Avaya IP Office™ Platform Feature Description

Release 12.1
Issue 27
March 2025

© 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 9
- **Chapter 1: Avaya IP Office™ Platform overview** 10
  - IP Office editions 10
- **Chapter 2: What's New** 12
  - New in IP Office Release 12.0 12
  - New in IP Office Release 12.1 13
  - New in IP Office Release 12.1 SP1 15

Part 2: Features 16
- **Chapter 3: Basic Call Handling** 17
  - Automatic Callback 17
  - Distinctive ringing 17
  - Call screening 18
  - Forwarding 18
    - Coverage to Operator 19
    - Follow Me 19
    - Forward Hunt Group 19
    - Forward On Busy 19
    - Forward On No Answer 20
    - Forward Unconditional 20
    - Unconditional Forward To Voicemail 20
  - Hold 20
    - Toggle Calls 20
    - Hold Call Waiting 21
    - Park 21
  - Personalized ringing 21
  - Tones 21
  - Transfer 22
  - Ring tone on transfer 22
- **Chapter 4: Advanced Call Handling** 23
  - Absence text 23
  - Call recording 24
  - Call tagging 25
  - Call waiting 25
  - Coaching intrusion 25
  - Conferencing 26
  - Conference Join 28
  - Dial On Pickup 28
  - Delayed Dial On Pickup 28
  - Do Not Disturb 28

Emergency 911 call ... 29
Hunt Group Enable/Disable ... 29
Inclusion ... 29
Off Hook Station ... 30
Pickup ... 30
User Privacy ... 30
Reclaim Call ... 31
Relay On/Off/Pulse ... 31
Restrict Network Interconnect ... 31
Chapter 5: Call administration features ... 33
Coverage to Operator ... 33
Dial Emergency ... 33
Dial plan ... 34
Direct Inward Dialing ... 34
Maximum call length ... 34
Paging ... 35
Transferable dial out privilege ... 35
Chapter 6: Contact center features ... 36
Account codes ... 36
Acquire Call ... 37
Hold music ... 37
Agent login ... 38
Monitor calls ... 38
Chapter 7: Outbound calling ... 39
Authorization codes ... 39
Call barring ... 39
Idle line preference ... 40
Override call barring ... 40
Private Call ... 40
Chapter 8: Inbound calling ... 41
Incoming call routing ... 41
Time profiles ... 42
Chapter 9: Hunt groups ... 43
Announcements ... 43
Assign Call On Agent Answer ... 44
Night Service and Out of Service modes ... 44
Overflow groups ... 44
Queuing ... 45
Queue threshold alert ... 45
Voicemail operation ... 45
Chapter 10: IP Telephony features ... 46
Auto-create extensions ... 46

Avaya cloud authorization ... 46
Direct media path ... 47
Early media and PRACK support ... 47
Fast start ... 47
Fax transport ... 48
Inbound call directory name display ... 48
Out of band DTMF ... 49
PAI and privacy headers ... 49
Silence suppression ... 49
SIP features ... 50
Voice compression ... 53
Chapter 11: Branch telephony ... 55
Telephony services ... 55
Survivability for centralized users ... 56
Messaging ... 58
Chapter 12: Messaging features ... 59
Messaging feature comparison ... 59
Chapter 13: Mobility features ... 64
Hot Desking ... 64
Remote access features ... 65
Remote hot desking ... 65
Remote Worker ... 66
Telecommuter mode ... 69
Twinning ... 69
Fallback Twinning ... 70
Simplified Mobile Access ... 71
VPN Phone ... 71
Chapter 14: Network features ... 72
Alternate Route Selection ... 72
Auto Connect ... 73
Callback ... 73
Firewall ... 73
Internet Access ... 74
Network Numbering Schemes ... 75
Service Quotas ... 75
Time Profiles ... 75
Multisite networking ... 76
Networking services ... 78
Dial-Up Circuit Support ... 78
DHCP Server ... 79
Domain Name Service (DNS) Proxy ... 79
LAN/WAN Services ... 79
LAN to LAN Routing ... 80

Integral 10/100 Mbit Layer 3 Ethernet Switch..... 80
Leased Line Support..... 80
Remote Access Server..... 80
SSL/VPN Remote Access..... 81
Chapter 15: Phone features..... 83
Alerting/ring tone for covered calls..... 83
Call history..... 83
Caller ID..... 84
Centralized Personal Directory..... 84
Language..... 85
On Hook Dialing..... 85
Self-Administration..... 85
Visual voice..... 85
Chapter 16: Appearance buttons..... 87
Line appearance buttons..... 87
Call appearance buttons..... 87
Bridged appearance buttons..... 88
Call coverage buttons..... 88
Multiple Access Directory Number buttons..... 89
Chapter 17: Buttons, keys and lamps..... 90
Programmable buttons..... 90
Busy lamp field indicators..... 90
External call lamps..... 91
Message waiting lamps..... 91
Part 3: Applications..... 93
Chapter 18: User applications..... 94
IP Office User Portal..... 94
Avaya Workplace Client..... 94
Avaya one-X® Portal for IP Office..... 97
SoftConsole..... 98
Chapter 19: Administration applications..... 101
IP Office Manager..... 101
Server Edition Manager..... 102
Web Manager..... 104
System Status Application (SSA)..... 104
SysMonitor..... 105
Customer Operations Manager..... 106
SNMP Management Console..... 106
Chapter 20: Branch Systems..... 108
Centralized management..... 108
Centralized licensing..... 108
Voice mail systems..... 109

Avaya Aura® