action**: Advanced | Set | Set Wrap Up Time.
- **Action Data**: Time in seconds. Range 0 to 99999 seconds.
- **Default Label**: WUTim or Wrap-up Time.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Speed Dial

When pressed, the button invokes the same process as dialing **Feature 0**.

- If **Feature 0** is followed by a 3-digit index number in the range 000 to 999, the system directory entry with the matching index number is dialed.
- If **Feature 0** is followed by ***** and a 2-digit index number in the range 00 to 99, the personal directory entry with the matching index number is dialed. Note: Release 10.0 allows users to have up to 250 personal directory entries. However, only 100 of those can be assigned index numbers.

Details

- **Action**: Advanced | Dial | Speed Dial.
- **Action Data**: None.
- **Default Label**: SpdDial.
- **Toggles**: No.

- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support**
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Stamp Log

The stamp log function is used to insert a line into any System Monitor trace that is running. The line in the trace indicates the date, time, user name and extension plus additional information. The line is prefixed with **LSTMP: Log Stamped** and a log stamp number. When invoked from a Avaya phone with a display, **Log Stamped#** is also briefly displayed on the phone. This allows users to indicate when they have experienced a particular problem that the system maintainer want them to report and allows the maintainer to more easily locate the relevant section in the monitor trace.

The log stamp number is set to 000 when the system is restarted. The number is then incremented after each time the function is used in a cycle between 000 and 999. Alternately if required, a specific stamp number can be assigned to the button or short code being used for the feature.

Details

- **Action**: Advanced | Miscellaneous | Stamp Log.
- **Action Data**: Optional. Blank or any 3 digit number.
- **Default Label**: Stamp Log.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
    1. Not supported on T7000, T7100, M7100 and M7100N telephones.
  - 1100 Series and 1200 Series.

Stored Number View

Supported for CTI emulation only.

Allows a user to view the contents of any programmed feature button.

Details

- **Action**: Emulation | Stored Number View.
- **Action Data**: None.
- **Default Label**: BtnVu.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Suspend Call

Uses the Q.931 Suspend facility. Suspends the incoming call at the ISDN exchange, freeing up the ISDN B channel. The call is placed in exchange slot 0 if a slot number is not specified. Only available when supported by the ISDN exchange.

Details

- **Action**: Advanced | Suspend | Suspend.
- **Action Data**: Exchange slot number or blank (slot 0).
- **Default Label**: Suspe.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Suspend CW

Uses the Q.931 Suspend facility. Suspends the incoming call at the ISDN exchange and answer the call waiting. The call is placed in exchange slot 0 if a slot number is not specified. Only available when supported by the ISDN exchange.

Details

- **Action**: Advanced | Suspend | Suspend CW.
- **Action Data**: Exchange slot number or blank (slot 0).
- **Default Label**: SusCW.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Swap CLID Name/Number

Allows the user to toggle between Caller Name and Caller ID.

Details

- **Action**: Emulation | Swap CLID Name/Number
- **Action Data**: None.
- **Default Label**:
- **Toggles**: Yes.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - M-Series and T-Series.

Time of Day

Displays the time and date on the user's telephone. This function is ignored on those Avaya phones that display the date/time by default.

Details

- **Action**: Emulation | Time of Day.
- **Action Data**: None.
- **Default Label**: TmDay.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

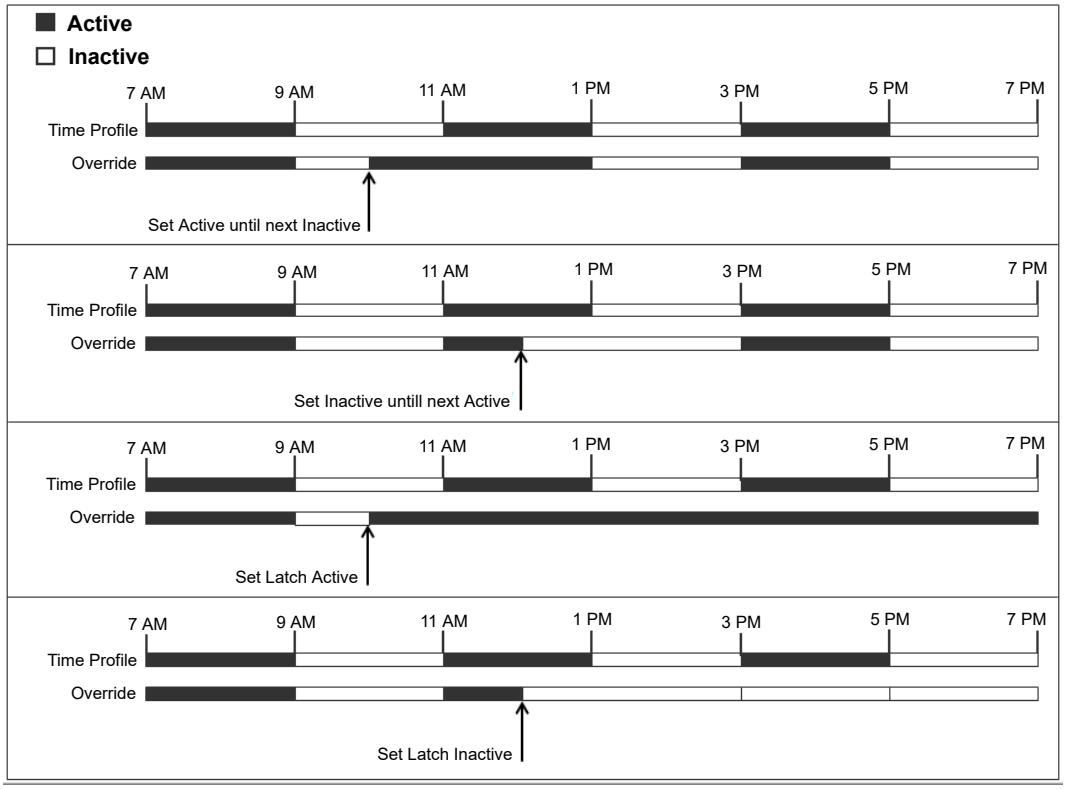
- **User Admin**: Yes.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Time Profile

You can manually override a time profile. The override settings allow you to mix timed and manual settings.

The button indicator will show the Time Profile state and pressing the button will present a menu with five options and an indication of the current state. The menu options are listed below.

Menu Option	Description
Timed Operation	No override. The time profile operates as configured.
Active Until Next Timed Inactive	Use for time profiles with multiple intervals. Select to make the current timed interval active until the next inactive interval.
Inactive Until Next Timed Active	Use for time profiles with multiple intervals. Select to make the current active timed interval inactive until the next active interval.
Latch Active	Set the time profile to active. Timed inactive periods are overridden and remain active.
Latch Inactive	Set the time profile to inactive. Timed active periods are overridden and remain inactive.



Details

- **Action**: Emulation | Time Profile
- **Action Data**: Time profile name.
- **Default Label**: TP or Time Profile
- **Toggles**: No.
- **Status Indication**:

Status	1400, 1600,	9608, 9611, J100	9621, 9641
On	**Green**	**Green On**	**Green**
Off	**Off**	**Off**	Grey

- **User Admin**: No
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.

Timer

Starts a timer running on the display of the user's extension. The timer disappears when the user ends a call.

This function can be used on Avaya phones (except 9600 Series) that display a call timer next to each call appearance. The button will temporarily turn the call timer on or off for the currently selected call appearance. The change only applies for the duration of the current call.

- **Action**: Emulation | Timer.
- **Action Data**: None.
- **Default Label**: Timer.
- **Toggles**: Yes.
- **Status Indication**: No.

Details

- **User Admin**: Yes.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Transfer

This function is intend for use with Avaya M-Series and T-Series phones only. When pressed, the button invokes the same transfer process as dialing **Feature 70**.

Details

- **Action**: Advanced | Call | Transfer.
- **Action Data**: None.
- **Default Label**: Xfer.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin:** No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.

Toggle Calls

Cycle between the user's current call and any held calls.

Details

- **Action**: Advanced | Call | Toggle Calls..
- **Action Data**: None.
- **Default Label**: Toggl.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Twinning

This action can be used by user's setup for mobile twinning. This action is not used for internal twinning.

While the phone is idle, the button allows the user to set and change the destination for their twinned calls. It can also be used to switch mobile twinning on/off and indicates the status of that setting.

When a call has been routed by the system to the user's twinned destination, the **Twinning** button can be used to retrieve the call at the user's primary extension.

In configurations where the call arrives over an IP trunk and the outbound call is on an IP trunk, multi-site network may optimise the routing and in this case the button may not be usable to retrieve the call.

Mobile Twinning Handover When on a call on the primary extension, pressing the **Twinning** button will make an unassisted transfer to the twinning destination. This feature can be used even if the user's **Mobile Twinning** setting was not enabled.

During the transfer process the button will wink. Pressing the twinning button again will halt the transfer attempt and reconnect the call at the primary extension.

The transfer may return if it cannot connect to the twinning destination or is unanswered within the user's configured **Transfer Return Time** (if the user has no **Transfer Return Time** configured, a enforced time of 15 seconds is used).

Details

- **Action**: Emulation | Twinning.

- **Action Data**: None.
- **Default Label**: Twinning.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	M-Series, T-Series
- On.	**Green on**	**Green on**	**Green**	On
- Off.	Off	Off	Grey	Off
- Twinned call at secondary	**Red on**	**Red on**	Blue	On

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.
  - This button action is also supported by the Vantage Connect Expansion application.

Unpark Call

This function is obsolete, since the Call Park function can be used to both park and retrieve calls and provides visual indication of when calls are parked. Retrieve a parked call from a specified system park slot.

Details

- **Action**: Advanced | Call | Unpark Call.
- **Action Data**: System park slot number. This must match a park slot ID used to park the call.
- **Default Label**: UnPark.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

User

Monitors whether another user's phone is idle or in use. The **Telephone Number** field should contain the users name enclosed in double quotes. The button can be used to make calls to the user or pickup their longest waiting call when ringing. On buttons with a text label, the user name is shown.

The actions performed when the button is pressed will depend on the state of the target user and the type of phone being used. It also depend on whether the user is local or on a remote multi-site network system.

Phone	Large display 1400, 1600, 9500, 9600, M-Series and T-Series Phones	Other Phones or across a multi-site network
Idle	Call the user. Whilst ringing the phone displays options to **Callback** (set an automatic callback) and **Drop** (end the call attempt).	
Ringing	• **Call Pickup:** Pickup the ringing call. • **Call**: Make a call to the user.	Picks up the call.
On a Call	The following options are displayed (name lengths may vary depending on the phone display): • **Call:** Make a call to the user. • **Message:** Cause a single burst of ringing on the target phone. On some phones, when they end their current call their phone will then display PLEASE CALL and your extension number. • **Voicemail:** Call the user's voicemail mailbox. • **Callback:** Set an automatic callback. • **Drop** Disconnect the user's current call. • **Acquire:** Shown if able to intrude on the user. Take control of the call. • **Intrude:** Shown if able to intrude on the user. Intrude into the call, turning it into a 3-way conference. • **Listen:** Shown if configured to be able to listen to (monitor) the user. Start silent monitoring of the user's call.	**Call**, **Voicemail** and **Callback** options are supported.

A User button can be used in conjunction with other buttons to indicate the target user when those buttons have been configured with no pre-set user target. In cases where the other button uses the phone display for target selection this is only possible using **User** buttons on an associate button module.

The following changes have been made to the indication of user status via BLF (busy lamp field) indicators such as a User button:

The status shown for a logged out user without mobile twinning will depend on whether they have **Forward Unconditional** enabled.

- If they have **Forward Unconditional** enabled the user is shown as idle.
- If they do not have **Forward Unconditional** enabled they will show as if on DND.

The status shown for a logged out user with mobile twinning will be as follows:

- If there are any calls alerting or in progress through the system to the twinned destination, the user status is shown as alerting or in-use as appropriate. This includes the user showing as busy/in-use if they have such a call on hold and they have **Busy on Held** enabled.
- If the user enables DND through Mobile Call Control or one-X Mobile client, their status will show as DND.
- Calls from the system direct to the user's twinned destination number rather than redirected by twinning will not change the user's status.

Details

- **Action**: User.
- **Action Data**: User name enclosed in "double-quotes".
- **Default Label**: <the user name>.
- **Toggles**: No.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series, M-Series
- Idle.	Off	Off	Grey	Off
- Alerting.	Red flash	Red flash	Blue	Slow flash
- In Use/Busy.	Red wink	Red wink	Blue	Fast flash
- DND	**Red on**	**Red on**	**Green**	On

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Visual Voice

This action provides the user with a menu for access to voicemail mailboxes. The menu provides the user with options for listening to messages, leaving messages and managing the mailbox. If

no action data is specified, then it is the user's mailbox. Action Data can be used to specify the mailbox of another user or group.

Note:

You can also use the “H” and “U” user source numbers to add another mailbox to your Visual Voice menu. See **Call Management** > **Users** > **Add/Edit Users** > **Source Numbers**

If the Action Data has been configured, pressing the button for an incoming call or while a call is connected sends the call to the user mailbox specified in the action data. If no Action Data is configured, the user is prompted to enter a mailbox.

On phones that have a display but do not support full visual voice operation as indicated below, use the button for user mailbox access using voice prompts and for direct to voicemail transfer during a call is supported.

Access to Visual Voice on supported phones can be triggered by the phone's **MESSAGES** button rather than requiring a separate Visual Voice programmable button. This is done using the option **System Settings** > **System** > **Voicemail** > **Messages button goes to Visual Voice**.

Details

- **Action**: Emulation | Visual Voice.
- **Action Data**: All local users and groups and all users and groups on systems in the network, except for the user on which the button is being programmed.
- **Default Label**: Voice.
- **Toggles**: No.
- **Status Indication**: When action data is configured, the status lamp provides a message waiting indicator for the monitored mailbox.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.

1. Takes the user direct to the listen part of Visual Voice. For the full Visual Voice menu options, the user should use **Menu | Settings | Voicemail Settings**.

Visual Voice Controls

The arrangement of options on the screen will vary depending on the phone type and display size.

Option	Description
Listen	Access your own voicemail mailbox. When pressed the screen will show the number of **New**, **Old** and **Saved** messages. Select one of those options to start playback of messages in that category. Use the ▲ up arrow and ▼ arrow keys to move through the message. Use the options below.
Listen	Play the message.

Table continues…

Option	Description
Pause	Pause the message playback.
Delete	Delete the message.
Save	Mark the message as a saved message.
Call	Call the message sender if a caller ID is available.
Copy	Copy the message to another mailbox. When pressed a number of additional options are displayed.
Message	Record and send a voicemail message to another mailbox or mailboxes.
Greeting	Change the main greeting used for callers to your mailbox. If no greeting has been recorded then the default system mailbox greeting is used.
Mailbox Name	Record a mailbox name. This feature is only available on systems using Embedded Voicemail.
Email	This option is only shown if you have been configured with an email address for voicemail email usage in the system configuration. This control allows you to see and change the current voicemail email mode being used for new messages received by your voicemail mailbox. Use **Change** to change the selected mode. Press `Done`when the required mode is displayed. Possible modes are:
Password	Change the voicemail mailbox password. To do this requires entry of the existing password.
Voicemail	Switch voicemail coverage on/off.

Voicemail Collect

Connects to the voicemail server. The telephone number must indicate the name of the Voicemail box to be accessed, eg. "?Extn201" or "#Extn201". The ? indicates "collect Voicemail" and the # indicates "deposit Voicemail". This action is not supported by voicemail using Intuity emulation mode.

When used with Voicemail Pro, names of specific call flow start points can also be used to directly access those start points via a short code. In these cases ? is not used and # is only used if ringing is required before the start points call flow begins.

Details

- **Action**: Advanced | Voicemail | Voicemail Collect.
- **Action Data**: See above.
- **Default Label**: VMCol or VMail Collect.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.

- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
    1. For access to the users own mailbox, this button is equivalent to **Feature 65** and **Feature 981**.

Voicemail Off

Disables the user's voicemail box from answering calls that ring unanswered at the users extension. This does not disable the user's mailbox and other methods of placing messages into their mailbox.

This button function is obsolete as the Voicemail On function toggles on/off.

Details

- **Action**: Advanced | Voicemail | Voicemail Off.
- **Action Data**: None.
- **Default Label**: VMOff.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.

Voicemail On

Enables the user's voicemail mailbox to answer calls which ring unanswered or arrive when the user is busy.

Details

- **Action**: Advanced | Voicemail | Voicemail On.

- **Action Data**: None.
- **Default Label**: VMOn or VMail On.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.
  - 1100 Series and 1200 Series.
  - This button action is also supported by the Vantage Connect Expansion application.

Voicemail Ringback Off

Disables voicemail ringback to the user's extension. This button function is obsolete as the Voicemail Ringback On function toggles on/off.

Details

- **Action**: Advanced | Voicemail | Voicemail Ringback Off.
- **Action Data**: None.
- **Default Label**: VMRB-
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 1400 Series and 1600 Series.

Voicemail Ringback On

Enables voicemail ringback to the user's extension. Voicemail ringback is used to call the user when they have new voicemail messages in their own mailbox or a hunt group mailbox for which they have been configured with message waiting indication.

The ringback takes place when the user's phone returns to idle after any call is ended.

Details

- **Action**: Advanced | Voicemail | Voicemail Ringback On.
- **Action Data**: None.
- **Default Label**: VMRB+ or VMail Ringback.
- **Toggles**: Yes.
- **Status Indication**: Yes.

Status	1400, 1600, 9500	9608, 9611, J100	9621, 9641	T-Series,
On	Green on	Green on	Green	On
Off	Off	Off	Grey	Off

- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.
  - M-Series and T-Series.

Whisper Page

This feature allows you to intrude on another user and be heard by them without being able to hear the user's existing call which is not interrupted.

For example: User A is on a call with user B. When user C intrudes on user A, they can be heard by user A but not by user B who can still hear user A. Whisper page can be used to talk to a user who has enabled private call.

- Intrusion features are controlled by the **Can Intrude** setting of the user intruding and the **Cannot Be Intruded** setting of user being intruded on. By default, no users can intrude and all users cannot be intruded.

The system support a range of other call intrusion methods in addition to this feature.

Details

- **Action**: Advanced | Call | Whisper Page.
- **Action Data**: User number or name or blank for entry when pressed.

- **Default Label**: Whisp or Whisper Page.
- **Toggles**: No.
- **Status Indication**: No.
- **User Admin**: No.
- **Phone Support:** Note that support for particular phone models is also dependent on the system software level.
  - 9500 Series, 9600 Series and J100 Series.
  - 1400 Series and 1600 Series.

1. Not supported on non-IP telephones when using a headset.

Part 15: Call Appearance Buttons

Appearance Buttons

Many Avaya phones supported on system have a programmable keys or buttons (the terms 'key' and 'button' mean the same thing in this context). A wide range of actions can be assigned to those buttons, see Button Programming Actions on page 1085.

These actions can be assigned to the programmable buttons on a user's phone. Those 'appearance' buttons can then be used to answer, share, switch between and in some case make calls. This type of call handling is often called 'key and lamp mode'.

The following sections in this documentation relate to a set of button actions collectively called 'appearance' actions. These are:

Appearance Button Type	Description
Call Appearances	Call appearance buttons are used to display alerts for incoming calls directed to a user's extension number or to a hunt group of which they are a member. Call appearance buttons are also used to make outgoing calls. By having several call appearance buttons, a user is able to be alerted about several calls, select which call to answer, switch between calls and take other actions. See Call Appearance Buttons on page 1200.
Bridged Appearances	A bridged appearance button shows the state of one of another user's call appearance buttons. It can be used to answer or join calls on that user's call appearance button. It can also be used to make a call that the call appearance user can then join or retrieve from hold. See Bridged Appearance Buttons on page 1205.
Line Appearances	Call coverage allows a user to be alerted when another user has an unanswered call. See Line Appearance Buttons on page 1215.

Table continues…

Appearance Button Type	Description
Call Coverage Appearances	Line appearance buttons allow specific individual line to be used when making calls or answered when they have an incoming call. It also allows users to bridge into calls on a particular line. See Call Coverage Buttons on page 1210.

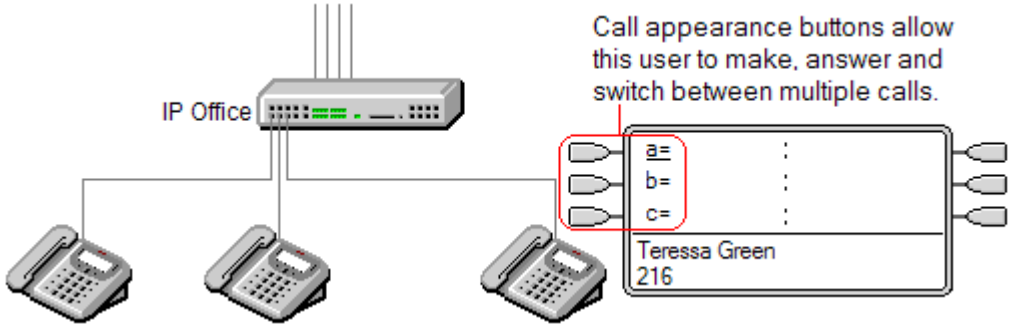
Note:

- For all the examples within this documentation, it is assumed that **Auto Hold** is on and **Answer Pre-Select** is off unless otherwise stated.
- The text shown on phone displays in the examples are typical and may vary between phone types, locales and system software releases.

Chapter 106: Call Appearance Buttons

Call appearance buttons are used to display alerts for incoming calls directed to a user's extension number or to a hunt group of which they are a member. Call appearance buttons are also used to make outgoing calls.

By having several call appearance buttons, a user is able to be alerted about several calls, select which call to answer, switch between calls and take other actions.



When all the user's call appearance buttons are in use or alerting, any further calls to their extension number receive busy treatment. Instead of busy tone, the user's forward on busy is used if enabled or otherwise voicemail if available.

Call appearance buttons are the primary feature of key and lamp operation. None of the other appearance button features can be used until a user has some call appearance button programmed[1].

There are also addition requirements to programming call appearance buttons:

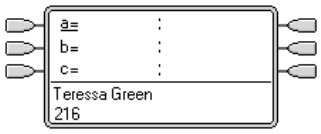
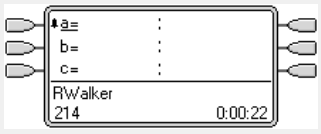
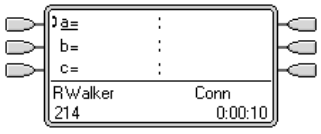
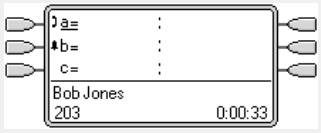
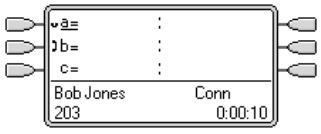
- Call appearance buttons must be the first button programmed for the user.
- Programming a single call appearance button for a user is not supported. The normal default is 3 call appearances per user except on phones where only two physical buttons are available.

Related links

Call Appearance Example 1 on page 1201
Call Appearance Example 2 on page 1201
How are Call Appearance Buttons Treated? on page 1202
Call Appearance Button Indication on page 1203

Call Appearance Example 1

In this example, the user has multiple call appearance buttons.

	**Phone Idle** The phone is currently idle.
	**First Call Alerts** A call arrives. It alerts against the first available call appearance button. Pressing that button will answer the call.
	**Call Answered** The call is now connected.
	**Second Call Alerts** A second call arrives whilst the first is still connected. It alerts against the next available call appearance button. As the user has a call in progress, the alert gives just a single ring and briefly display details of the caller.
	**Pressing the Second Call Appearance** Pressing the second call appearance button will hold the first call and answer the second.

Related links

Call Appearance Buttons on page 1200

Call Appearance Example 2

In this example, the user will use their call appearances to make two calls and start a conference between those calls.

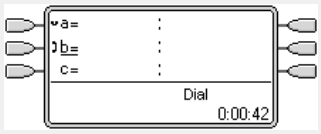
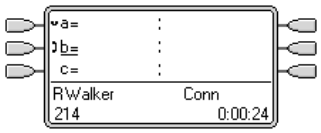
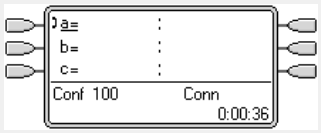
	Initial Call The user has a call in progress, shown on their first call appearance button. It is decided to conference another user into the call.
	**Make Conference Enquiry** Pressing the **CONFERENCE** button on the users phone automatically places the current call on hold and takes the phone off hook on the next available call appearance.

Table continues…

	**Enquiry in Progress** The other extension has been dialed and invited to join a conference call. The user presses the **CONFERENCE** button on their phone again.
	**Conference Starts** The conference call has started. The separate call appearances have collapsed to a single appearance that represents the conference.

Related links

Call Appearance Buttons on page 1200

How are Call Appearance Buttons Treated?

For incoming calls

- **Call Waiting** settings are ignored except for hunt group call waiting where the call waiting tone is replaced by an alert on a call appearance button if available.
- **Follow Me**, **Forward Unconditional** and **Forward Hunt Group Calls** are used when set.
- If **Do Not Disturb** is set, only calls from numbers in the user's Do Not Disturb Exception list will alert if a call appearance is available.

Busy status

In both cases below, even when busy, the user may still receive alerts on other appearance buttons.

- **For calls direct to the user's extension number** The user is busy when all their available call appearances are in use. Instead of busy tone, the user's forward on busy is used if enabled or otherwise voicemail if available.
- **For calls to a hunt group of which the user is a member** The user is busy to further hunt group calls when they have any appearance button in use on their phone. The only exception is calls to a collective hunt group with call waiting.

For outgoing calls

- Outgoing calls are treated exactly the same as calls made by non-appearance button users.
- External Calls made on a call appearance, which route out on a line for which the user also has a line appearance, will remain on the call appearance. The line appearance will indicate 'in use elsewhere'.

For call appearance buttons matched by a bridged appearance button

- If the bridged appearance is used to make or answer calls, the state of the call appearance will match that of the bridged appearance.
- If the call is put on hold by the bridged appearance user, the call appearance will show 'on hold elsewhere'.

Other

- **Held/Parked Call Timeout** If the user has parked a call, the parked call timer only starts running when the user is idle rather than on another call.
- Incoming calls routed directly to the user as the incoming call routes destination on a line for which the user also has a line appearance, will only alert on the line appearance. These calls do not follow any forwarding set but can be covered.

Related links

Call Appearance Buttons on page 1200

Call Appearance Button Indication

On phones with a text display area next to the button, by default **a=**, **b=** and so on is displayed. This can be replaced by another label if required.

When the user is not connected to a call, the button indicated as selected is the button that will be used if the user goes off hook without pressing an appearance button. When a user is connected to a call, that call is the selected button.

The following table shows how the different states of call appearance buttons (alerting, held, etc) are indicated. This is a general table, not all phone button types are covered. The ring that accompanies the visual indication can be delayed or switched off. See Ring Delay on page 1227.

Icon Button	Dual LED Button	Appearance Button State
CA1	Red off, Green off.	**Idle** The call appearance is not in use and is not currently selected.
CA1	Red on, Green off.	**Idle + Selected** The call appearance is not in use but is the current selected button that will be used if the user goes off hook.
CA1 Flashing icon.	Red off, Green steady flash.	**Alerting** The matching call appearance is alerting for an incoming call. This is accompanied by ringing. If the user is already on a call, only a single ring is given.
CA1 Flashing icon.	Red on, Green steady flash.	**Alerting + Selected** As above but **Ringing Line Preference** has made this the user's current selected button.
CA1	Red on, Green on.	**In Use Here** The user has a call connected on the call appearance or is dialing.
CA1	Red off, Green on.	**In Use Elsewhere** The call appearance button is in use on a bridged appearance.

Table continues…

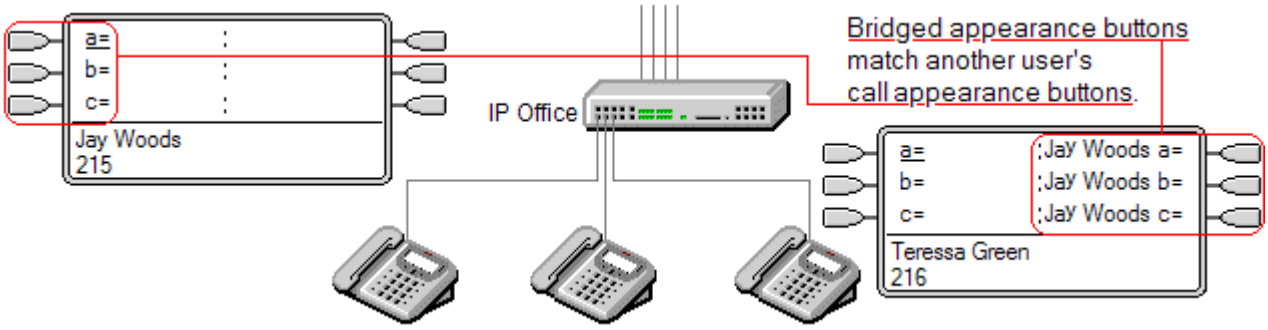
Icon Button	Dual LED Button	Appearance Button State
CA1	Red off, Green fast flash.	**On Hold Here** The call has been put on hold by this user.
CA1	Red fast flash, Green fast flash	**On Hold Pending Transfer** Applies to 1400, 1600, 9500 and 9600 Series phones.
CA1	Red off, Green intermittent flash.	**On Hold Elsewhere** A call on a bridged appearance button matched to the call appearance has been put on hold. Calls on a call appearance that are put on hold by another user will continue to show connected lamp status, though the phone display will indicate a held call.
CA1 Icon flashes off.	Red off, Green broken flash.	**Inaccessible** The button pressed is not accessible. The call is still dialing, ringing or cannot be bridged into.

Related links

Call Appearance Buttons on page 1200

Chapter 107: Bridged Appearance Buttons

A bridged appearance button shows the state of one of another user's call appearance buttons. It can be used to answer or join calls on that user's call appearance button. It can also be used to make a call that the call appearance user can then join or retrieve from hold.



When the user's call appearance button alerts, any associated bridged appearance buttons on other user's phones also alert. The bridged appearance buttons can be used to answer the call on the call appearance button user's behalf.

When the call appearance button user answers or makes a call, any associated bridged appearance buttons on other users' phones show the status of the call, ie. active, on hold, etc. The bridged appearance button can be used to retrieve the call if on hold or to join the call if active (subject to intrusion permissions).

Note Bridged appearance buttons are different from the action of bridging into a call (joining a call). See Joining Other Calls (Bridging).

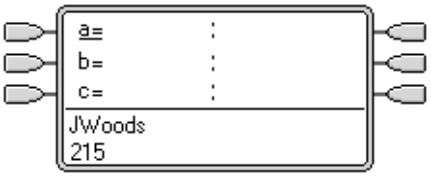
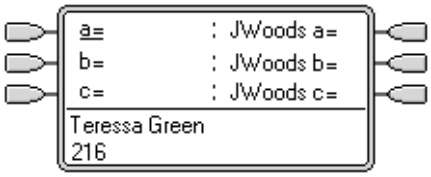
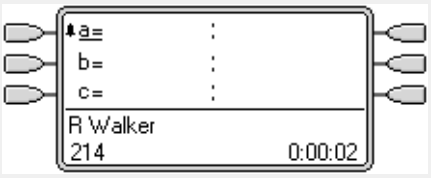
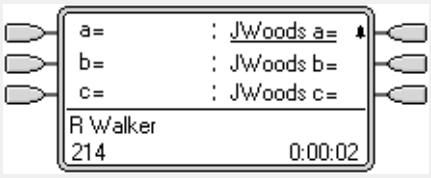
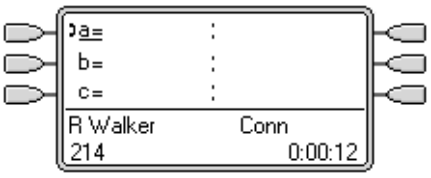
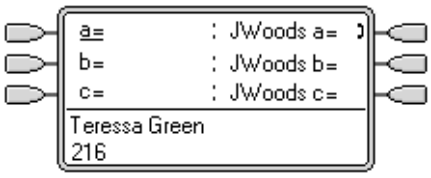
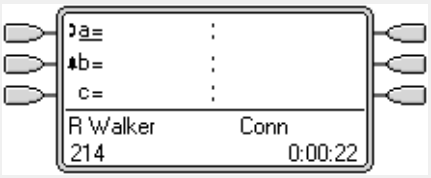
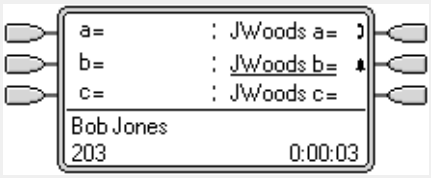
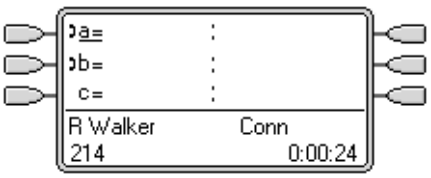
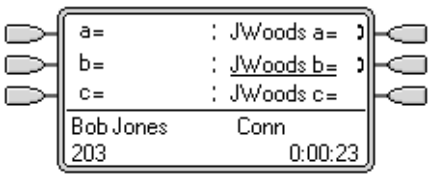
Bridged appearance buttons are not supported between users on different systems in a multi-site network.

Related links

Bridged Appearance Example 1 on page 1206
Bridged Appearance Example 2 on page 1206
Bridged Appearance Example 3 on page 1207
How are Bridged Appearances Treated? on page 1208
Bridged Appearance Button Indication on page 1209

Bridged Appearance Example 1

In this example, one user is able to see the status of the other user's call appearances, and when necessary answer calls for the other user. Both users have **Ringing Line Preference** and **Auto Hold** on.

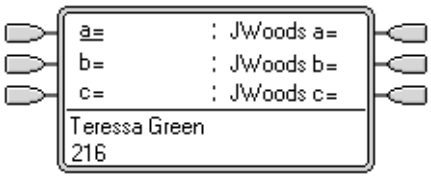
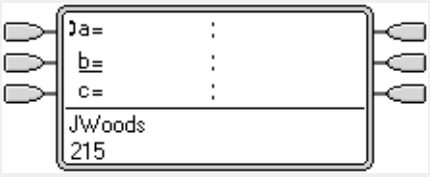
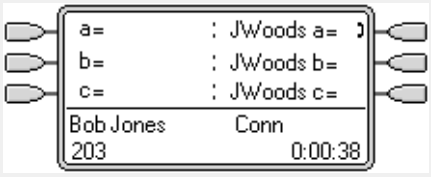
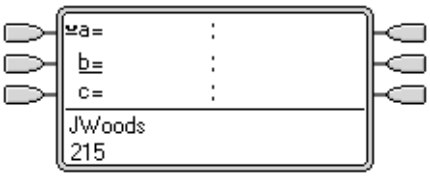
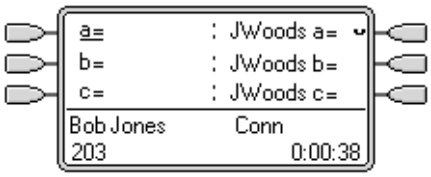
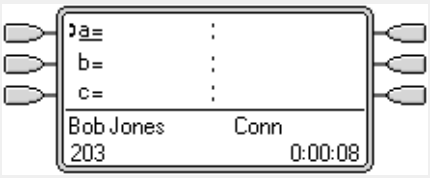
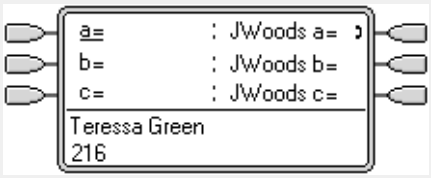
Call Appearance User	Bridged Appearance User	
		**Both Phone Idle** Our user has bridged appearance buttons that match a colleague's call appearances buttons.
		**First Call** The colleague has a call alerting on their first call appearance button. It also alerts on our user's first bridged appearance button.
		**Call Answered** The colleague has answered the call. The bridged appearance indicates 'in use elsewhere'.
		**Second Call** Another call alerts at the colleagues phone and again is mirrored on our user's second bridged call appearance button.
		**Call Answered** Our user has gone off hook and answered the incoming call alerting on the bridged call appearance.

Related links

Bridged Appearance Buttons on page 1205

Bridged Appearance Example 2

In this example, the bridged appearance user makes a call on behalf of the call appearance user. Once the call is connected, they put it on hold. The call appearance user is able to take the call off hold using their call appearance button. Both users have **Ringing Line Preference** and **Auto Hold** on.

Call Appearance User	Bridge Appearance User	
		**Both Phones Idle** Our user has bridged appearance buttons that match a colleague's call appearances buttons.
		**Bridged User Makes Call** Our user has pressed a bridged appearance and made a call on it. The matching call appearance shows 'in use elsewhere'.
		**Call Put on Hold** Having made the call, the bridged user puts it on hold. The matching call appearance indicates 'on hold elsewhere'.
		**Call Taken Off Hold** By pressing the call appearance, the first user has answered the held call. The bridged appearance user returns to idle.

Related links

[Bridged Appearance Buttons](#) on page 1205

Bridged Appearance Example 3

In this example, a call is passed from the call appearance user to the bridged appearance user. Both users have **Ringing Line Preference** and **Auto Hold** on.

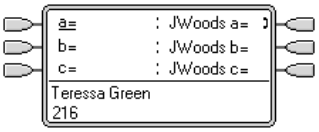
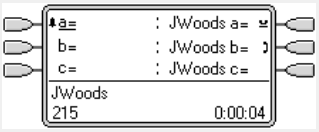
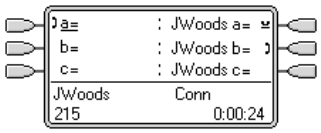
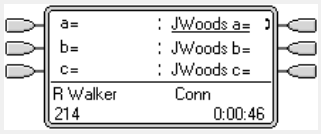
Bridged Appearance User	
	**Call on Colleague's Phone** The call appearance user has answered a call on one of their call appearances. The bridged appearance user's matching bridged appearance shows 'in use elsewhere'.
	**Call Held by Colleague** The call appearance user has put the call on hold and called the bridged appearance user. The first bridged call appearance shows a call 'on hold elsewhere' whilst the second matches the call between users.

Table continues…

	**Enquiry Call Between Colleagues** By going off hook, the bridged appearance user has answered the call from the call appearance user. They are asked to pickup the call on the colleagues first call appearance.
	**Call Taken Off Hold** Pressing the first bridged appearance button takes that call off hold and connects it to the bridged appearance user. In this example, **Auto Hold** is not set for the system, so pressing the bridged appearance button disconnected the call from the colleague. If **Auto Hold** had been set, the colleague's call would have been put on hold until they hung up.

Related links

Bridged Appearance Buttons on page 1205

How are Bridged Appearances Treated?

Bridged appearance buttons operate in parallel with their matching call appearance button.

- **Whose user settings control the call?** Until answered on a bridged appearance button, calls alerting on a bridged appearance button follow the settings of the user or hunt group to which the call was originally directed.
- If the call appearance is in use, any matching bridged appearance will indicate the same.
- If a bridged appearance is in use, the call appearance it matches will indicate the same.
- The bridge appearance will only alert if the call appearance is alerting. For example, direct intercom and paging call to the call appearance will show on the bridged appearance but will not give any audible alert.
- If the bridged appearance user put the call on hold, the call appearance indicates 'on hold elsewhere'.
- Bridged appearances to a user who has logged out, or has logged into a phone without appearance buttons will not operate.
- If the bridged appearance user has 'do not disturb' (DND) enabled, the bridge appearance button icon or lamps operates but alerting and ringing line preference selection is not applied unless the caller is in the user’s DND exception list.
- Bridged appearance buttons are not supported between users on different systems in a multi-site network.

Related links

Bridged Appearance Buttons on page 1205

Bridged Appearance Button Indication

On phones with a text display area next to the button, the name of the bridged user and the label from the bridged user's call appearance key are displayed.

The following table shows how the different states of call appearance buttons (alerting, held, etc) are indicated. This is a general table, not all phone button types are covered. The ring that accompanies the visual indication can be delayed or switched off. See Ring Delay on page 1227.

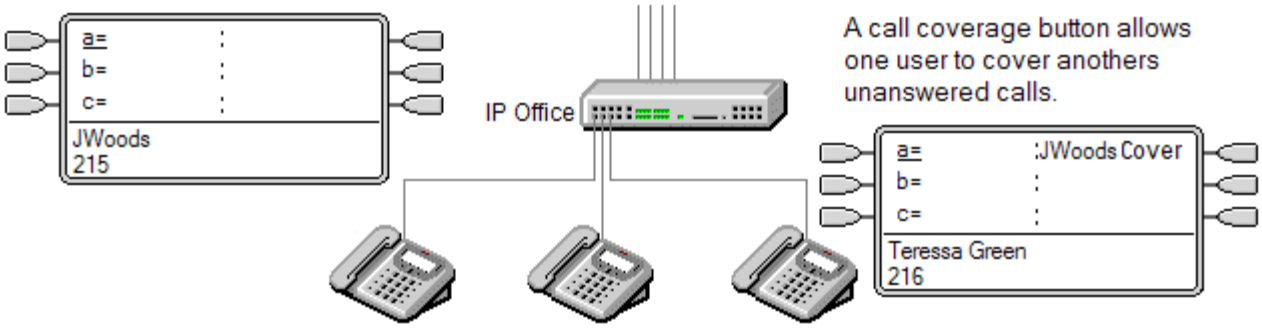
Icon Button	Dual LED Button	Appearance Button State
JWoods CA1	Red off, Green off.	**Idle** The bridged appearance is not in use.
JWoods CA1 Flashing icon.	Red off, Green steady flash.	**Alerting** The matching call appearance is alerting for an incoming call. This is accompanied by ringing. If the user is already on a call, only a single ring is given.
JWoods CA1 Flashing icon.	Red on, Green steady flash.	**Alerting + Selected** As above but **Ringing Line Preference** has made this the user's current selected button.
JWoods CA1	Red off, Green on.	**In Use Elsewhere** The matching call appearance button is in use.
JWoods CA1	Red on, Green on.	**In Use Here** The user has made a call or answered a call on the bridged appearance, or bridged into it.
JWoods CA1	Red off, Green fast flash.	**On Hold Here** The call has been put on hold by this user.
JWoods CA1	Red off, Green intermittent flash.	**On Hold Elsewhere** The call on that call appearance has been put on hold by another user.
JWoods CA1 Icon flashes off.	Red off, Green broken flash.	**Inaccessible** The button pressed is not usable. The call is still dialing, ringing or cannot be bridged into.

Related links

Bridged Appearance Buttons on page 1205

Chapter 108: Call Coverage Buttons

Call coverage allows a user to be alerted when another user has an unanswered call.



The user being covered does not necessarily have to be a key and lamp user or have any programmed appearance buttons. Their Individual Coverage Time setting (default 10 seconds) sets how long calls will alert at their extension before also alerting on call coverage buttons set to that user.

The user doing the covering must have appearance buttons including a call coverage appearance button programmed to the covered users name.

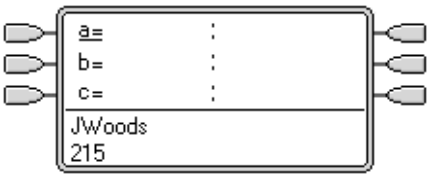
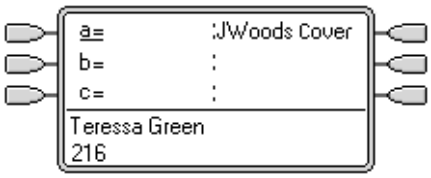
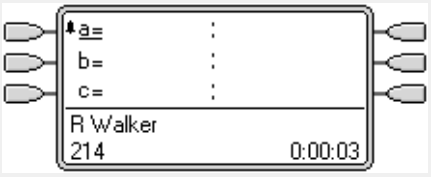
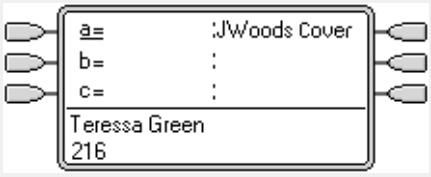
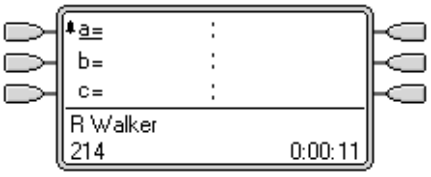
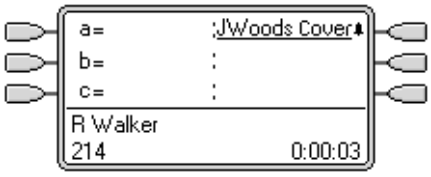
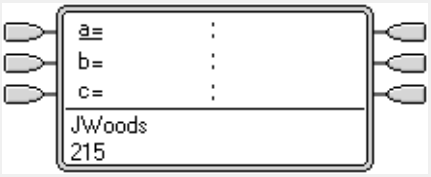
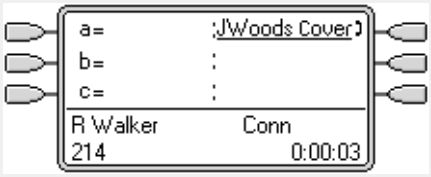
Call coverage appearance buttons are not supported between users on different systems in a multi-site network.

Related links

Call Coverage Example 1 on page 1210
Call Coverage Example 2 on page 1211
How is Call Coverage Treated? on page 1212
Call Coverage Button Indication on page 1213

Call Coverage Example 1

In this example, the covering user is able to answer their colleagues call when it rings unanswered. Both users have **Ringing Line Preference** and **Auto Hold** on.

Covered User	Covering User	Both Phones Idle
		Our user has a call coverage button to cover their colleague.
		**Call to Covered User** A call arrives for the covered user.
		**Call Alerts to Coverage** After ringing for the covered user's Individual Coverage Time, the call also begins alerting on the call coverage button .
		**Covering User Answers** By going off hook or pressing the alerting button, the covering user has answered the call.

Related links

Call Coverage Buttons on page 1210

Call Coverage Example 2

In this example, the covered user has calls on all their available call appearances. Both users have **Ringing Line Preference** and **Auto Hold** on.

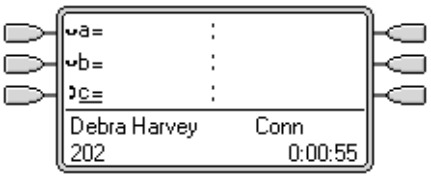
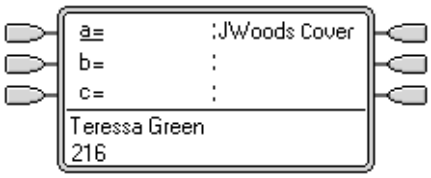
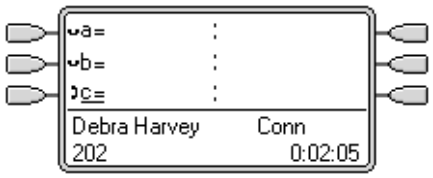
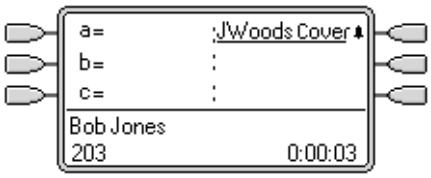
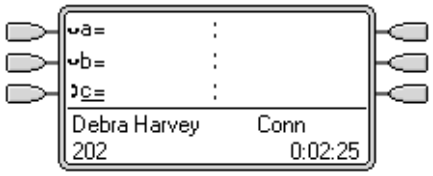
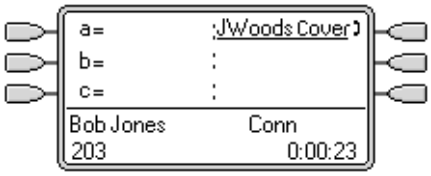
Covered User	Covering User	Calls in Progress
		The covered user already has a number of calls in progress on all their call appearance keys.

Table continues…

		**Call Alerts to Coverage** The covered user is treated as busy, so their next call goes immediately to call coverage.
		**Covering User Answers** The covering user has answered the call.

Related links

Call Coverage Buttons on page 1210

How is Call Coverage Treated?

Whose user settings control the call ?

Until answered, calls alerting on a call coverage button follow the settings of the user to which the call was originally directed.

Once answered, the call follows the user settings of the user who answered it.

Coverage is applied to :

- Internal calls dialed to the covered user's extension number.
- External calls routed to the covered user by a incoming call route.
- Calls forwarded internally by the covered user or on follow me from the covered user.

Coverage is not applied to :

- Hunt group calls to a hunt group of which the covered user is a member.
- Calls forwarded to the covered user using forward or follow me functions.
- Calls alerting on the covered user's bridged appearance and call coverage buttons.
- Coverage is only applied to calls alerting on a line appearance if the call was also routed to that user by an incoming call route.
- Page and intercom calls.
- Parked, transferred and held calls ringing back to the user.
- Automatic callback calls set by the covered user.
- Voicemail ringback calls.
- Call coverage appearance buttons are not supported between users on different systems in a multi-site network.

Coverage is applied :

- If the covered user's phone is available, call coverage is applied only after the covered user's Individual Coverage Time has expired.
- If the covered user's phone is busy, call coverage is applied immediately.
- If the covered user is using follow me or forward all to an internal number to divert their calls, call coverage is still applied.
- If the covered user has 'do not disturb' on, call coverage is applied immediately except for calls from numbers in the covered user's do not disturb exceptions list.

Other items :

If the call is not answered after the covered user's **No Answer Time** it will go to the covered user's voicemail if available or follow their forward on no answer settings.

If the covered user has several alerting calls, the call answered by the call coverage button is the covered user's longest ringing call.

Calls will not alert at a covering user who has 'do not disturb' enabled, except when the calling number is in the covering user's do not disturb exception list.

Related links

Call Coverage Buttons on page 1210

Call Coverage Button Indication

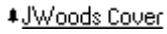
On phones with a text display area next to the button, the name of the covered user is displayed followed by the word **Cover**.

When the user is not connected to a call, the button indicated as selected is the button that will be used if the user goes off hook without pressing an appearance button. When a user is connected to a call, that call is the selected button.

The following table shows how the different states of call appearance buttons (alerting, held, etc) are indicated. This is a general table, not all phone button types are covered. The ring that accompanies the visual indication can be delayed or switched off. See Ring Delay on page 1227.

Icon Button	Dual LED Button	Appearance Button State
JWoods Cover	Red off, Green off.	**Idle** The button is not in use.
JWoods Cover Flashing icon.	Red off, Green steady flash.	**Alerting** The call coverage is alerting for an unanswered call at the covered user's phone. This is accompanied by ringing. If the user is already on a call, only a single ring is given.

Table continues…

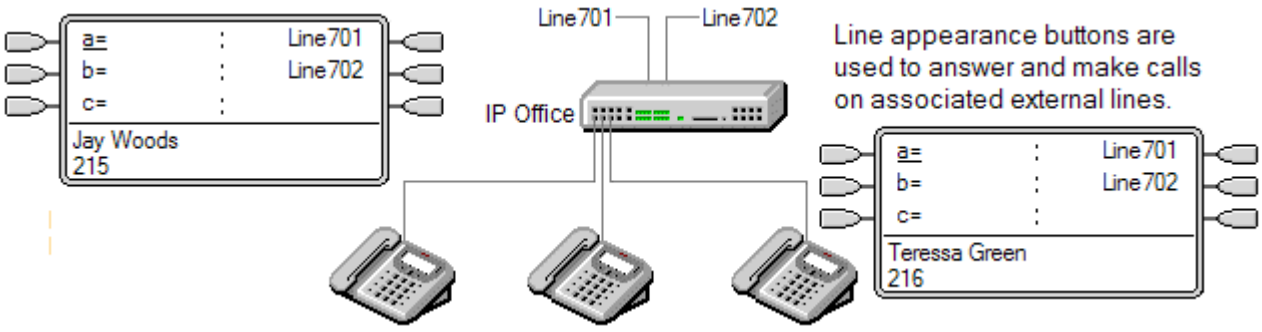
Icon Button	Dual LED Button	Appearance Button State
 Flashing icon.	Red on, Green steady flash.	**Alerting + Selected** As above but **Ringing Line Preference** has made this the user's current selected button.
	Red on, Green on.	**In Use Here** The user has answered the call requiring coverage.
	Red off, Green fast flash.	**On Hold Here** The covered call has been put on hold by the call coverage button user.

Related links

Call Coverage Buttons on page 1210

Chapter 109: Line Appearance Buttons

Line appearance buttons allow specific individual line to be used when making calls or answered when they have an incoming call. It also allows users to bridge into calls on a particular line.



Incoming call routing is still used to determine the destination of all incoming calls. Line appearance buttons allow a call on a specific line to alert the button user as well as the intended call destination. When these are one and the same, the call will only alert on the line appearance but can still receive call coverage.

When alerting on suitable phones, details of the caller and the call destination are shown during the initial alert.

Individual line appearance ID numbers to be assigned to selected lines on a system. Line appearance buttons are only supported for analog, E1 PRI, T1, T1 PRI, and BRI PSTN trunks; they are not supported for other trunks including E1R2, QSIG and IP trunks.

Line appearance buttons are not supported for lines on remote systems in a multi-site network.

Using Line Appearances for Outgoing Calls

In order to use a line appearance to make outgoing calls, changes to the normal external dialing short codes are required. For full details see Outgoing Line Programming on page 1242.

Private Lines

Special behavior is applied to calls where the user has both a line appearance for the line involved and is also the Incoming Call Route destination of that call. Such calls will alert only on the Line Appearance button and not on any other buttons. These calls will also not follow any forwarding.

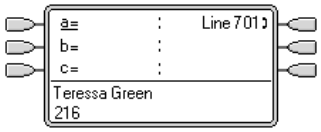
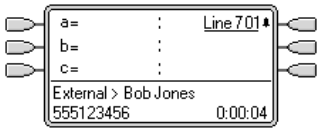
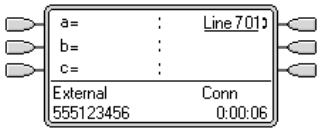
Related links

Line Appearance Example 1 on page 1216
Line Appearance Example 2 on page 1216
How are Line Appearances Treated? on page 1217

Line Appearance Button Indication on page 1218

Line Appearance Example 1

In this example, the user is able to answer a call alerting on a particular line.

	**Line Goes Active** A call is active on the line with line ID number 601. This is indicated as 'in use elsewhere'. For an incoming call, the line will show active but will not alert until call routing has been determined. On analog ICLID lines, alerting is delayed until the ICLID that might be used to do the call routing has been received.
	**Line Appearance Alerting** The routing of the call has been complete and it is ringing against its destination. On our user's phone the line appearance also alerts and ringing line preference has made it the current selected button.
	**Answer Call** By going off hook or pressing the line appearance, our user has answered the call on that line.

Related links

Line Appearance Buttons on page 1215

Line Appearance Example 2

In this example, two users exchange a call using line appearance buttons set to the same line. Note that this requires that the user who first answers the call to have **Cannot be Intruded** off. Both users have **Ringing Line Preference** and **Auto Hold** on.

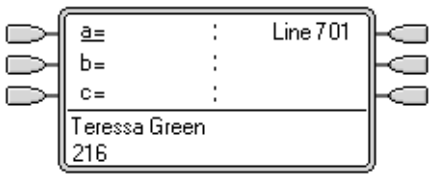
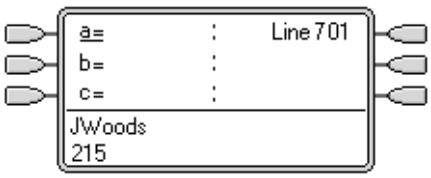
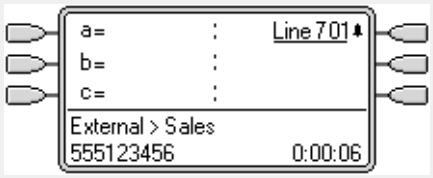
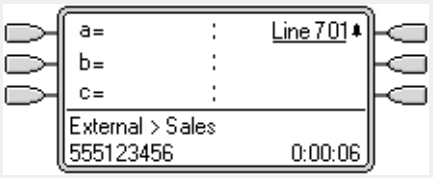
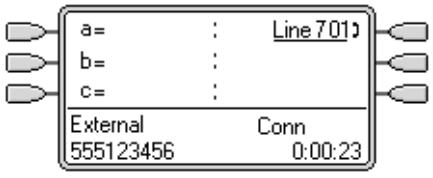
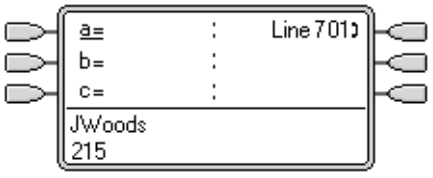
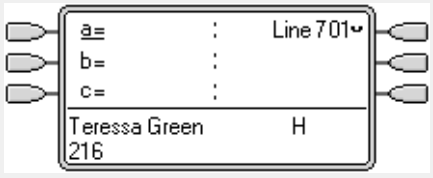
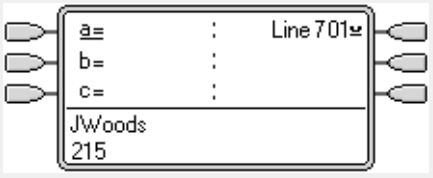
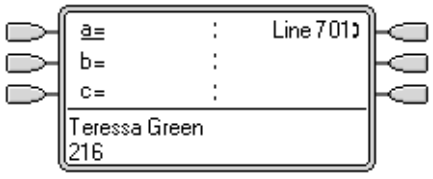
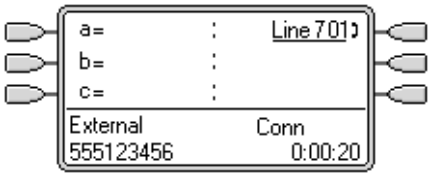
		**Idle** The two users has line appearances for the same line.

Table continues…

		**Call Alerts** A call arrives. Either user can answer it by pressing the alerting line appearance
		**Call Answered** The first user has answer the call.
		**Line Held** The first user has put the call on hold.
		**Line Retrieved** The second user has retrieved the held call by pressing the line appearance.

Related links

Line Appearance Buttons on page 1215

How are Line Appearances Treated?

Incoming Calls

- **Until answered using a line appearance button, incoming calls alerting on a line appearance, follow the settings of the incoming call route's destination group or user. They do not follow the settings of any line appearance user**.
- If an incoming calls destination is voicemail, or once the incoming call has passed from its destination to voicemail, it cannot be answered or bridged into using a line appearance button.
- If the line appearance user is also the incoming call route destination for the call, the call will alert on their line appearance only. In this case:
  - It will alert on the line appearance even if all call appearances are in use.
  - The call will not follow any of the user's forwarding settings .
  - The call will receive call coverage from other user's with call coverage buttons set to the line appearance user.
  - The ring delay used is that of the first free call appearance.

- For analog lines set to ICLID, any line appearances show active while the system waits for ICLID information. During this time the line has not been routed and cannot be answered using a line appearance button.
- Calls alerting on a line appearance can also alert on a call coverage appearance on the same phone. If Ringing Line Preference is set, the current selected button will change from the line appearance to the call coverage appearance.
- If the line appearance user has do not disturb (DND) enabled, the line appearance button icon or lamps will still operate but alerting and ringing line preference selection are not applied unless the caller is in their DND exception list.

Outgoing Calls

- In order to be used for making outgoing calls, some additional system programming may be required. See Outgoing Line Programming.
- Calls made on a call appearance, which are routed out on a line for which the user also has a line appearance, will remain on the call appearance. The line appearance will indicate 'in use elsewhere'.

Additional Notes

- Line appearance buttons are not supported for lines on remote systems in a multi-site network.
- Where a line appearance button is used to answer a call for which automatic call recording is invoked, the recording will go to the automatic recording mailbox setting of the original call destination.
- If a call indicated by a line appearance is parked, it cannot be joined or unparked by using another line appearance.
- Calls alerting on a line appearance do not receive call coverage or go to a users voicemail unless the user was the call's original incoming call route destination.

Related links

Line Appearance Buttons on page 1215

Line Appearance Button Indication

On phones with a text display area next to the button, the label **Line** and the line number are displayed.

When the user is not connected to a call, the button indicated as selected is the button that will be used if the user goes off hook without pressing an appearance button. When a user is connected to a call, that call is the selected button.

The following table shows how the different states of call appearance buttons (alerting, held, etc) are indicated. This is a general table, not all phone button types are covered. The ring that accompanies the visual indication can be delayed or switched off. See Ring Delay on page 1227.

Icon Button	Dual LED Button	Appearance Button State
Line 601	All off.	**Idle** The associated line is not in use.
Line 601	Red on. Green off.	**Idle + Selected** The associated line is not in use but the button is the user currently selected button.
Line 601 Flashing icon.	Red off Green steady flash.	**Alerting** The line is ringing at its incoming call route destination. This is accompanied by ringing. If the user is already on a call, only a single ring is given.
Line 601 Flashing icon.	Red on Green steady flash.	**Alerting + Selected** As above but **Ringing Line Preference** has made this the user's current selected button.
Line 601	Red off Green on.	**In Use Elsewhere** The line is in use.
Line 601	Red on Green on.	**In Use Here** The user has answered the line, made a call on it or bridged into the call on the line.
Line 601	Red off Green fast flash.	**On Hold Here** The call on the line has been put on hold by this user.
Line 601	Red off Green intermittent flash.	**On Hold Elsewhere** The call on the line has been put on hold by another appearance button user.
Line 601 Icon flashes off.	Red off Green broken flash.	**Inaccessible** The button pressed is not accessible. The call is still dialing, ringing, routing or cannot be bridged into.

Related links

Line Appearance Buttons on page 1215

Chapter 110: Appearance Button Features

Appearance functions are only supported on Avaya phones which have programmable buttons and also support multiple calls. Appearance functions are also only supported on those buttons that have suitable adjacent indicator lamps or a display area. Appearance buttons are not supported across a multi-site network.

Related links

Selected Button Indication on page 1220
Idle Line Preference on page 1221
Ringing Line Preference on page 1223
Answer Pre-Select on page 1225
Auto Hold on page 1226
Ring Delay on page 1227
Delayed Ring Preference on page 1228
Collapsing Appearances on page 1230
Joining Calls on page 1231
Multiple Alerting Appearance Buttons on page 1233
Twinning on page 1234
Busy on Held on page 1234
Reserving a Call Appearance Button on page 1235
Logging Off and Hot Desking on page 1235
Applications on page 1236

Selected Button Indication

During appearance button usage, one of the user's appearance buttons may be indicated as the user's current selected button. This is the appearance button already in use, or if idle, the appearance button that will be used if the user goes off hook by lifting the handset.

On phones with a display area next to each button, the current selected button is indicated by either an _ underscore of the button label, or a shaded background. On phones with twin LED lamps, the current selected button is indicated by the red lamp being on.

The system sets which appearance button is the current selected button using the following methods:

Method	Description
Idle Line Preference	This feature can be set on or off for each individual user, the default is on. When on, it sets the current selected button as the first available idle call/line appearance button. See Idle Line Preference on page 1221.
Ringing Line Preference	This feature can be set on or off for each individual user, the default is on. When on, it sets the current selected button as the button which has been alerting at the user's phone for the longest. **Ringing Line Preference** overrides **Idle Line Preference**. See Ringing Line Preference on page 1223.
Delayed Ring Preference	This setting is used in conjunction with ringing line preference and appearance buttons set to delayed or no ring. It sets whether ringing line preference should observe or ignore the delayed ring applied to the user's appearance buttons when determining which button should have current selected button status.
User Selection	The phone user can override both **Idle Line Preference** and **Ringing Line Preference** by pressing the appearance button they want to use or answer. That button will then remain the current selected button whilst active. If the user currently has a call connected, pressing another appearance button either holds or disconnect that call. The action is determined by the system's **Auto Hold** setting.

Answer Pre-Select

Normally when a user has multiple alerting calls, only the details of the call on current selected button are shown. Pressing any of the alerting buttons will answer the call on that button, going off-hook will answer the current selected button.

Enabling the user telephony setting **Answer Pre-Select** allows the user to press any alerting button to make it the current selected button and displaying its call details without answering that call. To answer a call when the user has **Answer Pre-Select** enabled, the user must press the alerting button to display the call details and then either press the button again or go off-hook.

Related links

Appearance Button Features on page 1220

Idle Line Preference

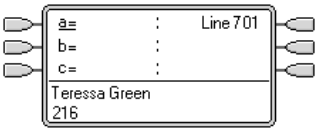
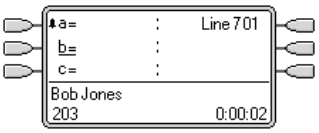
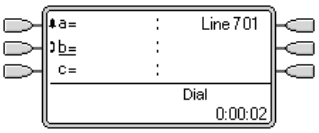
Idle Line Preference determines the user's currently selected button as the first available idle call/line appearance button. Selected button indication is applied to that button and if the user goes off-hook, for example by lifting their handset, an outgoing call is started on that button.

- **?Why Would I Use Just Idle Line Preference** In environments that are focused on making outgoing calls, for example telemarketing, incoming calls are infrequent and user's go off-hook expecting to make a call. Using **Idle Line Preference** without **Ringing Line Preference** ensures that the user doesn't inadvertently answer a call when expecting to make a call.
- If all the available call/line appearance buttons are in use, no current selected button choice is made by **Idle Line Preference**. In this case, going off hook will have no effect.

- For appearance button users with **Idle Line Preference** off, going off-hook (lifting the handset or pressing **SPEAKER**, **HEADSET**, etc) will have no effect until an appearance button is pressed.
- By default **Idle Line Preference** is on for all users.
- **Idle Line Preference** is overridden by **Ringing Line Preference** if also on for the user.

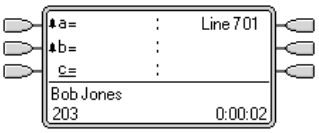
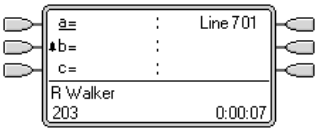
Idle Line Preference Example 1

In this example, only **Idle Line Preference** has been programmed for the user. **Ringing Line Preference** has not been programmed.

	**Phone Idle** The phone is idle. The current selected button determined by Idle Line Preference is the first available idle call appearance button. This is shown by the _ underscore of the button text.
	**First Call to User** A call for the user arrives. It alerts on the first available call appearance button. Idle Line Preference has changed the current selected button to the next available idle call appearance.
	**User Goes Off Hook** 1. With the call still alerting, if the user goes off hook, it will be interpreted as making a call using the currently selected button, not as answering the alerting button. 2. To answer the alerting call, the user should press the alerting button.

Idle Line Preference Example 2

In this example, only **Idle Line Preference** has been programmed for the user. **Ringing Line Preference** has not been not programmed.

	**Two Calls Alerting** The users has two incoming calls alerting. Idle Line Preference has set the currently selected button to their third call appearance.
	**First Caller Abandons** If the first incoming caller disconnects, the currently selected button changes to the first call appearance as this is now the first available idle call appearance button.

Idle Line Preference Example 3

In this example, both **Idle Line Preference** and **Ringing Line Preference** are set for the user.

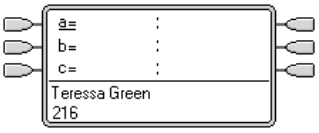
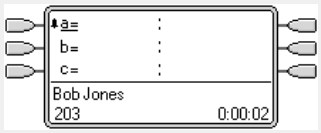
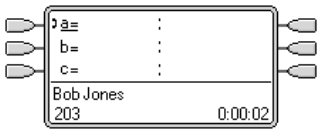
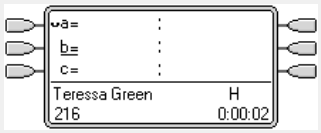
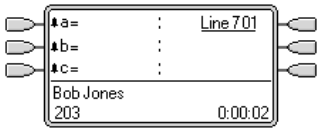
	**Phone Idle** The phone is idle and **Idle Line Preference** has assigned current selected button to the first call appearance.

Table continues…

	**Call Alerting** A call has arrived and **Ringing Line Preference** keeps the current selected button at the first call appearance.
	**Call Answered** With the call answered it retains current selected button status.
	**Call Held** When the call is put on hold, **Idle Line Preference** assigns current selected button status to the next available call appearance button.

Idle Line Preference Example 4

In this example, only **Idle Line Preference** has been programmed for the user. **Ringing Line Preference** has not been programmed.

	**All Call Appearances Alerting** In this case, all the users call appearance buttons are alerting incoming calls. Idle Line Preference has changed the currently selected button to the first available line appearance.

Related links

Appearance Button Features on page 1220

Ringing Line Preference

Ringing Line Preference determines the user's currently selected button as the button which has been alerting the longest. Selected button indication is applied to that button and if the user goes off-hook, for example by lifting their handset, the alerting call on that button is answered.

- Ringing Line Preference includes calls alerting on call appearance, line appearance, bridged appearance and call coverage buttons.
- **Ringing Line Preference** overrides **Idle Line Preference**.
- By default **Ringing Line Preference** is on for all users.
- **Ringing Line Preference Order** When a user's longest waiting call alerts on several of the user's appearance buttons and Ringing Line Preference is set for the user, the order used for current selected button assignment is;
  - Call appearance.
  - Bridged appearance.
  - Call coverage.

- Line appearance.

- **Example:**

  A user has a call to a covered user alerting initially on a line appearance button. Ringing Line Preference assigns current selected button status to the line appearance. When the same call also begins to alert on the call coverage appearance button, current selected button status switches to the call coverage appearance button.

- **Ring Delay and Ringing Line Preference**

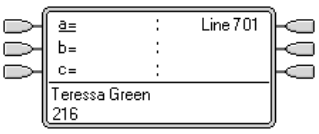
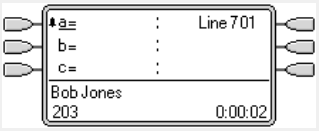
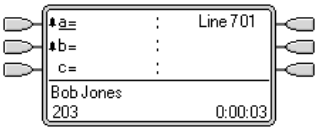
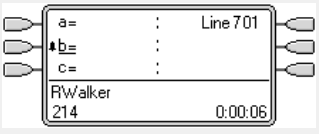
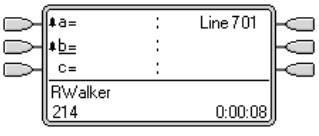
  Appearance buttons can be set to **Delayed Ring** or **No Ring**. These buttons still alert visually but do not give an audible ring or tone. Ringing line preference is still applied to alerting buttons even if set to **Delayed Ring** or **No Ring**.

- **Delayed Ring Preference**

  For users with **Ringing Line Preference** selected, their **Delayed Ring Preference** setting sets whether ringing line preference is used or ignores buttons that are visually alerting but have **Delayed Ring** or **No Ring** set. The default is off, ie. ignore ring delay.

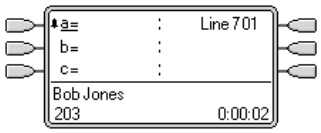
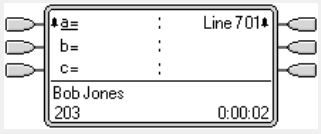
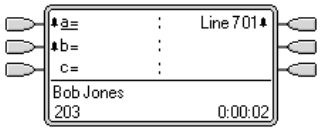
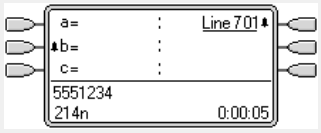
Ringing Line Preference Example 1

In this example, both **Ring Line Preference** and **Idle Line Preference** have been set for the user. They also have **Ringing Line Preference** on and **Auto Hold** is on. **Answer Pre-Select** is off.

	**Phone Idle** The phone is idle. The current selected button has been determined by Idle Line Preference as the first available idle call appearance button. This is shown by the _ underscore next to that button.
	**First Call Alerting** A call for the user arrives. It alerts on the first available call appearance button. Ringing Line Preference uses this as the currently selected button as it is the only alerting call.
	**Second Call Alerting** Another call for the user arrives. It alerts on the next available call appearance button. As the first call has been alerting longer, under Ringing Line Preference it retains the currently select button status.
	**The First Call Abandons** The first caller disconnects. Ringing Line Preference changes the currently selected button status to the second call appearance button.
	**Another Call Arrives** Another call arrives. It alerts as the first free call appearance button. However the call at the second call appearance has been alerting longer and so under Ringing Line Preference retain the currently selected button status.

Ringing Line Preference Example 2

In this example, the user has both Ring Line Preference and Idle Line Preference programmed. They also have **Ringing Line Preference** on and **Auto Hold** is on. **Answer Pre-Select** is off.

	**First Call to User** A call for the user arrives. It alerts on the first available call appearance button. Ringing Line Preference uses this as the currently selected button as it is the only alerting call.
	**Call on Line 601** The user's Line Appearance is alerting due to an incoming call on the associated line. Details of the call and its destination are shown. Ringing Line Preference keeps the currently selected button status on the call appearance button as this has been alerting longest.
	**Second Call to User** A second call to the user arrives and alerts on the second call appearance button. Ringing Line Preference keeps the currently selected button status on the call appearance button as this has been alerting longest.
	**The First Caller Abandons** The first call to the user disconnects. Ringing Line Preference passes the currently selected button status to the Line Appearance button as this has been alerting longest.

Related links

Appearance Button Features on page 1220

Answer Pre-Select

On some phones, only the details of the call alerting or connected on the current selected button are shown. The details of calls alerting on other buttons are not shown or only shown briefly when they are first presented and are then replaced again by the details of the call on the current selected button.

By default, pressing any of the other alerting buttons will answer the call on that button. Answer pre-select allows a user to press alerting buttons other than the current selected button without actually answering them. Instead the button pressed becomes the current selected button and its call details are displayed.

Note that using answer pre-select with a currently connected call will still either hold or end that call in accordance with the system's Auto Hold setting.

Answer Pre-Select Example 1

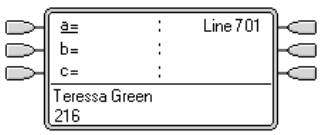
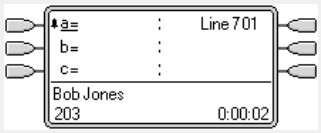
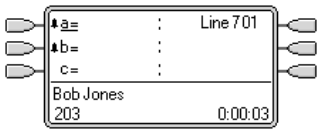
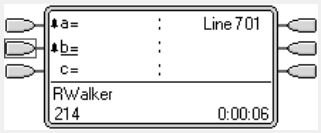
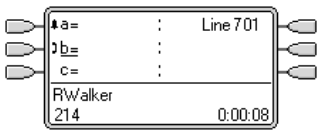
	**Phone Idle** The phone is idle. The current selected button has been determined by Idle Line Preference as the first available idle call appearance button. This is shown by the _ underscore next to that button.

Table continues…

	**First Call Alerting** A call for the user arrives. It alerts on the first available call appearance button. Ringing Line Preference uses this as the currently selected button as it is the only alerting call.
	**Second Call Alerting** Another call for the user arrives. It alerts on the next available call appearance button. As the first call has been alerting longer, under Ringing Line Preference it retains the currently select button status.
	**The User Presses the Second Call Appearance** Pressing the second call appearance overrides ringing line preference and assigns current selected button status to the button without actually answering the call. The details of the caller are displayed.
	**The User Answers the Call** The user can press the button again to answer the call or just go off-hook to answer as it is now the currently selected button.

Related links

Appearance Button Features on page 1220

Auto Hold

Auto Hold is a system wide feature that affects all appearance button users. This feature determines what happens when a user, who is already on a call, presses another appearance button. The options are:

- If **Auto Hold** is **off**, the current call is disconnected.
- If **Auto Hold** is **on**, the current call is placed on hold.

Auto Hold Example 1

In this example, the user has two calls currently shown on call appearance buttons. **Answer Pre-Select** is off.

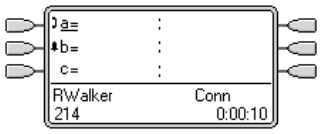
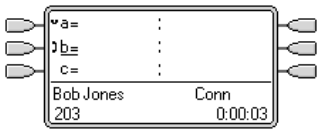
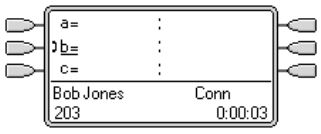
	1. This user has three call appearance buttons. They have answer one call and are still connected to it, shown by the icon. A second call is now alerting on their second call appearance button, shown by the icon. 2. What happens when the user presses the second call appearance key is determined by the system's **Auto Hold** setting:

Table continues…

	**Auto Hold On** When the second call appearance key is pressed, that call is answered and the first call is put on hold, shown by the icon. The user can switch between calls using the call appearance buttons and make/receive other calls if they have additional call appearance buttons
	**Auto Hold Off** When the second call appearance key is pressed, that call is answered and the first call is disconnected.

Related links

Appearance Button Features on page 1220

Ring Delay

Ring delay can be applied to appearance buttons. This option can be used with all types of appearance buttons and can be selected separately for each appearance button a user has. Using ring delay does not affect the buttons visual alerting through the display and display icons or button lamps.

Ring delay is typically used with line appearance buttons for lines which a user wants to monitor but does not normally answer. However ring delay can be applied to any type of appearance button.

The selectable ring delay options for an appearance button are listed below. The option is selected as part of the normal button programming process.

Option	Description
Immediate	Provide audible alerting as per normal system operation.
Delayed Ring	Only provide audible alerting after the system ring delay or, if set, the individual user's ring delay.
No Ring	Do not provide any audible alerting.

There are two possible sources for the delay used when delayed ringing is selected for a button.

- **User** > **Telephony** > **Multi-line Options** > **Ring Delay**: Default = Blank (Use system setting), Range 1 to 98 seconds. This setting can be used to override the system setting. It allows a different ring delay to be set for each user.
- **System** > **Telephony** > **Telephony** > **Ring Delay**: Default = 5 seconds, Range 1 to 98 seconds. This is the setting used for all users unless a specific value is set for an individual user.

Notes

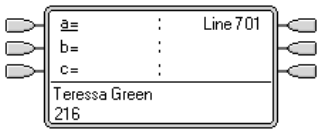
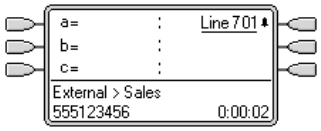
- **Calls That Ignore Ring Delay** - Ring delay is not applied to hold recall calls, park recall calls, transfer return calls, voicemail ringback calls and automatic callback calls. For phones using

Internal Twinning, ring delay settings are not applied to calls alerting at a secondary twinned extension (except appearance buttons set to **No Ring** which are not twinned).

- **Auto Connect Calls** - Ring delay is applied to these calls before auto-connection. This does not apply to page calls.
- **Multiple Alerting Buttons** - Where a call is presented on more than one button on a user's phone, see Multiple Alerting Buttons, the shortest delay will be applied for all the alerting buttons. For example, if one of the alerting buttons is set to **Immediate**, that will override any alerting button set to **Delayed Ring**. Similarly if one of the alerting buttons is set to **No Ring**, it will be overridden if the other alerting button is set to **Immediate** or **Delayed Ring**.
- **Line Appearance Buttons** - Calls routed to a user that could potentially be presented on both a call appearance button and a line appearance button are only presented on the line appearance button. In this scenario, the ring delay settings used is that of the first free call appearance button.
- **Delay on Analog Lines** - Analog lines set to Loop Start ICLID already delay ringing whilst the system waits for the full ICLID in order to resolve incoming call routing. In this scenario the ring delay operates in parallel to the routing delay.
- **Ring Delay and Ringing Line Preference** - Appearance buttons can be set to **Delayed Ring** or **No Ring**. However, ringing line preference is still applied to alerting buttons even if set to **Delayed Ring** or **No Ring**.
- The user's **Delayed Ring Preference** setting is used to determine whether ringing line preference is used with or ignores buttons that are alerting but have **Delayed Ring** or **No Ring** set.

Ring Delay Example 1

In this example, the user has a line appearance button set but configured to no ring.

	**Phone Idle** The phone is idle. The current selected button has been determined by Idle Line Preference as the first available call appearance button. This is shown by the _ underscore next to that button.
	**Incoming Call Alerting on the Line** An incoming call arrives on the line and begin to alert somewhere on the system. The user's line appearance button shows this visually but doesn't ring audibly. Ringing line preference would makes the line appearance the user's currently selected button and therefore they would answer the line if they went off-hook.

Related links

Appearance Button Features on page 1220

Delayed Ring Preference

When a call is alerting at an idle phone, by default Ringing Line Preference sets the call as the currently selected button and if the user then goes off-hook they will answer that call.

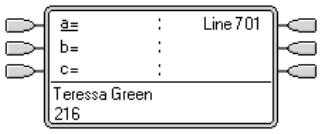
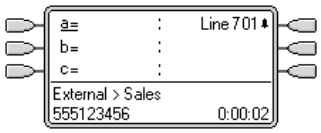
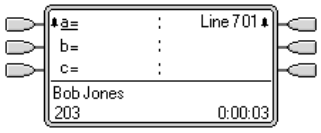
In most situations this is acceptable as the user hears ringing which informs them that there is a call waiting to be answered. If the user wants to make a call instead, they can press another call appearance button to go off-hook on that other button.

When ring delay is being used there can potentially be a problem if the user lifts the handset to make a call without looking at the display. If they do this while the a call is alerting silently on a button with ring delay, the user will actually answer the waiting call rather than get dial tone to make a call.

Once the call alerting on a button has currently selected call status, it retains that status even if a prior call on a button with ring delay applied comes out of its ring delay period.

Delayed Ring Preference Example 1

In this example the user has a line appearance button for a line they monitor. This line appearance button has been set to no ring as the user occasionally need to use that line but does not normally answer calls on that line.

	**Phone Idle** The phone is idle. The current selected button has been determined by Idle Line Preference as the first available call appearance button. This is shown by the _ underscore next to that button.
	**Incoming Call Alerting on the Line** An incoming call arrives on the line and begin to alert somewhere on the system. The user's line appearance button shows this visually but doesn't ring audibly. Normally ringing line preference would make the line appearance the user's currently selected button and therefore they would answer the line if they went off-hook expecting to make a call. However, because **Delayed Ring Preference** is on for the user, ringing line preference is not applied and idle line preference makes their current selected button the first call appearance. If the user were to go off-hook they would be making a call on that call appearance.
	**Call Alerting for the User** A call for the user arrives. It alerts on the first available call appearance button. Ringing line preference is applied and makes that the users currently selected button. If the user goes off-hook now that will answer the call on the call appearance and not the line appearance.

Delayed Ring Preference Example 2

This is similar to the previous example except that the user and the line has been configured for a 15 second ring delay. This informs the users that the line has not been answered for some reason and allows them to answer it by just going off-hook.

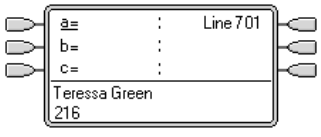
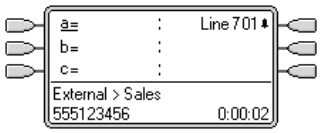
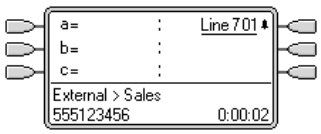
	**Phone Idle** The phone is idle. The current selected button has been determined by Idle Line Preference as the first available call appearance button. This is shown by the _ underscore next to that button.

Table continues…

	**Incoming Call Alerting on the Line** An incoming call arrives on the line and begin to alert somewhere on the system. The user's line appearance button shows this visually but doesn't ring audibly. Because **Delayed Ring Preference** is on for the user, ringing line preference is not applied and idle line preference makes their current selected button the first call appearance. If the user were to go off-hook they would be making a call on that call appearance.
	**Call Continues Alerting** When the ring delay for the line appearance expires, if no other call has taken ringing line preference it becomes the current selected call and will be answered if the user goes off-hook.

Related links

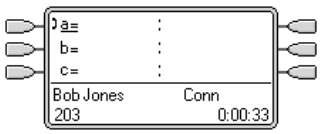
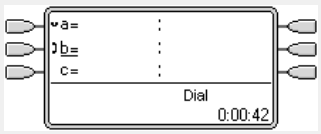
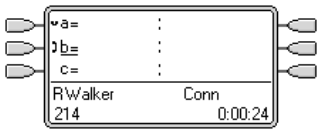
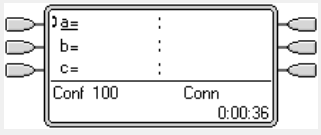
[Appearance Button Features](#) on page 1220

Collapsing Appearances

This topic covers what happens when a user with several calls on different appearance buttons, creates a conference between those calls. In this scenario, the call indication will collapse to a single appearance button and other appearance buttons will return to idle. The exception is any line appearance buttons involved which will show 'in use elsewhere'.

Collapsing Appearances Example 1

In this example, the user will setup a simple conference. **Ringing Line Preference** and **Idle Line Preference** are set for the user. **Auto Hold** for the system is on. **Answer Pre-Select** is off.

	**Initial Call** The user has a call in progress, shown on their first call appearance button. It is decided to conference another user into the call.
	**Make Conference Enquiry** Pressing the **CONFERENCE** button on the users phone automatically places the current call on hold and takes the phone off hook on the next available call appearance.
	**Enquiry in Progress** The other extension has answered and is invited to join a conference call. The user presses the **CONFERENCE** button on their phone again.
	**Conference Starts/Call Appearances Collapse** The conference call has started. The call appearances have collapsed to a single appearance.

Related links

Appearance Button Features on page 1220

Joining Calls

Appearance buttons can be used to "join" existing calls and create a conference call. A user can join calls that are shown on their phone as 'in use elsewhere'.

This feature is often referred to as 'bridging into a call'. However this causes confusion with Bridged appearance buttons and so the term should be avoided.

The ability to join calls is controlled by the following feature which can be set for each user:

- **Cannot be Intruded**: Default = On

  If this option is set on for the user who has been in the call the longest, no other user can join the call. If that user leaves the call, the status is taken from the next internal user who has been in the call the longest. The exceptions are:

  - Voicemail calls are treated as **Cannot be Intruded** at all times.
  - When an external call is routed off switch by a user who then leaves the call, the **Cannot be Intruded** status used is that of the user who forwarded the call off switch.
  - Any call that does not involve an internal user at any stage is treated as **Cannot be Intruded** on. For example:
    - When an external call is routed off switch automatically using a short code in the incoming call route.
    - multi-site network calls from other systems that are routed off-switch.
    - VoIP calls from a device not registered on the system.
- The **Can Intrude** setting is not used for joining calls using appearance buttons.

The following also apply:

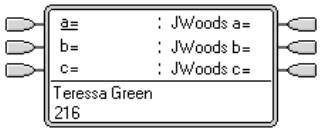
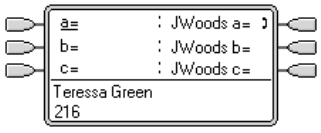
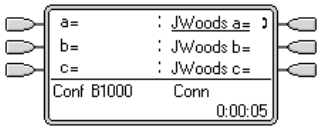
Inaccessible - In addition to the use of the **Cannot be Intruded** setting above, a call is inaccessible if:

- The call is still being dialed, ringing or routed.
- It is a ringback call, for example a call timing out from hold or park.
- If all the internal parties, if two or more, involved in the call have placed it on hold.
- **Conferencing Resources** - The ability to bridge depends on the available conferencing resource of the system. Those resources are limited and will vary with the number of existing parties in bridged calls and conferences. The possible amount of conferencing resource depends on the system type and whether Conferencing Center is also installed.

- **Conference Tone** - When a call is joined, all parties in the call hear the system conferencing tones. By default this is a single tone when a party joins the call and a double-tone when a party leaves the call. This is a system setting.
- **Holding a Bridged Call** - If a user puts a call they joined on hold, it is their connection to the joined call (conference) that is put on hold. The other parties within the call remain connected and can continue talking. This will be reflected by the button status indicators. The user who pressed hold will show 'on hold here' on the button they used to join the call. All other appearance users will still show 'in use here'.
- **Maximum Two Analog Trunks** - Only a maximum of two analog trunks can be included in a conference call.
- **Parked Calls** - A Line Appearance button may indicate that a call is in progress on that line. Such calls to be unparked using a line appearance.

Joining Example 1: Joining with a Bridged Appearance

In this example, the user joins a call using a bridged appearance button. **Answer Pre-Select** is off.

	**User with Bridged Appearance Buttons** The user has bridged appearance buttons that match their colleagues call appearance buttons.
	**Call on Bridged Appearance** The colleague has a call in progress on their first call appearance. This is matched on the first bridged appearance button.
	**User Joins the Call** Pressing the bridged appearance button will take our user off hook and join them into their colleagues call, creating a conference call.

Joining Example 2: Joining with a Line Appearance

In this example, the user joins a call by pressing a line appearance button. **Answer Pre-Select** is off.

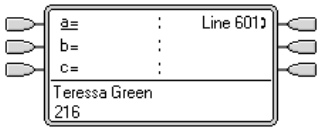
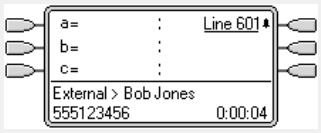
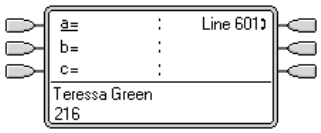
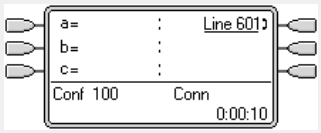
	**Line Goes Active** A call is active on the line with line ID number 601. If this is an incoming call, it will show active but will not alert until its call routing has been determined. On ICLID analog lines, alerting is delayed until the ICLID that might be used to do that routing has been received.
	**Line Appearance Alerting** The call routing is completed and the call is now ringing against its target. The line appearance also begins alerting and Ringing Line Preference has made it the current selected button.

Table continues…

	**Call Answered** Alerting on the line appearance has stopped but the line is still active. This indicates that the call has probably been answered. As our user's phone is idle, Idle Line Preference has returned the current select button to the first available call appearance button.
	**User Joins the Call** Our extension user has been asked by their colleague to join the call just answered on line 601. By pressing the line appearance button they have joined the call on that line and created a conference call.

Related links

[Appearance Button Features](#) on page 1220

Multiple Alerting Appearance Buttons

In some scenarios, it is may be potentially possible for the same call to alert on several appearance buttons. In this case the following apply:

- **Line appearance buttons override call and bridged appearance buttons**

  In cases where a call on a line goes directly to the user as the incoming call route's destination, the call will only alert on the line appearance. In this scenario the ring delay settings used is that of the first free call appearance button.

- **A call can alert both call appearance, line appearance and bridged appearance buttons**

  The most common example of this will be hunt group calls where the hunt group members also have bridged call appearances to each other. In this case the button used to answer the call will remain active whilst the other button will return to idle.

- **Calls on a line/bridged appearance buttons can also alert on call coverage button**

  In this case alerting on the call coverage button may be delayed until the covered user's **Individual Coverage Time** has expired.

- **Ringing Line Preference Order**

  When a call alerts on several of the user's appearance buttons and **Ringing Line Preference** is set for the user, the order used for current selected button assignment is:

  1. Call appearance.
  2. Bridged appearance.
  3. Call coverage.
  4. Line appearance.

Example

A user has a call to a covered user alerting initially on a line appearance button. **Ringing Line Preference** will assign current selected button status to the line appearance. When the same

call also begins to alert on the call coverage appearance button, current selected button status switches to the call coverage appearance button.

Ring Delay

Where ring delays are being used, the shortest delay will be applied for all the alerting buttons. For example, if one of the alerting buttons is set to **Immediate**, that will override any alerting button set to **Delayed Ring**. Similarly if one of the alerting buttons is set to **No Ring**, it will be overridden if the other alerting button is set to **Immediate** or **Delayed Ring**.

Related links

Appearance Button Features on page 1220

Twinning

Twinning is a mechanism that allows an user to have their calls alert at two phones. The user's normal phone is referred to as the primary, the twinned phone as the secondary.

By default only calls alerting on the primary phone's call appearance buttons are twinned. For internal twinning, the system supports options to allow calls alerting on other types of appearance buttons to also alert at the secondary phone. These options are set through the **User | Twinning** section of the system configuration and are **Twin Bridge Appearances**, **Twin Coverage Appearances** and **Twin Line Appearances**. In all cases they are subject to the secondary having the ability to indicate additional alerting calls.

Call alerting at the secondary phone ignoring any Ring Delay settings of the appearance button being used at the primary phone. The only exception is buttons set to No Ring, in which case calls are not twinned.

Related links

Appearance Button Features on page 1220

Busy on Held

For a user who has **Busy on Held** selected, when they have a call on hold, the system treats them as busy to any further calls. This feature is intended primarily for analog phone extension users. Within Manager, selecting **Busy on Held** for a user who also has call appearance keys will cause a prompt offering to remove the **Busy on Held** selection.

Related links

Appearance Button Features on page 1220

Reserving a Call Appearance Button

Functions such as transferring calls using a **Transfer** key require the user to have at least one available call appearance button in order to complete the outgoing call part of the process. However, by default all call appearance button are available to receive incoming calls at all times. Through the system configuration it is possible to reserve the user's last call appearance button for making outgoing calls only.

1400, 1600, 9500 and 9600 Series telephone users can put a call on hold pending transfer if they already have held calls even if they have no free call appearance button available. See Context Sensitive Transfer on page 903.

Reserving a Call Appearance

On the **User | Telephony | Multi-line Options** tab, select the option **Reserve Last CA**.

Related links

Appearance Button Features on page 1220

Logging Off and Hot Desking

Users can be setup to log in and log out at different phones, this is called 'hot desking'. All the users settings, including their extension number, are transferred to the phone at which the user is logged in. This includes their key and lamp settings and appearance buttons.

This type of activity has the following effect on appearance buttons:

If logged out, or logged in at a phone that doesn't support appearance button functions:

- Bridged appearances set to the user will be inactive.
- Call coverage set to the user will still operate.

If logged in at a phone with fewer buttons than programmed for the user:

- Those buttons which are inaccessible on the logged in phone will be inactive.
- Any bridged appearances to those button from other users will be inactive.

Remote Hot Desking

Release 4.0+ supports, through the addition of license keys, users hot desking between systems within a multi-site network. However, the use of appearance buttons (call coverage, bridged appearance and line appearance) within a multi-site network is not supported. Therefore when a user logs in to a remote system, any such button that they have will no longer operate. Similarly any button that other users have with the remote user as the target will not operate.

Related links

Appearance Button Features on page 1220

Applications

A number of system applications can be used to make, answer and monitor calls. These applications treat calls handled using key and lamp operation follows:

SoftConsole

This application can display multiple calls to or from a user and allow those calls to be handled through its graphical interface.

- All calls alerting on call appearance buttons are displayed.
- Calls on line, call coverage and bridged appearance buttons are not displayed until connected using the appropriate appearance button
- Connected and calls held here on all appearance button types are displayed.

Related links

Appearance Button Features on page 1220

Chapter 111: Programming Appearance Buttons

About this task

This section covers the programming of appearance buttons for users into existing system configurations.

Appearance Functions The functions **Call Appearance**, **Bridged Appearance**, **Coverage** and **Line Appearance** are collectively known as "appearance functions". For full details of their operation and usage refer to the Appearance Button Operation section. The following restrictions must be observed for the correct operation of phones.

Appearance functions programmed to buttons without suitable status lamps or icons are treated as disabled. These buttons are enabled when the user logs in on a phone with suitable buttons in those positions.

Line appearance buttons require line ID numbers to have been assigned, see Programming Line Appearance Numbers. The use of line appearances to lines where incoming calls are routed using DID (DDI) is not recommended.

How many buttons are allowed? The supported limits depend on the type of system. They are 10 for IP500 V2 systems, 20 for Server Edition and 40 for Server Edition Select. The limits are applied as follows:

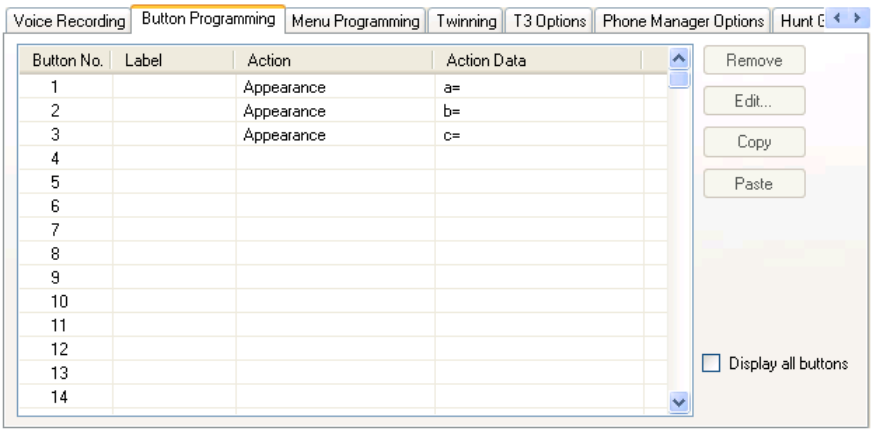
- Number of bridged appearances to the same call appearance.
- Number of line appearances to the same line.
- Number of call coverage appearances of the same covered user.

Programming Appearance Buttons Using Manager

If only button programming changes are required, the configuration changes can be merged back to the system without requiring a reboot.

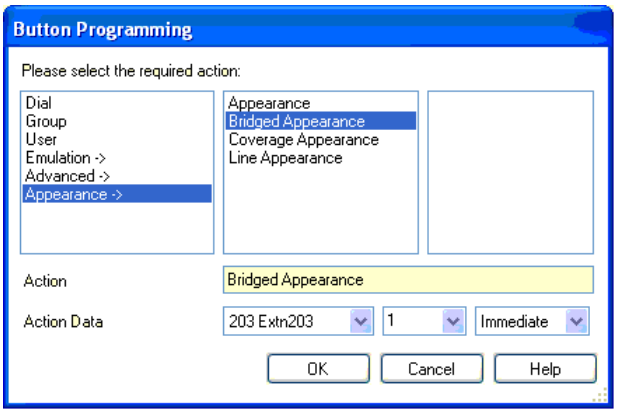
Procedure

1. Start Manager and load the current configuration from the system.
2. Locate and select the user for whom appearance buttons are required.
3. Select **Button Programming**.



The number of buttons displayed is based on the phone associated with the user when the configuration was loaded from the system. This can be overridden by selecting **Display all buttons**.

4. For the required button, click the button number and then click **Edit**.
5. Click the **...** button.



6. From the list of options that appears, click **Appearance**.
7. Select the type of appearance button required.
8. Use the **Action Data** drop-down fields to select the required settings.

   Click **OK**.
9. Repeat for any additional call appearance buttons required.

   Click **OK**.
10. Repeat for any other users requiring appearance buttons.

Related links

[Appearance Function System Settings](#) on page 1239
[Appearance Function User Settings](#) on page 1239
[Programming Line Appearance ID Numbers](#) on page 1241

Outgoing Line Programming on page 1242

Appearance Function System Settings

System settings are applied to all users and calls. The system settings that affect appearance operation are found on the System | Telephony tabs and are:

- Auto Hold
- Conferencing Tone
- Ring Delay
- Visually Differentiate External Call

Related links

Programming Appearance Buttons on page 1237

Appearance Function User Settings

User settings are applied separately to each individual user. In addition to button programming, the following user settings are applicable to appearance button operation:

Cannot be Intruded: Default = On. This feature controls whether other users can use their appearance buttons to join the users call. It applies when the user is the longest present internal party already within the call.

- **Individual Coverage Time (secs):** Default = 10 seconds, Range 1 to 99999 seconds. This function sets how long the phone will ring at your extension before also alerting at any call coverage users. This time setting should not be equal to or greater than the **No Answer Time** applicable for the user.
- **Ring Delay**: Default = Blank (Use system setting). Range = 0 (use system setting) to 98 seconds. This setting is used when any of the user's programmed appearance buttons is set to Delayed ringing. Calls received on that button will initially only alert visually. Audible alerting will only occur after the ring delay has expired.
- **Coverage Ring**: Default = Ring. This field selects the type of ringing that should be used for calls alerting on any the user's call coverage and bridged appearance buttons. **Ring** selects normal ringing. **Abbreviated Ring** selects a single non-repeated ring. **No Ring** disables audible ringing. Note that each button's own ring settings (**Immediate**, **Delayed Ring** or **No Ring**) are still applied.

The ring used for a call alerting on a call coverage or bridged appearance button will vary according to whether the user is currently connected to a call or not.

- If not currently on a call, the **Coverage Ring** setting is used.

- If currently on a call, the quieter of the **Coverage Ring** and **Attention Ring** settings is used.

Attention Ring Setting	Coverage Ring Setting		
	Ring	**Abbreviated**	**Off**
Ring	Ring	Abbreviated	Off
Abbreviated	Abbreviated	Abbreviated	Off

- **Attention Ring**: Default = Abbreviated Ring. This field selects the type of ringing that should be used for calls alerting on appearance buttons when the user already has a connected call on one of their appearance buttons. **Ring** selects normal ringing. **Abbreviated Ring** selects a single ring. Note that each button's own ring settings (**Immediate**, **Delayed Ring** or **No Ring**) are still applied.
- **Ringing Line Preference**: Default = On. For users with multiple appearance buttons. When the user is free and has several calls alerting, ringing line preference assigns currently selected button status to the appearance button of the longest waiting call. Ringing line preference overrides idle line preference.
- **Idle Line Preference**: Default = On. For users with multiple appearance buttons. When the user is free and has no alerting calls, idle line preference assigns the currently selected button status to the first available appearance button.
- **Delayed Ring Preference**: Default = Off. This setting is used in conjunction with appearance buttons set to delayed or no ring. It sets whether ringing line preference should use or ignore the delayed ring settings applied to the user's appearance buttons.

When on, ringing line preference is only applied to alerting buttons on which the ring delay has expired.

When off, ringing line preference can be applied to an alerting button even if it has delayed ring applied.

- **Answer Pre-Select**: Default = Off. Normally when a user has multiple alerting calls, only the details and functions for the call on currently selected button are shown. Pressing any of the alerting buttons will answer the call on that button, going off-hook will answer the currently selected button. Enabling **Answer Pre-Select** allows the user to press any alerting button to make it the current selected button and displaying its call details without answering that call until the user either presses that button again or goes off-hook. Note that when both **Answer Pre-Select** and **Ringing Line Preference** are enabled, once current selected status is assigned to a button through ringing line preference it is not automatically moved to any other button.
- **Reserve Last CA**: Default = Off. Used for users with multiple call appearance buttons. When selected, this option stops the user's last call appearance button from being used to receive incoming calls. This ensures that the user always has a call appearance button available to make an outgoing call and to initiate actions such as transfers and conferences.

1400, 1600, 9500 and 9600 Series telephone users can put a call on hold pending transfer if they already have held calls even if they have no free call appearance button available. See Context Sensitive Transfer.

Abbreviated Ring: This option has been replaced by the **Attention Ring** setting above.

Related links

Programming Appearance Buttons on page 1237

Programming Line Appearance ID Numbers

Line appearances are supported for analog, E1 PRI, T1, T1 PRI, and BRI PSTN trunks. They are not supported for E1R2, QSIG and IP trunks.

Note that setting and changing line settings including line appearance ID numbers requires the system to be rebooted.

Related links

Programming Appearance Buttons on page 1237

Automatic Renumbering

About this task

Procedure

1. Select **Tools | Line Renumber**.
2. Select the starting number required for line numbering and click **OK**.
3. All lines that support **Line Appearance ID** will be numbered in sequence.

Manual Renumbering

About this task

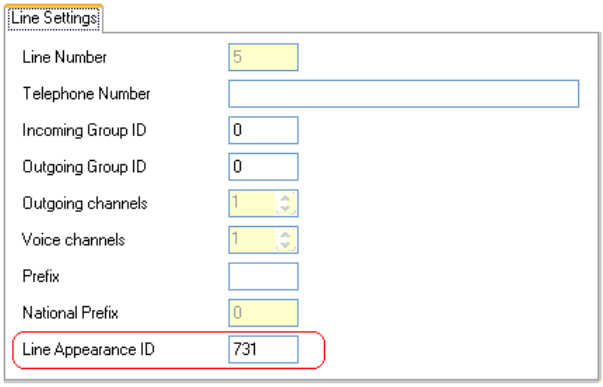
Procedure

1. Start Manager and load the current configuration from the system.
2. Select **Line**.
3. Select the line required.

   The tab through which line appearance ID numbers are set will vary depending on the type of line. A couple of examples are shown below.

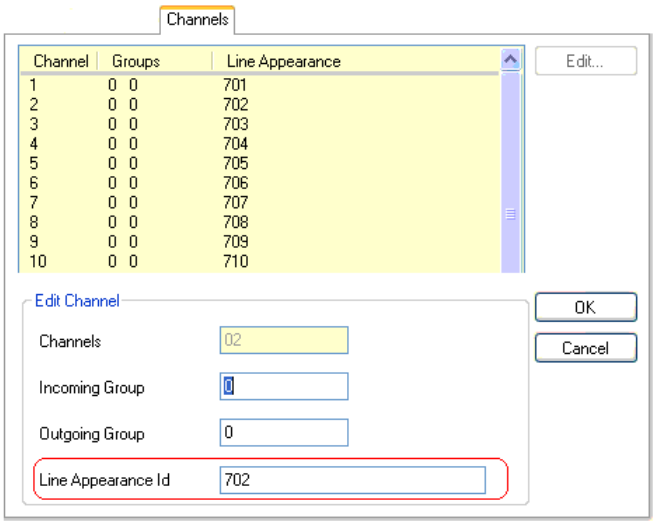
   a. Analog Line

      On the **Line Settings** tab select **Line Appearance ID** and enter the ID required.



b. Basic/Primary Rate Trunks

On the Channels tab select the individual channel and click Edit. Select **Line Appearance ID** and enter the required ID, then click **OK**. Repeat for all the channels required.



4. Click **OK**and repeat for any other lines.

Outgoing Line Programming

Assigning line ID numbers to lines and associating line appearance buttons to those lines is sufficient for answering incoming calls on those lines. However, to use line appearance buttons for outgoing calls may require further programming.

Short Codes and Outgoing Line Appearance Calls Once a line has been seized using a line appearance button, short code matching is still applied to the number dialed. That can include user, system and ARS short codes.

The short codes matching must resolve to an off-switch number suitable to be passed direct to the line.

The final short code applied must specify a 'dial' feature. This allows call barring of specific matching numbers to be applied using short codes set to features such as 'Busy'.

Related links

Programming Appearance Buttons on page 1237

Part 16: SMDR Call Records

Chapter 112: Appendix: SMDR Call Records

The control unit is able to send SMDR (Station Message Detail Reporting) records to a specified IP address and port. Various third-party call billing applications are able to process those records to produce call reports.

- An SMDR record is output for each call between two parties.
- The SMDR record is output when the call between the parties ends.
- In some scenarios, for example transferred calls, multiple SMDR records are output for each part of the call. That is, each part of the call where one of the parties involved changes. The different parts of the call are referred to as ‘call legs’ or ‘call segments’.
- Each SMDR call record is output in a CSV format with a comma between each field.

Related links

Enabling SMDR on page 1245
SMDR Record Buffering on page 1246
Checking SMDR Generation on page 1246
SMDR Record Output on page 1246
SMDR Record Format on page 1247
Call Times in SMDR on page 1247
SMDR Fields on page 1248

Enabling SMDR

SMDR output is enabled as follows:

1. Access the system configuration using your preferred manager application.
2. Select **System** settings and then select the **SMDR** tab.
3. Use the **Output** drop down box to select **SMDR only** and enter the required **IP Address** and **TCP Port**.
4. Adjust any other SMDR output settings if required.
5. For systems in a network of IP Offices, repeat this for all systems.

Related links

Appendix: SMDR Call Records on page 1245

SMDR Record Buffering

The system generates a record at the end of a call or each call leg. It attempts to send the record at the time it is generated. However, if not possible, it buffers records up to the limit set for the system. By default that is 500 records.

- Whilst buffering, it still attempts to send a record when that new record is generated. If successful, it will also send any buffered records.
- If the buffer limit is reached, the system deletes the oldest record each time a new record is added. The buffer is maintained through system restarts.

Related links

Appendix: SMDR Call Records on page 1245

Checking SMDR Generation

Having enabled SMDR output, the generation of records can be view by enabling the **Call** trace option **Call Logging** in System Monitor. Note that this causes any records displayed to be removed from the buffer.

Related links

Appendix: SMDR Call Records on page 1245

SMDR Record Output

An SMDR record is generated at the end of each call between two devices on the system. Devices include extensions, trunk lines (or channels on a trunk), voicemail channels, conference channels and system tones.

- SMDR records are only produced for calls which are presented to another device or a barred short code. For example, an internal user dialing a short code that simply changes a setting does not produce a SMDR record.
- SMDR records are generated when each call or call leg ends. Therefore the output order of the SMDR records does not match the call start times.
- Each record contains a **Call ID** :
  - The **Call ID** starts from 1,000,000 and is reset back to that value following each system restart.

- The **Call ID** is increased by 1 for each subsequent new call.
- When a call moves from one device to another, separate SMDR records are output each part of the call. Each of these records has the same **Call ID**.
- Each record indicates in its **Continuation** field whether there are further records for the same call.

Related links

Appendix: SMDR Call Records on page 1245

SMDR Record Format

The format used for the SMDR record output is:

- Each SMDR record contains call information in a comma-separated format (CSV), that is a byte stream of variable width fields delimited by commas (0x2C).
- Each record is terminated by carriage-return (0x0D), newline (0x0A) sequence. There is no quoting or escaping currently defined as fields do not include ',' or 'newline' characters.

Related links

Appendix: SMDR Call Records on page 1245

Call Times in SMDR

Each SMDR record can include values for ringing time, connected time, held time and parked time. The total duration of an SMDR record is the sum of those values.

- The time when a call is not in one of the states above, is not included in the SMDR record.
- All times are rounded up to the nearest second.
- Where announcements are being used, the connected time for a call begins either when the call is answered or the first announcement begins.
- Each SMDR record has a **Call Start Time** taken from the system time. For calls being transferred or subject to call splitting, each of the multiple SMDR records for the call has the same **Call Start** time as the original call.
- The **UTC Time** shown at the end of the record is the time at which the SMDR record was generated.

Related links

Appendix: SMDR Call Records on page 1245

SMDR Fields

The format used for the SMDR record output is:

- Each SMDR record contains call information in a comma-separated format (CSV), that is a byte stream of variable width fields delimited by commas (0x2C).
- Each record is terminated by carriage-return (0x0D), newline (0x0A) sequence. There is no quoting or escaping currently defined as fields do not include ',' or 'newline' characters.

Each SMDR record can contain the following fields.

- Note that time values are rounded up to the nearest second.
- Empty fields are shown if the field is not applicable to the call.

No.	Field	Description
1.	**Call Start Time**	The call start time in the format YYYY/MM/DD HH:MM:SS. This is based on the system time including any DST offset. • All records relating to the same call, that is having the same **Call ID**, have the same **Call Start Time**. • If the system has **Call Splitting for Diverts** enabled, the **Call Start Time** is changed to the time the forward occurred for all records following that stage of the call. However, the records for the externally forwarded call retain the original **Call ID**.
2.	**Connected Time**	Duration of the connected part of the call in HH:MM:SS format. This does not include ringing, held and parked time. A lost or failed call will have a duration of 00:00:00. The total duration of a record is calculated as **Connected Time** + **Ring Time** + **Hold Time** + **Park Time**.
3.	**Ring Time**	Duration of the ring part of the call in seconds. • For inbound calls, this represents the interval between the call arriving at the switch and it being answered. It does not match the time a call rang at an individual extension. • For outbound calls, this indicates the interval between the call being initiated and being answered at the remote end if supported by the trunk type. Analog trunks are not able to detect remote answer and therefore cannot provide a ring duration for outbound calls.
4.	**Caller**	The caller's number. If the call originated at an extension, this is the extension number. If the call originated externally, this is the CLI of the caller if available, otherwise blank. For SIP trunks, the field can contain the number plus IP address. For example, 12345@192.0.2.123.
5.	**Direction**	The direction of the call ; **I** for inbound, **O** for outbound. This value can be used in conjunction with the **Is Internal** value below to determine the call type.

Table continues…

No.	Field	Description
6.	**Called Number**	This is the number called by the system. For a call that is transferred, this field shows the original called number, not the number of the party who transferred the call. • **Internal calls** – The extension, group or short code called • **Inbound calls** – The target extension number for the call • **Outbound calls** – The dialed digits • **Voice Mail** – Calls to a user's own voicemail mailbox
7.	**Dialed Number**	For internal calls and outbound calls, this is identical to the **Called Number** above. For inbound calls, this is the DDI of the incoming caller.
8.	**Account Code**	The last account code attached to the call.
9.	**Is Internal**	This field indicates whether both parties on the call are internal (**1**) or not (**0**). Note that calls to destinations on other switches in a network are treated as internal. This value can be used in conjunction with the **Direction** value above to determine the call type as follows:
10.	**Call ID**	This is a numerical identifier, which is incremented for each unique call. If the call has generates several SMDR records, each record has the same **Call ID**. Note that the Call ID is restarted from 1,000,000 following any system restart.
11.	**Continuation**	This value indicates if the call has any further records with the same **Call ID**. It is **1** if there is a further record, otherwise **0**.
12.	**Party1 Device**	The device 1 number. This is usually the call initiator though in some scenarios, such as conferences, this may vary. If an extension/hunt group is involved in the call, its details have priority over any trunk. That includes remote network destinations.

Direction	Is Internal	Call Type
I	**0**	Incoming external call.
O	**1**	Internal call.
O	**0**	Outgoing external call.

Type	Party Device	Party Name
Internal Number	**E**<extension number>	<name>
Voicemail	**V**<9500 + channel number>	**VM Channel** <channel number>
Conference	**V**<1><conference number>+<channel number>	**CO Channel** <conference number.channel number>
Line	**T**<9000+line number>	**Line** <line number>.<channel if applicable>
Other	**V**<8000+device number>	**U**<device class> <device number>.<device channel>
Unknown/Tone	**V8000**	**U1 0.0**

Table continues…

No.	Field	Description
13.	**Party1 Name**	The name of the device. For an extension or agent, this is the user name encoded in UTF-8.
14.	**Party2 Device**	The other party for the call segment. Encoded as per **Party1 Device** above. For barred calls, this field shows **Barred**.
15.	**Party2 Name**	The other parties name. See **Party1 Name** above. For barred calls, this field shows **Barred**.
16.	**Hold Time**	The number of seconds the call has been held during this call segment.
17.	**Park Time**	The number of seconds the call has been parked during this call segment.
18.	**Authorization Valid**	This field is used for authorization codes. This field shows **1** for valid authorization or **0** for invalid authorization. This is Blank, no code is used.
19.	**Authorization Code**	For security, this field shows **n/a** regardless of the authorization code used. This is blank, no code is used.
20.	**User Charged**	This and fields 21 to 27 are used for ISDN Advice of Charge (AoC). If blank, AoC is not being used. This field indicates the user to which the call charge has been assigned. This is not necessarily the user involved in the call.
21.	**Call Charge**	The total call charge calculated using the line cost per unit and user markup.
22.	**Currency**	The currency. This is a system wide setting set in the system configuration.
23.	**Amount at Last User Change**	The current AoC amount at user change.
24.	**Call Units**	The total call units.
25.	**Units at Last User Change**	The current AoC units at user change.
26.	**Cost per Unit**	This value is set in the system configuration against each line on which AoC signalling is set. The values are 1/10,000th of a currency unit. For example, if the call cost per unit is £1.07, a value of 10700 should be set on the line.
27.	**Mark Up**	Indicates the mark up value set in the system configuration for the user to which the call is being charged. The field is in units of 1/100th, for example an entry of 100 is a markup factor of 1 .
28.	**External Targeting Cause**	This field indicates who or what caused the external call and a reason code. For example **U FU** indicates that the external call was caused by the Forward Unconditional settings of a User.

Table continues…

No.	Field	Description
Targeted by		**Reason Code**	
HG	Hunt Group.	**fb**	Forward on Busy.
U	User.	**fu**	Forward unconditional.
LINE	Line.	**fnr**	Forward on No Response.
AA	Auto Attendant.	**fdnd**	Forward on DND.
ICR	Incoming Call Route.	**CfP**	Conference proposal (consultation) call.
RAS	Remote Access Service.	**Cfd**	Conferenced.
?	Other.	**MT**	Mobile Twinning.
		TW	Teleworker.
		XfP	Transfer proposal (consultation) call.
		Xfd	Transferred call.
29.	**External Targeter ID**	The associated name of the targeter indicated in the **External Targeting Cause** field. • For hunt groups and users, this is their name in the system configuration. • For an incoming call route, this is the route's **Tag** value if set, otherwise **ICR**.
30.	**External Targeted Number**	This field is used for forwarded, Incoming Call Route targeted and mobile twin calls to an external line. It shows the external number called by the system as a result of the off-switch targeting whereas other called fields give the original number dialled.
31.	**Calling Party Server IP Address**	This IP address identifies the server where the calling extension is logged in.
32.	**Unique Call ID for the Caller Extension**	Numerical value that is a unique identifier of the call on the server where the call was initiated.
33.	**Called Party Server IP Address**	This IP address identifies the server where the called extension is logged in. If the field does not contain an IP address, then the call is to a trunk outside the IP Office network.
34.	**Unique Call ID for the Called Extension**	Numerical value that is a unique identifier of the call on the server where the called extension is logged in.
35.	**SMDR Record Time**	The system date and time, not including any DST offset, at which the SMDR record was generated. It uses the format YYYY/MM/DD HH:MM:SS.
36.	**Caller Consent Directive**	This field is used for calls going through an auto-attendant service that is configured to ask for caller consent to some choice. • 0 = Consent Not Requested • 2 = Consent Given • 6 = Consent Denied

Table continues…

No.	Field	Description
37.	**Calling Number Verification**	Show the authentication level provided by the ISP on SIP lines configured to use calling number verification. Shows `A`, `B`, `C` or `N/A` is not authentication level information provided. A record is still shown for calls which the system rejects due to failed authentication. For more details, see SIP Calling Number Verification (STIR/SHAKEN) on page 959.

Related links

Appendix: SMDR Call Records on page 1245

Chapter 113: SMDR Examples

The following are examples of system SMDR records for common call scenarios.

In the following examples, the underlined fields indicate key values in the interpretation of the scenario. ... is used to indicate that further fields have been omitted for clarity as they are not relevant to the example.

Related links

SMDR Example: Lost Incoming Call on page 1254
SMDR Example: Transfer on page 1254
SMDR Example: Call Answered by Voicemail on page 1255
SMDR Example: Call Transferred to Voicemail on page 1255
SMDR Example: Internal Call on page 1255
SMDR Example: External Call on page 1255
SMDR Example: Outgoing Call on page 1256
SMDR Example: Voicemail Call on page 1256
SMDR Example: Parked Call on page 1256
SMDR Example: Incoming Call with Account Code on page 1257
SMDR Example: Conference Using Conference Add Short Code on page 1257
SMDR Example: Conference Using Conference Button on page 1258
SMDR Example: Adding a Party to a Conference on page 1258
SMDR Example: Busy/Number Unavailable Tone on page 1259
SMDR Example: Call Pickup on page 1259
SMDR Example: Internal Twinning on page 1259
SMDR Example: Park and Unpark on page 1260
SMDR Example: Distributed Hunt Group Call on page 1260
SMDR Example: Voicemail Supervised Transfer on page 1260
SMDR Example: Outgoing External Call on page 1261
SMDR Example: Rerouted External Call on page 1261
SMDR Example: External Forward Unconditional on page 1261
SMDR Example: Call Transferred Manually on page 1262
SMDR Example: Mobile Twinned Call Answered Internally on page 1262
SMDR Example: Mobile Twinned Call Answered at the Mobile Twin on page 1263
SMDR Example: Mobile Twinned Call Picked Up Using the Twinning Button on page 1263
SMDR Example: External Conference Party on page 1264

SMDR Example: Call Routed by Incoming Call Route on page 1264
SMDR Example: Two Outgoing External Calls Transferred Together on page 1264
SMDR Example: Authorization code on page 1265
SMDR Example: Internal Network Call on page 1265
SMDR Example: Caller Consent Request on page 1265

SMDR Example: Lost Incoming Call

In this record, the **Connected Time** is zero and the **Continuation** field is 0, indicating that the call was never connected. The **Ring Time** shows that it rang for 9 seconds before ending.

```
2014/06/28 09:28:41,00:00:00,9,8004206,I,4324,4324,,0,1000014155,0,E4324,Joe
Bloggs,T9161,LINE 5.1,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Transfer

In this example, 2126 has called 2102. The 1st record has the **Continuation** set a 1, indicating that it the call has further records. The 3rd record has the same **Call ID** but the **Party 2 Device** and **Party 2 Name** fields have changed, indicating that the call is now connected to a different device. We can infer the blind transfer from the 2nd record which shows a call of zero **Connected Time** between the original call destination 2102 and the final destination 2121.

```
2014/07/09
17:51,00:00:38,18,2126,O,2102,2102,,1,1000019,1,E2126,Extn2126,E2102,Extn2102,19,0,...
```

```
2014/07/09
17:52,00:00:00,7,2102,O,2121,2121,,1,1000020,0,E2102,Extn2102,E2121,Extn2121,0,0,...
```

```
2014/07/09
17:51,00:00:39,16,2126,O,2102,2102,,1,1000019,0,E2126,Extn2126,E2121,Extn2121,0,0,...
```

In this second example, extension 402 answers an external call and then transfers it to extension 403. Again the two legs of the external call have the same time/date stamp and same call ID.

```
2014/08/01
15:23:37,00:00:04,7,01707299900,I,4001,390664,,0,1000019,1,E402,Extn402,T9001,Line
1.1,6,0,...
```

```
2014/08/01
15:23:46,00:00:00,3,402,O,403,403,,1,1000020,0,E402,Extn402,E403,Extn403,0,0,...
```

```
2014/08/01
15:23:37,00:00:04,4,01707299900,I,4001,390664,,0,1000019,0,E403,Extn403,T9001,Line
1.1,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Call Answered by Voicemail

In this example, 215 has made a call to 211. However, the **Party2Device** and **Party2Name** fields show that the call was answered by voicemail.

```
2014/10/20 06:43:58,00:00:10,21,215,O,211,211,,I,28,0,E215,Extn215,V9051,VM Channel
1,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Call Transferred to Voicemail

In this example, the **Continuation** field being 1 in the first record tells us that it was not the end of the call. The matching **Call ID** identifies the second record as part of the same call. The change in **Party 1** details between the two records show that the call was transferred to voicemail.

```
2014/06/28 09:30:57,00:00:13,7,01707392200,I,299999,299999,,0,1000014160,1,E4750,John
Smith,T9002,LINE 1.2,11,0,...
```

```
2014/06/28 09:30:57,00:00:21,0,01707392200,I,299999,299999,,0,1000014160,0,V9502,VM
Channel 2,T9002,LINE 1.2,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Internal Call

The **Is Internal** field being 1 indicates that this is an internal call. The **Ring Time** was 4 seconds and the **Connected Time** was 44 seconds.

```
2014/06/26 10:27:44,00:00:44,4,4688,O,4207,4207,,1,1000013898,0,E4688,Joe
Bloggs,E4207,John Smith,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: External Call

The **Is Internal** field being 0 indicates that this is an external call. The **Direction** field being **I** shows that it was an incoming call. The **Ring Time** was 7 seconds and the total **Connected Time** was 5 seconds.

```
2014/08/01
15:14:19,00:00:05,7,01707299900,I,403,390664,,0,1000013,0,E403,Extn403,T9001,Line
1.2,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Outgoing Call

The combination of the **Direction** field being outbound and the **Is Internal** field being 0 show that this was a outgoing external call. The line or channel used is indicated by the **Party2 Name** and being a digital channel the **Ring Time** before the call was answered is also shown.

```
2014/06/28 08:55:02,00:08:51,9,4797,O,08000123456,08000123456,,0,1000014129,0,E4797,Joe
Bloggs,T9001,LINE 1.1,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Voicemail Call

The two records below show calls to voicemail. The first shows the **Dialed Number** as ***17**, the default short code for voicemail access. The second shows the **Dialed Number** as **VoiceMail**, indicating some other method such as the **Message** key on a phone was used to initiate the call.

```
2014/06/28 09:06:03,00:00:19,0,4966,O,*17,*17,,1,1000014131,0,E4966,John Smith,V9501,VM
Channel 1,0,0,...
```

```
2014/06/28 09:06:03,00:00:19,0,4966,O,VoiceMail,VoiceMail,,1,1000014134,0,E4966,John
Smith,V9501,VM Channel 1,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Parked Call

In this example the first record has a **Park Time** showing that the call was parked for 7 seconds. The **Continuation** field indicates that the call did not end yet and there are further records. The second record has the same **Call ID** and shows a change in the Party2Name, indicating that another party unparked the call. Note also that both records share the same call start time.

```
2014/10/20
07:18:31,00:00:12,3,215,O,210,210,,1,1000038,1,E215,Extn215,E210,Extn210,0,7,...
```

```
2014/10/20
07:18:31,00:00:10,0,215,O,210,210,,1,1000038,0,E215,Extn215,E211,Extn211,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Incoming Call with Account Code

Incoming call with Account Code

In this example, at some stage as the call was made or during the call, an Account Code has been entered. During a call, another account code can be entered. The SMDR record shows the last account code used before the record was generated.

```
2014/06/28
11:29:12,00:00:02,2,5002,I,1924,1924,123456789,0,1000014169,0,E1924,Extn1924,T9620,LINE
8.20,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Conference Using Conference Add Short Code

In this example, a user conferences 2 calls. This creates 5 SMDR records; 2 initial 2–party calls and then 3 calls connected to a system's conference.

First 2101 has made a call and put it on hold (record 2), then made another call and put it on hold (record 1) and then dialled the default short code *47 to conference their held calls (record 3). The records for the first two calls have the **Continuation** field set as 1 indicating that the calls continued in further records.

Record 3 shows 2101 making a new call in which they dial *47, which places them and their held calls into a conference. This is shown by the **Party 2 Device** and **Party 2 Name** details as being a conference (100) and the conference channel used for each.

```
2014/07/09
17:55,00:00:03,3,2101,O,8262623#,8262623#,,0,1000024,1,E2101,Extn2101,T9002,Line
2.1,8,0,...
```

```
2014/07/09
17:54,00:00:29,7,2101,O,2121,2121,,1,1000023,1,E2101,Extn2101,E2121,Extn2121,23,0,...
```

```
2014/07/09 17:55,00:00:46,0,2101,O,*47,*47,,1,1000026,0,E2101,Extn2101,V11001,CO
Channel 100.1,0,0,...
```

```
2014/07/09
17:54,00:00:49,0,,O,71234567890,71234567890,,1,1000023,0,E2121,Extn2121,V11003,CO
Channel 100.3,0,0,...
```

```
2014/07/09 17:55,00:00:49,0,,O,8262623#,8262623#,,0,1000024,0,V11002,CO Channel
100.2,T9002,Line 2.1,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Conference Using Conference Button

In this example, an extension user answers a call and then brings in another user by using the **Conference** button on their phone. Again we see records for the initial call, the conference proposal call and then for the 3 parties in the conference that is created.

```
2014/07/09
15:05:41,00:00:04,3,203,O,201,201,,1,1000009,1,E203,Extn203,E201,Extn201,0,0,...

2014/07/09
15:05:26,00:00:09,3,207,O,203,203,,1,1000008,1,E207,Extn207,E203,Extn203,10,0,...

2014/07/09 15:05:41,00:00:08,0,,O,,,,1,1000009,0,E201,Extn201,V11001,CO Channel
100.1,0,0,...

2014/07/09 15:05:50,00:00:10,0,203,O,201,201,,1,1000010,0,E203,Extn203,V11002,CO
Channel 100.2,0,0,...

2014/07/09 15:05:26,00:00:10,0,207,O,203,203,,1,1000008,0,E207,Extn207,V11003,CO
Channel 100.3,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Adding a Party to a Conference

This example is a variant on that above. Having started a conference, extension 203 adds another party.

```
2014/07/09
15:08:31,00:00:03,3,203,O,201,201,,1,1000014,1,E203,Extn203,E201,Extn201,0,0,...

2014/07/09
15:08:02,00:00:22,6,207,O,203,203,,1,1000013,1,E207,Extn207,E203,Extn203,9,0,...

2014/07/09 15:08:45,00:00:02,4,203,O,403,403,,0,1000016,1,E203,Extn203,E403,Libby
Franks,0,0,...

2014/07/09 15:08:02,00:00:24,0,207,O,203,203,,1,1000013,0,E207,Extn207,V11003,CO
Channel 100.3,0,0,...

2014/07/09 15:08:39,00:00:17,0,203,O,201,201,,1,1000015,0,E203,Extn203,V11002,CO
Channel 100.2,8,0,...

2014/07/09 15:08:31,00:00:26,0,,O,,,,1,1000014,0,E201,Extn201,V11001,CO Channel
100.1,0,0,...

2014/07/09 15:08:45,00:00:12,0,,O,403,403,,0,1000016,0,E403,Libby Franks,V11004,CO
Channel 100.4,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Busy/Number Unavailable Tone

In this example, 2122 calls 2123 who is set to DND without voicemail. This results in 2122 receiving busy tone.

The records shows a call with a **Connected Time** of 0. The **Call Number** field shows 2123 as the call target but the **Party 2 Device** and **Party 2 Name** fields show that the connection is to a virtual device that is generating the audio tone.

```
2014/07/09 17:59,00:00:00,0,2122,O,2123,2123,,1,1000033,0,E2122,Extn2122,V8000,U1
0.0,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Call Pickup

The first record shows a call from 2122 to 2124 with a **Connected Time** of zero but a **Ring Time** of 8. The **Continuation** field indicates that the call has further records.

The second record has the same **Call ID** but the **Party 2 Device** and **Party 2 Name** details show that the call has been answered by 2121.

```
2014/07/09
18:00,00:00:00,8,2122,O,2124,2124,,1,1000038,1,E2122,Extn2122,E2124,Extn2124,0,0,...
```

```
2014/07/09
18:00,00:00:38,1,2122,O,2124,2124,,1,1000038,0,E2122,Extn2122,E2121,Extn2121,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Internal Twinning

The records for scenarios such as internal call forwarding or follow me indicate the rerouting in a single record by having **Caller** and **Called Number** details that differ from the final **Party 1** and **Party 2** details. Internal twinning differs is showing a call answered at the twin exactly the same as having been answered at the primary.

203 is internally twinned to 201. Call from 207 to 203 but answer at 201.

```
2014/07/09
16:25:26,00:00:03,7,207,O,203,203,,1,1000037,0,E207,Extn207,E203,Extn203,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Park and Unpark

Parking and unparking of a call at the same extension is simply shown by the **Park Time** field of the SMDR record. Similarly, calls held and unheld at the same extension are shown by the **Held Time** field of the SMDR record for the call. The records below however, show a call parked at one extension and then unparked at another.

The records show a call from 207 to 203. 203 then parks the call shown by the **Park Time**. The call is unparked by 201, hence the first record is indicated as continued in its **Continuation** field. The matching **Call ID** indicates the subsequent record for the call.

```
2014/07/09
16:39:11,00:00:00,2,207,O,203,203,,1,1000052,1,E207,Extn207,E203,Extn203,0,4,...
```

```
2014/07/09
16:39:11,00:00:02,0,207,O,203,203,,1,1000052,0,E207,Extn207,E201,Extn201,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Distributed Hunt Group Call

An incoming call to site A is targeted to a distributed hunt group member on site B. They transfer the call back to a hunt group member on site A.

```
2014/08/01
15:32:52,00:00:10,19,01707299900,I,4002,390664,,0,1000024,1,E209,Luther-209,T9001,Line
1.2,0,0,...
```

```
2014/08/01
15:33:19,00:00:00,2,209,I,403,403,,0,1000025,0,E209,Luther-209,E403,Extn403,0,0,...
```

```
2014/08/01
15:32:52,00:00:03,3,01707299900,I,4002,390664,,0,1000024,0,E403,Extn403,T9001,Line
1.2,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Voicemail Supervised Transfer

A call is routed to a voicemail module that performs a supervised transfer.

```
2014/08/01 16:36:04,00:00:09,0,01707299900,I,xfer,390664,,0,1000061,1,T9001,Line
1.1,V9508,VM Channel 8,0,0,...
```

```
2014/08/01 16:36:07,00:00:03,4,,I,402,402,,0,1000062,0,E402,Extn402,V8000,U12
0.8,0,0,...
```

```
2014/08/01
16:36:04,00:00:09,0,01707299900,I,402,390664,,0,1000061,0,E402,Extn402,T9001,Line
1.1,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Outgoing External Call

The **External Targeting Cause** indicates that the external call was caused by a user. The lack of specific reason implies that it was most likely dialed. The **External Targeter ID** is the user name in this example

```
2014/08/01 16:23:06,00:00:04,5,203,O,9416,9416,,0,1000035,0,E203,Extn203,T9005,Line
5.1,0,0,,,Extn203,,,,,,,,U,Extn203,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Rerouted External Call

In this example, an incoming external call has been rerouted back off switch, shown by the **Party 1** fields and the **Party 2** fields being external line details. The **External Targeter Cause** shows that rerouting of the incoming call was done by an incoming call route (ICR). The **External Targeter ID** in this case is the **Tag** set on the incoming call route. The **External Targeted Number** is the actual external number call.

```
2014/08/01 08:14:27,00:00:03,5,392200,I,9416,200,,0,1000073,0,T9005,Line 5.1,T9005,Line
5.2,0,0,,,,0000.00,,0000.00,0,0,618,0.01,ICR,Main ICR,416,...
```

Related links

SMDR Examples on page 1253

SMDR Example: External Forward Unconditional

In this example, user 203 has a forward unconditional number set for calls. This is indicated by the **External Targeting Cause** showing user and forward unconditional. The **External Targeter ID** shows the source of the call being forwarded, in this example user 207. The **External Targeted Number** shows the actual external number called by the system.

```
2014/08/01 16:22:41,00:00:02,5,207,O,203,203,,0,1000034,0,E207,Extn207,T9005,Line
5.1,0,0,,,Extn203,0000.00,,0000.00,0,0,618,1.00,U fu,Extn207,9416,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Call Transferred Manually

In this example the internal user transfers a call to an external number. The **External Targeting Cause** in the first record indicates that this external call is the result of a user (**U**) transfer proposal (**XfP**) call. The **Continuation** field indicates that another record with the same **Call ID** will be output.

The additional records are output after the transferred call is completed. The first relates to the initial call prior. The second is the transferred call with the **External Targeting Cause** now indicating user (**U**) transferred (**Xfd**).

```
2014/08/01 16:33:19,00:00:05,3,203,O,9416,9416,,0,1000044,1,E203,Extn203,T9005,Line
5.1,0,0,,,,,,,,,,U XfP,Extn207,...
```

```
2014/08/01
16:33:09,00:00:02,2,207,O,203,203,,1,1000043,0,E207,Extn207,E203,Extn203,11,0,...
```

```
2014/08/01 16:33:19,00:00:04,0,207,O,9416,9416,,0,1000044,0,E207,Extn207,T9005,Line
5.1,0,0,,,Extn207,,,,,,,,U Xfd,Extn203,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Mobile Twinned Call Answered Internally

For this example, user 203 has mobile twining enabled to the external number 9416 as their twin. Their mobile dial delay is set to 2 seconds. The call is answered at the user's internal extension.

In this scenario the record for the external call part of twinning is output immediately the call is answered internally. The **Call Start Time** for this record differs due to the user's **Mobile Dial Delay** setting. The **External Targeting Cause** indicates the external call was the result of user (**U**) mobile twinning (**MT**) settings. If the call had been answered before the mobile dial delay expired, no external call and therefore no record would be produced. When the call is completed the second record is output.

```
2014/08/01 16:17:59,00:00:00,7,,O,9416,9416,,0,1000028,0,E203,Extn203,T9005,Line
5.1,0,0,,,,,,,,,,U MT,Extn203,9416,...
```

```
2014/08/01
16:17:58,00:00:07,9,207,O,203,203,,1,1000027,0,E207,Extn207,E203,Extn203,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Mobile Twinned Call Answered at the Mobile Twin

This is the same scenario as the example above except that the call is answered at the external mobile twinning destination. Unlike the previous example, the external call record has a non-zero **Connected Time**, showing that the call was also answered externally.

```
2014/08/01 16:17:04,00:00:06,9,,O,9416,9416,,0,1000026,0,E203,Extn203,T9005,Line
5.1,0,0,,,,,,,,,,U MT,Extn203,9416,...
```

```
2014/08/01
16:17:02,00:00:06,11,207,O,203,203,,1,1000025,0,E207,Extn207,E203,Extn203,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Mobile Twinned Call Picked Up Using the Twinning Button

This is the same scenario as the example above, however after answering the call on the external twinned device, the user has picked it up internally by using a twinning button. The first two records are for the answered external call and are output when that call is picked up by the internal extension. The third record is output when the call is ended internally.

```
2014/08/01
16:19:18,00:00:05,11,207,O,203,203,,1,1000029,1,E207,Extn207,E203,Extn203,0,0,...
```

```
2014/08/01 16:19:20,00:00:05,9,,O,9416,9416,,0,1000030,0,E203,Extn203,T9005,Line
5.1,0,0,,,,,,,,,,U MT,Extn203,9416,...
```

```
2014/08/01
16:19:18,00:00:05,0,207,O,203,203,,1,1000029,0,E207,Extn207,E203,Extn203,0,0,...
```

Related links

SMDR Examples on page 1253

SMDR Example: External Conference Party

This is similar to internal conferencing (see examples above) but the conference setup and progress records include **External Targeting Cause** codes for user (**U**) conference proposal (**CfP**) and user (**U**) conferenced (**Cfd**).

```
2014/08/01 16:48:58,00:00:02,2,203,O,9416,9416,,0,1000066,1,E203,Extn203,T9005,Line
5.1,0,0,,,,,,,,,,U CfP,Extn203,...
```

```
2014/08/01
16:48:37,00:00:04,3,203,O,207,207,,1,1000064,1,E203,Extn203,E207,Extn207,7,0,...
```

```
2014/08/01 16:49:04,00:00:08,0,203,O,9416,9416,,1,1000067,0,E203,Extn203,V11002,CO
Channel 100.2,0,0,...
```

```
2014/08/01 16:48:37,00:00:13,0,,O,,,,1,1000064,0,E207,Extn207,V11003,CO Channel
100.3,0,0,...
```

```
2014/08/01 16:48:58,00:00:13,0,,O,9416,9416,,0,1000066,0,V11001,CO Channel
100.1,T9005,Line 5.1,0,0,,,Extn203,,,,,,,,U Cfd,Extn203,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Call Routed by Incoming Call Route

Call from external number 403 rerouted by incoming call route (ICR) for incoming line group 701 back out to 404.

```
2014/08/01 11:45:36,00:00:01,2,403,I,9404,,,0,1000007,0,T9001,Line 1.0,T9010,Line
10.0,0,0,0,n/a,,,,,,,,,ICR,ICR701,404,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Two Outgoing External Calls Transferred Together

This scenario shows an outgoing call which is then transferred to another outgoing call.

```
2009/02/19 11:13:26,00:00:06,0,203,O,9403,9403,,0,1000012,1,E203,Extn203,T9001,Line
1.0,8,0,0,n/a,,,,,,,,,U,Extn203,...
```

```
2009/02/19 11:13:36,00:00:02,0,203,O,8404,8404,,0,1000013,0,E203,Extn203,T9002,Line
2.0,0,0,0,n/a,,,,,,,,,U XfP,Extn203,...
```

```
2009/02/19 11:13:26,00:00:11,0,8404,I,404,,,0,1000012,0,T9002,Line 2.0,T9001,Line
1.0,0,0,0,n/a,,,,,,,,,LINE Xfd,0.1038.0 13 Alog Trunk:2,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Authorization code

In this example, an authorization code was used and the 0 indicates that it is invalid.

```
2014/02/20 11:04:59,00:00:00,0,319,O,,,,0,1000009,0,E319,Alice,V8000,U1 0.0,0,0,0,n/
a,,,,,,,,U,Alice,...
```

In this example, the authorization code is valid.

```
2014/02/20 11:04:59,00:00:00,0,319,O,,,,0,1000009,0,E319,Alice,V8000,U1 0.0,0,0,1,n/
a,,,,,,,,U,Alice,...
```

Related links

SMDR Examples on page 1253

SMDR Example: Internal Network Call

The SMDR records include fields (31 to 34) that identifying the calling and called IP Office systems. These are useful for calls between systems in an IP Office network. This still requires each system in the network to be configured to output its own SMDR records..

In this example, 806 on the 1st IP Office system (192.168.0.182) makes an internal call to 706 on the 2nd IP Office system (192.168.0.180). Both systems output their own SMDR record for the same call.

Record from 1st IP Office system with the calling extension 806

```
2020/03/06
10:33:27,00:00:15,8,806,I,706,706,,1,1000018,0,E806,Extn806,E706,Extn706,7,0,,,,,,,,,,
,,192.168.0.182,1049,192.168.0.180,1087,
2020/03/06 10:33:56,0
```

Record from 2nd IP Office system with the called extension 706

```
2020/03/06
10:33:27,00:00:22,8,806,O,706,706,,1,1000004,0,E806,Extn806,E706,Extn706,0,0,,,,,,,,,,
,,192.168.0.182,1049,192.168.0.180,1087,
2020/03/06 10:33:56,0
```

Related links

SMDR Examples on page 1253

SMDR Example: Caller Consent Request

The actions in Embedded Voicemail auto-attendants and Voicemail Pro call flows can be assigned a consent setting value. By selecting the particular action the caller can indicated their consent. That value is indicated the SMDR record for the call.

Consent Not Requested

In this example, the call action used to route the call does not have a consent setting. Therefore, the consent setting within the SMDR record remains 0.

```
2020/03/06 10:35:42,00:00:02,0,201,O,*99,*99,,1,1000000,1,E201,Extn201,V9511,VM Channel
11,0,0,,,,,,,,,,,,,192.168.0.1,1002,192.168.0.1,1004,
2020/03/06 10:35:45,0
2020/03/06
10:35:42,00:00:02,2,201,O,*99,*99,,1,1000000,0,E201,Extn201,E202,Extn202,0,0,,,,,,,,,,
,,192.168.0.1,1002,192.168.0.1,1005,
2020/03/06 10:35:49,0
```

Consent Denied

In this example, the call action used to route the call is set to indicate consent denied. Therefore, the consent setting in the SMDR record is changed to 6.

```
2020/03/06 10:35:54,00:00:02,0,201,O,*99,*99,,1,1000001,1,E201,Extn201,V9511,VM Channel
11,0,0,,,,,,,,,,,,,192.168.0.1,1007,192.168.0.1,1009,
2020/03/06 10:35:56,6
2020/03/06
10:35:54,00:00:01,4,201,O,*99,*99,,1,1000001,0,E201,Extn201,E202,Extn202,0,0,,,,,,,,,,
,,192.168.0.1,1007,192.168.0.1,1010,
2020/03/06 10:36:00,6
```

Consent Given

In this example, the consent action used to route the call is set to indicate consent accepted. Therefore, the consent setting in the SMDR record is changed to 2.

```
2020/03/06 10:36:08,00:00:02,0,201,O,*99,*99,,1,1000003,1,E201,Extn201,V9511,VM Channel
11,0,0,,,,,,,,,,,,,192.168.0.1,1014,192.168.0.1,1016,
2020/03/06 10:36:09,2
2020/03/06
10:36:08,00:00:01,1,201,O,*99,*99,,1,1000003,0,E201,Extn201,E202,Extn202,0,0,,,,,,,,,,
,,192.168.0.1,1014,192.168.0.1,1017,
2020/03/06 10:36:11,2
```

Related links

SMDR Examples on page 1253

Part 17: Further Help

Chapter 114: Additional Help and Documentation

The following pages provide sources for additional help.

Related links

Additional Manuals and User Guides on page 1268
Getting Help on page 1268
Finding an Avaya Business Partner on page 1269
Additional IP Office resources on page 1269
Training on page 1270

Additional Manuals and User Guides

The Avaya Documentation Center website contains user guides and manuals for Avaya products including IP Office.

- For a listing of the current IP Office manuals and user guides, look at the Avaya IP Office™ Platform Manuals and User Guides document.
- The Avaya IP Office Knowledgebase and Avaya Support websites also provide access to the IP Office technical manuals and users guides.
  - Note that where possible these sites redirect users to the version of the document hosted by the Avaya Documentation Center.

For other types of documents and other resources, visit the various Avaya websites (see Additional IP Office resources on page 1269).

Related links

Additional Help and Documentation on page 1268

Getting Help

Avaya sells IP Office through accredited business partners. Those business partners provide direct support to their customers and can escalate issues to Avaya when necessary.

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner. See Finding an Avaya Business Partner on page 1269.

Related links

Additional Help and Documentation on page 1268

Finding an Avaya Business Partner

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner.

Procedure

1. Using a browser, go to the Avaya Website at https://www.avaya.com
2. Select **Partners** and then **Find a Partner**.
3. Enter your location information.
4. For IP Office business partners, using the **Filter**, select **Small/Medium Business**.

Related links

Additional Help and Documentation on page 1268

Additional IP Office resources

In addition to the documentation website (see Additional Manuals and User Guides on page 1268), there are a range of website that provide information about Avaya products and services including IP Office.

- Avaya Website (https://www.avaya.com)

  This is the official Avaya website. The front page also provides access to individual Avaya websites for different regions and countries.
- **Avaya Sales & Partner Portal** *(*https://sales.avaya.com*)*

  This is the official website for all Avaya business partners. The site requires registration for a username and password. Once accessed, you can customize the portal to show specific products and information type that you want to see.
- **Avaya Support** *(*https://support.avaya.com*)*

  This site provide access to Avaya product software, documentation and other services for Avaya product installers and maintainers.

  - **Avaya Support Forums** *(*https://support.avaya.com/forums/index.php*)*

    This site provides forums for discussing product issues.

- **International Avaya User Group** *(*https://www.iuag.org*)*

  This is the organization for Avaya customers. It provides discussion groups and forums.

- **Avaya Learning** *(*https://www.avaya-learning.com/*)*

  This site provides access to training courses and accreditation programs for Avaya products.

Related links

Additional Help and Documentation on page 1268

Training

Avaya training and credentials ensure our Business Partners have the capabilities and skills to successfully sell, implement, and support Avaya solutions and exceed customer expectations. The following credentials are available:

- Avaya Certified Sales Specialist (APSS)
- Avaya Implementation Professional Specialist (AIPS)
- Avaya Certified Support Specialist (ACSS)

Credential maps are available on the Avaya Learning website.

Related links

Additional Help and Documentation on page 1268

Index

Numerics

1500 DECT extensions 36
911 View 773
911–View 1142

A

AA Number 263, 659
about 43
Access Control Lists 506
accessibility 49
account code 272, 273
Account Code 45
account code configuration 840
ACO persistent gateway 36
Acquire
    Button 1117
Action
    Dial By Conference 666
    Dial By Name 667
    Dial By Number 669
    Leave Message 670
    Park & Page 672
    Replay Menu 674
    Speak By Name 675
    Speak By Number 676
    Supervised Transfer 671
    Transfer to Auto Attendant 678
    Unsupervised Transfer 677
actions 104, 110
    backup 105
    remote operations management 109
    restore 105
    synchronize APNP system-ID 108
    synchronize APNS configuration 108
    synchronize service user and system password 107
    synchronize single sign-on configuration 107
    transfer ISO 106
    upgrade 106
Actions 666
actions button 46
Ad-Hoc conference
    Add 694
Ad-Hoc Conference 694
add
    template 82
    user/extension from template 82
Add
    Auto-Attendant 656
    System Conference 700
additional hard drive
    settings 153
Administrator 1268
alarms 628
alternate route selection 275
    add alternate route 275
Alternate Route Selection 45
analog 214
Announcement
    Auto-Attendant 263, 659
announcements 197
APIs 1269
app center
    settings 154
Apple
    push notifications 849, 850
Application Notes 1269
application server 102
    IP Office IP address 49
applications
    centralized media manager audit trail 633
    file manager 601
    IP Office Manager 602
    one-X Portal 604
        Voicemail Pro
            system preferences
                alarms 615
                backup config 617
                email 607
                general 605
                Gmail integration 610
                housekeeping 611
                outcalling 613
                SNMP alarm 612
                Syslog 615
                user group 617
                voicemail recording 614
    Voicemail Pro call flow management 618
    web license manager 624
        WebRTC 619
            media gateway settings 621
            SIP server settings 620
            system settings 619
Applications 45
applications menu 600
Archival Solution 709
Archive
    Recordings 719
ARS 45
Attendant
    Consent 653
    Dial By Conference 666
    Dial By Name 667
    Dial By Number 669
    Leave Message 670

Attendant *(continued)*
Park & Page ... 672
Replay Menu ... 674
Speak By Name ... 675
Speak By Number ... 676
Supervised Transfer ... 671
Transfer to Auto Attendant ... 678
Unsupervised Transfer ... 677
Audio Output ... 263, 659
audit trail ... 631
centralized media manager ... 633
Audit trail ... 717
authentication
settings ... 149
authorization code ... 280
add authorization code ... 280
Authorization Codes ... 45
auto attendant ... 259
add auto attendant
actions ... 260
embedded voicemail ... 257
setup wizard ... 74
Auto Attendants ... 45
auto intercom deny off ... 997
auto intercom deny on ... 997
Auto-attendant
Actions ... 666
Prompts ... 679
Auto-Attendant ... 649
Actions ... 267, 663
Add ... 656
Callflow ... 652
Consent ... 653
Delete ... 657
Delete multiple ... 657
Dial By Conference ... 666
Dial By Name ... 667
Dial By Number ... 669
Edit ... 656
External calls ... 683
Fallback Action ... 267, 663
Fallback options ... 652
Greeting ... 263, 659
Internal call ... 683
Language ... 650
Leave Message ... 670
Menu ... 263, 659
Name prompts ... 681
Park & Page ... 672
Pre-recorded prompts ... 680
Recording prompts ... 679
Replay Menu ... 674
Route calls to ... 683
Settings ... 263, 659
Short code ... 683
Speak By Name ... 675
Speak By Number ... 676
Auto-Attendant *(continued)*
Supervised Transfer ... 671
Transfer to Auto Attendant ... 678
Unsupervised Transfer ... 677
Auto–Attendant
List ... 656
Settings ... 263, 659
Avaya Cloud Services ... 532
Avaya Push Notification ... 535
Avaya support ... 43

B

backup ... 105, 638, 644
Backup ... 729
backup and restore
disk space ... 641
backup and restore policy ... 639
barred calls ... 821
applying ... 821
overriding ... 822
Barring Calls ... 838
blind transfer ... 900
Break out ... 878
business partner locator ... 1269
Button
911 View ... 773
Call Steal ... 1117
Emergency View ... 773
button programming ... 174
user ... 205
Button programming ... 1082
buttons
actions ... 46
configuration ... 46
solution settings ... 46

C

Call
Auto-Attendant ... 683
call access control
location ... 423
Call Barring ... 838
Call Flow Management ... 45
call management ... 156, 158, 209, 254
4400/6400 ... 203
add extension ... 211
announcements ... 197
auto attendant ... 257–260
button programming ... 174
call settings ... 175
create from template ... 159, 210
dial in ... 204
do not disturb ... 196
edit extension
common fields ... 211

telephony *(continued)*
edit extension *(continued)*
H323 VoIP ... 217
IP DECT ... 227
SIP T38 fax ... 225
edit user
multiline options ... 181
telephony ... 181
edit user advanced ... 202, 203
export users ... 158
extensions ... 210
forwarding ... 186
group membership ... 194
groups ... 229
add groups ... 230
announcements ... 249
fallback ... 239
group settings ... 230
overflow ... 237
queuing ... 234
SIP ... 252
voice recording ... 248
voicemail ... 242
hunt group ... 202
import users ... 158
menu programming ... 201–203
mobility ... 190
personal directory ... 199
provision extensions ... 210
provision users ... 159
short codes ... 185
SIP ... 200
source numbers ... 204
T3 Telephony ... 202
telephony ... 174
call log ... 183
supervisor settings ... 178
TUI ... 184
template management ... 159
users ... 157, 159, 160
voice recording ... 194
voicemail ... 168
Call Management ... 45
Conference ... 702
call recordings
user playback ... 205
Call Records ... 1245
call reporting ... 205
call routes
incoming ... 78
outgoing ... 79
call steal ... 912
Call Steal
Button ... 1117
Callflow ... 698, 705
Auto-Attendant ... 652
Calling Number Verification ... 959, 961–963, 966
centralized licensing ... 792
centralized media manager
audit trail ... 633
Centralized Media Manager ... 708, 709
recordings ... 635
certificate ... 40
certificate management ... 758
overview ... 758
Windows certificate store ... 760
certificate support ... 763
file import ... 769
file naming and format ... 763
identity certificate ... 764
signing certificate ... 767
trusted certificate store ... 766
certificates ... 569, 590
general ... 139
change Linux password ... 151
change login password ... 49
change root password
settings ... 151
cloud ... 849
authorization ... 849
Codec renegotiation ... 404
codec selection ... 950
COM ... 729
Conference
Add a system conference ... 700
Auto-Attendant ... 263, 659
Deleting a system conference ... 701
Direct By Conference ... 263, 659
Editing a system conference ... 701
Personal Meet-Me PIN ... 696
System Conference settings ... 702
System Conferences ... 700
User controls ... 687
Conference ID ... 689
conferences ... 254
Conferences ... 45
Conferencing ... 686
Capacity ... 688
configuration ... 625
configuration button ... 46
configuration field
DHCP pools IPv4 ... 480
DHCP pools IPv6 ... 483
extension ... 220
IP route ... 294
LAN settings IPv4 ... 480
LAN settings IPv6 ... 483
location ... 423
MS Teams line ... 348
MS Teams line VoIP ... 351
SIP engineering ... 355, 404
SIP VoIP ... 220
subscription ... 447, 726
time profile ... 787

IP security tunnel *(continued)*
tunnel
IP security tunnel 543
IKE policies 544
IPSec policies 545
main 543
L2TP tunnel 540, 542
configure 119
add system 119
convert to Select licensed system 121
remove system 121
connector 627
Consent 653
consolidate objects 49
Contact Center 532
Convert to...
Subscription 121
courses 1269
create from template
extensions 210
users 159
CTI
Subscription 728
Customer Operations Manager 729

D

dashboard 64, 125
Dashboard 65
data sets 642
date
settings 148
Date 783
Manual 786
System Status 785
Daylight Saving Time 784
daylight-saving
location 423
debug logs 135
DECT R5 36
Default
TTS language 651, 655
default gateway 146
delete
template 83
Delete 63
Auto–Attendant 657
Delete multiple 63
Multiple Auto–Attendants 657
Recording 715
System Conference 701
Destination
Auto-attendant 683
DHCP pools
IPv4 480
IPv6 483
Dial By Conference 666
Dial By Name 667
Recording name prompts 681
Dial By Number 669
dial in 204
Dial To Record Greeting 263, 659
Direct By Conference 263, 659
Direct By Number 263, 659
directory services 506
HTTP 510
LDAP 506
disk usage 642
Display
Auto-Attendants 656
DNS
IPv4 477
IPv6 483
Subscription 731
do not disturb 196
download
recordings 205
template 83
Download 135
Recording 714
download configuration 108
DST 784
location 423
DTag 971
DTMF 951

E

E1 line 357
E1 PRI channels 363
E1 PRI line 357
E1 short codes 363
E1 R2 line 365
E1–R2 advanced 369
E1–R2 channels 367
E1–R2 MFC group 369
E1–R2 options 365
edit
template 83
Edit
Auto–Attendant 656
Daylight Saving Time 784
Edit multiple entries 62
Quick edit 61
System Conference 701
edit user
multiline options 181
telephony 181
edit user advanced
4400/6400 203
hunt group 202
menu programming 202, 203
T3 Telephony 202
Email alarm 774

embedded call reporting 205
Emergency Call
System Alarm 774
Emergency View 773, 1142
enable 109
enable IPv6 146
Enable local recording 679
Enable Local Recording 263, 659
End of support 33
erase
template 83
Erase 63
Erase multiple 63
erase configuration 129
expansion
link 122
Export
Audit Trail 717
export users 158
extension 209
add extension 211
analog 214
create from template 82
edit extension
common fields 211
H323 VoIP 217
IP DECT 227
SIP T38 fax 225
save as template 81
template management 209
templates 81
Extension
Emergency Call Indication 773
extension configuration fields
SIP VoIP 220
extensions
create from template
provision extensions 210
Extensions 45

F

failed server
restore 646
Fallback 652
Fallback Action 267, 663
fax over SIP 952
file manager 601
File Manager 45
Filter 60, 712
firewall
settings 152
firewall profile 281
Firewall Profiles 45
forums 1269
forwarding 186

G

general
backup and restore 141
EASG settings 142
media manager 145
settings 137
voicemail settings 142
web control 141
Gmail integration 610, 833
Google Storage 720
Google TTS 651, 655
granular access 41
Greeting 263, 659
Pre-recorded 680
Short code 679
TTS 681
group
rights group 41
group membership 194
group operation 883
groups 229
add groups 230
announcements 249
fallback 239
group settings 230
overflow 237
queuing 234
setup wizard 77
SIP 252
voice recording 248
voicemail 242
Groups 45

H

H.323
setup wizard 70
Headers
SIP 971
help 43
Help 1268
hold music
setup wizard 74
Hold Reminders 956
hold scenarios 952
host name 146
Hot desking 878
HTTP server 150

I

ICU 64, 66
import users 158
inactivity timeout 49
incoming call
call scenarios 946

incoming call route 283
add 283
destinations 291
general settings 286
MSN configuration 293
voice recording 289
Incoming call route
Auto-attendant 683
incoming call routes
setup wizard 78
Incoming Call Routes 45
incoming calls
media path connection 944
increase
root partition 150
initial configuration utility 64, 66
Internal call
Auto-attendant 683
Intrusion 834
IP address 146
IP Office 49
proxy 49
SIP extension 220
IP Office Manager 45
launch 602
IP route
configuring 744
IPv4 294
IP Routes 45
IP security tunnel 543
IKE policies 544
IPSec policies 545
main 543
IPSec 540
IPv4
DHCP Pools 480
LAN settings 480
IPv6 34
DHCP Pools 483
DNS 483
LAN settings 483
location 423
SIP extension IP address 220
IPv6 address 146

K

Keepalives 404
knowledgebase 43

L

L2TP 540
L2TP tunnel 540
L2TP 542
PPP 542
LAN
LAN *(continued)*
network topology 495
settings 148
VoIP 487
LAN settings
IPv4 480
IPv6 483
LAN1 479
LAN2 501
Language
Auto-Attendant 650
TTS default 651, 655
LDAP 89, 852
connect to directory service 90
manage user provisioning rules 95
synchronize user fields 92
view jobs 95
LDAP synchronization
creating a user provisioning rule 853
performing 852
Leave Message 670
license
configuring 790
license file
uploading 799
license migration 804
license source 122
licenses 296
licensing
enterprise branch 802
setup wizard 77
licensing server 299
line 303
ACO line 305
ACO Line VoIP 307
ACO T.38 fax 309
add line
analog line 311
analog line options 313
analog line settings 311
call details 384
H323 line 324
H323 line short codes 327
H323 line VoIP 325
H323 line VoIP settings 328
IP DECT gateway 331
IP DECT line 331
IP DECT VoIP 333
IP Office line 335, 336
IP Office line short codes 341
IP Office line T38 Fax 344
IP Office line VoIP settings 341
Session Manager 414
SIP advanced 398
SIP Credentials 397
SIP line 376, 377
SIP T.38 fax 395

add line *(continued)*
add line *(continued)*
SIP transport ... 381
SIP VoIP ... 391
SM line ... 414, 417, 421
T38 fax ... 421
VoIP ... 417
BRI line
add line
channels ... 324
line settings ... 320
MS Teams line ... 348
PRI trunks ... 356
SIP DECT base ... 346
SIP DECT line ... 345
SIP DECT VoIP ... 347
line configuration fields
MS Teams line ... 348
MS Teams line VoIP ... 351
SIP engineering ... 355, 404
lines
setup wizard ... 78
Lines ... 45
link expansions ... 122
load
template ... 84
Local Media Manager ... 709
Local recording ... 679
Local Recording ... 263, 659
location ... 640
Location ... 739
location configuration fields ... 423
locations ... 423
address ... 426
Locations ... 45, 784
Log files ... 729
logging level ... 49
login
certificate ... 40
Login ... 39
login password
change ... 49
logout
inactivity timeout ... 49
Logout ... 41
logs ... 134
Loop Count ... 263, 659

M

madn ... 1162
Manager
Time ... 783
Manuals ... 1268
Maximum Inactivity ... 263, 659
Media Archival Solution ... 709
media manager ... 625, 628, 630
Media Manager ... 627, 631
Centralize ... 709
Centralized Media Manager ... 708
Local ... 709
Subscription ... 728
media path connection ... 944
Media Preference ... 711
Media Retrieval Preference ... 711
Menu Announcement ... 263, 659
menu bar ... 45
Menu Loop Count ... 263, 659
menu programming ... 201
4400/6400 ... 203
hunt group ... 202
T3 Telephony ... 202
menus ... 43
message waiting indication ... 855
Microsoft Teams ... 96
Migrate
Subscription ... 733
migrating ADI licenses ... 804
migration ... 630
mobility ... 190
Modes ... 37
Modify
Auto-Attendant ... 656
move ... 912
MS Teams
connect to directory service ... 97
manage user provisioning rules ... 101
synchronize user fields ... 98
view jobs ... 101
MS Teams line ... 348
VoIP ... 351
multiple call appearance ... 1162
music on hold
alternate source ... 779
system source ... 779

N

name
template ... 84
Name
Auto-Attendant ... 263, 659
Match Order ... 263, 659
Recording name prompts ... 681
new
template ... 82
New
Auto-Attendant ... 656
new in this release
R12.0 ... 33
R12.1 ... 34
R12.1 SP1 ... 36
No Match Prompt ... 263, 659
No User ... 847

NoCallerId alarm
suppressing ... 848
NoUser
Source Numbers ... 915
NTP ... 783
Number
Auto-Attendant ... 263, 659
Direct By Number ... 263, 659
Number Verification ... 959, 961, 963, 966
NUSN ... 915

O

obtain DNS from provider ... 146
offline mode ... 52
on-boarding ... 127
on-boarding: configuring SSL VPN ... 747
one-x portal
general ... 144
one-X Portal ... 45, 604
online mode ... 52
Optional Greeting ... 263, 659
optional services ... 132
outgoing call
call scenarios ... 938
outgoing call routes
setup wizard ... 79

P

packet capture
general ... 143
Panels ... 65
Park & Page ... 672
password
change ... 49
synchronization ... 49
Password
Change ... 42
password rules
settings ... 151
persistent gateway ... 36
personal directory ... 199
Personal Meet-Me ... 696
PIN
Personal Meet-Me ... 696
platform ... 125, 126
launch SSA ... 127
logs ... 134
service commands ...
erase security settings ... 129
reboot ... 128
settings ... 137, 146
system ... 132, 146
updates ... 136
platform view ... 131
Platform View
Platform View *(continued)*
Software Repositories ... 138
PLDS licensing ... 790
Ports
Subscription ... 732
Pre-recorded prompt files ... 680
preferences ... 49
user ... 43
Preferences
Voicemail Pro ... 45
prefix ... 146
PRI trunks
E1 line ... 357
E1 PRI channels ... 363
E1 short codes ... 363
E1 R2 line ... 365
E1–R2 advanced ... 369
E1–R2 channels ... 367
E1–R2 MFC group ... 369
E1–R2 options ... 365
T1 line ... 371
T1 channels ... 373
US T1 line ... 371
T1 PRI line ... 405
T1 ISDN ... 406
T1 ISDN call by call ... 412
T1 ISDN channels ... 409
T1 ISDN special ... 412
T1 ISDN TNS ... 411
Privacy ... 834
Consent ... 653
Programmable buttons ... 1082
Prompt
Name prompts ... 681
No Match Prompt ... 263, 659
Pre-recorded ... 680
Short code ... 679
TTS ... 681
Prompts
Announcements
Text-to-Speech ... 650
Text-to-Speech ... 650
protocol version
TLS minimum ... 49
provision extensions ... 210
provision users ... 159
proxy ... 49, 88

Q

Quick Reference Guides ... 1268

R

R12.1 ... 34
R12.1 SP1 ... 36
RAS ... 429

RAS *(continued)*
add RAS ... 429
Receptionist
Subscription ... 728
record consolidation ... 51
Recording
Consent ... 653
Delete ... 715
Download ... 714
Recording prompts ... 679
recordings ... 628
Centralized Media Manager ... 635
user playback ... 205
Recordings
Archive ... 719
Max retention ... 709
Playing ... 713
Remote access ... 729
Remote hot desking ... 878
remote operations ... 536
remote server ... 87
add remote server ... 87
remote server connection ... 644
remove
template ... 83
Remove ... 63
Remove multiple ... 63
rename
template ... 84
Replay Menu ... 674
Request Methods
SIP ... 970
Reseller ... 1268
resilience ... 121
Response Methods
SIP ... 971
restore ... 105, 638, 645
Restore ... 729
Retention ... 709
Retrieval Preference ... 711
retrieve ... 912
RFC ... 968
rights group ... 41
Ringback tone ... 955
Rocky Linux ... 33

S

sales ... 1269
save
save as template ... 81
Save to IP Office ... 52
schedule jobs ... 86
SDKs ... 1269
Search ... 60
security ... 573
rights group ... 41
security *(continued)*
service users ... 41
Security ... 45
security field
rights groups
configuration ... 584
group details ... 583
security administration ... 585
system status
external ... 588
HTTP ... 589
security administration ... 586
Telephony APIs ... 586
web services ... 586
security manager
certificates ... 590
service users ...
synchronize security database ... 589
security settings
general ... 573
rights groups ... 583
security services ... 581
system ... 577
system details ... 577
unsecured interfaces ... 579
security warning ... 49
self-administration ... 205
server edition
record consolidation ... 51
server edition licenses
distributing ... 792
server menu ... 124
dashboard ... 125
download configuration ... 130
initial configuration ... 129
logs ... 134
on-boarding ... 127
platform ... 125, 126
launch SSA ... 127
service commands ...
erase security settings ... 129
reboot ... 128
settings ... 137
system ... 132
updates ... 136
platform view ... 131
service commands ... 128
view upgrade report ... 130
Server Name Indication ... 404
service ... 132, 849
TCP Tunnels ... 444
service commands ... 128
erase configuration ... 129
service users ... 41, 561
synchronize security database ... 589
services ... 432
add normal, WAN, or internet service ... 433

services *(continued)*
add SSL VPN ... 441
Services ... 45
Set All Nodes
Subscription ... 121
set login banner
general ... 144
settings
security settings ... 573
system ... 138
systems ... 139
Settings
Auto-Attendant ... 263, 659
setup wizard ... 64, 76
auto attendant ... 74
groups ... 77
H.323 ... 70
hold music ... 74
incoming call routes ... 78
LAN settings ... 66
licensing ... 77
lines ... 78
outgoing call routes ... 79
SIP ... 70
system ... 66
users ... 77
voicemail ... 74
VoIP ... 70
SHAKEN ... 959, 961, 963, 966
Short code
Auto-attendant ... 683
Short Code
Auto-attendant prompt ... 679
short code feature
auto intercom deny off ... 997
auto intercom deny on ... 997
short codes ... 185
add system short code ... 445
Short Codes ... 45
Simultaneous ... 911
SIP ... 200, 970
Headers ... 971
Hold Reminders ... 956
Request Methods ... 970
Response Methods ... 971
RFC ... 968
Ringback tone ... 955
setup wizard ... 70
STIR/SHAKEN ... 959, 961, 963, 966
Tag length ... 971
SIP engineering ... 355, 404
SIP extension
VoIP settings ... 220
SIP line
Codec renegotiation ... 404
Keepalives ... 404
SNI ... 404
sip line appearances ... 388
SIP messaging ... 950
SIP prefix ... 941, 944
SIP REFER ... 954
SIP trunk
configuring ... 924
overview ... 924
sip uri ... 385
SLIC ... 404
SMDR ... 478, 1245
examples ... 1253
field descriptions ... 1248
SNI ... 404
SNMP
add SNMP traps ... 471
SNMP settings ... 469
SNMP alarm ... 774
SNTP ... 783
SoftConsole
Subscription ... 728
Software Repositories ... 138
solution ... 85
actions ... 104, 110
add system ... 119
application server ... 102
backup ... 105
configure ... 119, 121
convert to Select licensed system ... 121
download configuration ... 108
LDAP user synchronization ... 90, 92, 95
MS Teams synchronization ... 97
MS Teams user synchronization ... 98, 101
remote operations management ... 109
remove system ... 121
restore ... 105
schedule jobs ... 86
server menu ...
on-boarding ... 127
solution settings ... 86
synchronize APNP system-ID ... 108
synchronize APNS configuration ... 108
synchronize service user and system password ... 107
synchronize single sign-on configuration ... 107
transfer ISO ... 106
upgrade ... 106
user synchronization using LDAP ... 89
user synchronization using MS Teams ... 96
Solution ... 45
solution menu ... 43
solution objects ... 43
solution settings ... 86
proxy ... 88
remote server ... 87
add remote server ... 87
solution settings button ... 46
Sort ... 60
source numbers ... 204

Source Numbers 913
Speak By Name 675
Recording name prompts 681
Speak By Number 676
Speech AI 263, 651, 655, 659
Speech Voice 263, 659
SRTP 571
Station Message Detail Reporting 1245
examples 1253
field descriptions 1248
steal 912
Steal
Button 1117
STIR 959, 961, 963, 966
subinterface 146
subnet address
location 423
subnet mask 146
subscription
error mode 730
expiry 730
grace period 730
setup wizard 64, 76
Subscription
DNS 731
Internet Access 731
IP Route 731
Migrate to 733
Ports 732
Time Source 731
subscription configuration fields 726
Subscription mode 121
subscriptions 447
Subscriptions 45
Applications 728
CTI 728
Media Manager 728
Receptionist 728
SoftConsole 728
Telephony User 727
Telephony User Plus 727
Trial Mode 727
Unified Communications User 727
User Subscriptions 727
supervised transfer 900
Supervised Transfer 671
support 1269
Avaya 43
supported browsers 37
synchronization
password 49
user 49
synchronize APNP system-ID 108
synchronize APNS configuration 108
synchronize single sign-on configuration 107
syslog
general 138
Syslog alarm 774
syslog event viewer 135
system 451
Access Control Lists 506
Avaya Cloud Services 532
Contact Center 532
directory services 506
HTTP 510
LDAP 506
DNS 477
LAN 487, 495
LAN1 479
LAN2 501
network topology 495
remote operations 536
settings 145
setup wizard 66
SMDR 478
SMTP 476
system events 469
telephony 512
call log 528
MS Teams 527
park and page 521
SM 526
tones and music 522
TUI 529
voicemail 461
VoIP 487, 501
VoIP Security 503
System 45
System Administrator 1268
System Alarm 774
System Conference
Add 700
Delete 701
Edit 701
Settings 702
System Conferences 700
system configuration fields
DHCP pools IPv4 480
DHCP pools IPv6 483
IP route 294
LAN settings IPv4 480
LAN settings IPv6 483
system directory 449
add directory entry 449
System Directory 45
system DNS 146
system events 756
system identification
settings 152
System Phone 786
System Preferences 45
system security fields
rights groups
configuration 584

system status *(continued)*
rights groups *(continued)*
group details ... 583
security administration ... 585
system status
external ... 588
HTTP ... 589
security administration ... 586
Telephony APIs ... 586
web services ... 586
system settings ... 270
account code ... 272, 273
ACO line ... 305
ACO Line VoIP ... 307
ACO T.38 fax ... 309
add line
analog line ... 311
analog line options ... 313
analog line settings ... 311
call details ... 384
H323 line ... 324
H323 line short codes ... 327
H323 line VoIP ... 325
H323 line VoIP settings ... 328
IP DECT gateway ... 331
IP DECT line ... 331
IP DECT VoIP ... 333
IP Office line ... 335, 336
IP Office line short codes ... 341
IP Office line T38 fax ... 344
IP Office line VoIP settings ... 341
SIP advanced ... 398
SIP Credentials ... 397
SIP line ... 376, 377
SIP T.38 fax ... 395
SIP transport ... 381
SIP VoIP ... 391
SM line
Session Manager ... 414
T38 fax ... 421
VoIP ... 417
add RAS ... 429
alternate route selection ... 275
add alternate route ... 275
authorization code ... 280
add authorization code ... 280
Avaya Push Notification ... 535
BRI line
add line
channels ... 324
line settings ... 320
DNS ... 477
firewall profile ... 281
incoming call route ... 283
add ... 283
destinations ... 291
general settings ... 286
add WAN port *(continued)*
incoming call route *(continued)*
MSN configuration ... 293
voice recording ... 289
licenses ... 296
licensing server ... 299
line ... 303
locations ... 423
address ... 426
PRI trunks
E1 line ... 357, 363
E1 R2 line ... 365, 367, 369
T1 line ... 371, 373
T1 PRI line ... 405, 406, 409, 411, 412
RAS ... 429
service ...
TCP Tunnels ... 444
services ... 432
add normal, WAN, or internet service ... 433
add SSL VPN ... 441
short codes ... 445
add short code ... 445
SIP DECT base ... 346
SIP DECT line ... 345
SIP DECT VoIP ... 347
SNMP
add SNMP trap ... 471
SNMP settings ... 469
system ... 451
Access Control Lists ... 506
Avaya Cloud Services ... 532
Contact Center ... 532
directory services ... 506, 510
LAN network topology ... 495
LAN VoIP ... 487
LAN1 ... 479
LAN2 ... 501
remote operations ... 536
SMDR ... 478
SMTP ... 476
system events ... 469
telephony ... 512
voicemail ... 461
VoIP ... 501
VoIP Security ... 503
system directory ... 449
add directory entry ... 449
telephony ...
call log ... 528
MS Teams ... 527
park and page ... 521
SM ... 526
tones and music ... 522
TUI ... 529
time profiles ... 537
add time profile ... 537
user rights ... 546

add WAN port *(continued)*
user rights *(continued)*
add user right ... 546–554
WAN port ... 556
add WAN port
sync Frame Relay ... 557
sync PPP ... 556
System Settings ... 45
System Status Application ... 127

T

T1 line ... 371
T1 channels ... 373
US T1 line ... 371
T1 PRI line ... 405
T1 ISDN ... 406
T1 ISDN call by call ... 412
T1 ISDN channels ... 409
T1 ISDN special ... 412
T1 ISDN TNS ... 411
Tag length ... 971
TCP Tunnels ... 444
Technical Bulletins ... 1269
telephony ... 174, 512
call log ... 183, 528
call settings ... 175
MS Teams ... 527
multiline options ... 181
park and page ... 521
SM ... 526
supervisor settings ... 178
tones and music ... 522
TUI ... 184, 529
Telephony User ... 727
Telephony User Plus ... 727
template
add ... 82
analog trunk ... 807, 808
create user/extension ... 82
creating ... 807
delete ... 83
download ... 83
edit ... 83
rename ... 84
save as template ... 81
upload ... 84
template management ... 159
templates ... 81
Text-to-Speech ... 263, 650, 659
Recording a Prompt ... 681
time
settings ... 148
Time ... 783
Manual ... 786
Subscription ... 731
System Status ... 785
time offset
location ... 423
time profile configuration fields ... 787
time profiles ... 537
add time profile ... 537
Time Profiles ... 45
time zone
location ... 423
timeout ... 49
TLS
minimum protocol ... 49
training ... 1269, 1270
transfer ... 900
transfer ISO ... 106
transfer return ... 900
Transfer to Auto Attendant ... 678
Transport Protocols
SIP ... 970
Trial Mode
Subscription ... 727
trunk templates ... 806
trunks
setup wizard ... 78
TTS ... 650
Enable ... 651, 655
Recording a prompt ... 681
Speech AI ... 263, 659
Tunnel ... 540
tunnel configuration fields ... 540, 542–545
twinning ... 842

U

UCM ... 33
Unified Communications Module ... 33
Unified Communications User ... 727
unsupervised transfer ... 900
Unsupervised Transfer ... 677
upgrade ... 106, 107
upload
template ... 84
use DHCP ... 146
use DHCPv6 ... 146
use proxy ... 49
user ... 160
button programming ... 205
create from template ... 82
No User ... 847, 848
preferences ... 49
save as template ... 81
self-administration ... 205
subscriptions ... 447
suppressing NoCallerId alarm ... 848
templates ... 81
web self-administration ... 205
User
Call Barring ... 838

User *(continued)*
Edit multiple entries ... 62
NoUser Source Numbers ... 915
Recordings ... 710
Source Numbers ... 913
User Guides ... 1268
user management overview ... 831
user portal ... 205
user preferences ... 43
user rights ... 546
add user right
button programming ... 548
forwarding ... 554
short code ... 547
telephony ... 548
call log ... 551
call settings ... 549
multiline options ... 551
supervisor settings ... 550
user ... 547
user rights membership ... 552
voicemail ... 553
User Rights ... 45
users ... 157
actions ... 158
announcements ... 197
button programming ... 174
create from template
provision users ... 159
dial in ... 204
do not disturb ... 196
edit user
multiline options ... 181
telephony ... 181
edit user advanced ... 202, 203
export users ... 158
forwarding ... 186
group membership ... 194
import users ... 158
menu programming ... 201
4400/6400 ... 203
hunt group ... 202
T3 Telephony ... 202
mobility ... 190
personal directory ... 199
setup wizard ... 77
short codes ... 185
SIP ... 200
source numbers ... 204
telephony ... 174
call log ... 183
call settings ... 175
supervisor settings ... 178
TUI ... 184
template management ... 159
user ... 160
voice recording ... 194
telephony *(continued)*
voicemail ... 168
Users ... 45

V

View
Auto-Attendants ... 656
Viewing recordings ... 712
voice recording ... 194
Voice Recording Library ... 708
Voice Recordings
Archive ... 719
voicemail ... 168, 461
setup wizard ... 74
Voicemail Pro
Auto-Attendant ... 649
call flow management ... 618
Call Flow Management ... 45
system preferences
alarms ... 615
backup config ... 617
email ... 607
general ... 605
Gmail integration ... 610
housekeeping ... 611
outcalling ... 613
SNMP alarm ... 612
Syslog ... 615
user group ... 617
voicemail recording ... 614
System Preferences ... 45
Time ... 783
VoIP ... 501
setup wizard ... 70
VoIP Security ... 503

W

WAN port ... 556
sync Frame Relay ... 557
sync PPP ... 556
warning
security warning ... 49
Watchdog
general ... 144
web control ... 125, 126
Web Control
Software Repositories ... 138
web control menus ... 131
web license manager ... 624
Web License Manager ... 791
web manager
logging level ... 49
preferences ... 49
web self-administration ... 205
WebLM ... 791

WebLM *(continued)*
installing a license file 798
WebLM host ID 798
WebRTC 619
media gateway settings 621
SIP server settings 620
system settings 619
websites 1269
widgets 64
Widgets 65
WINS 477
Wireless DECT R5 36
wizard 64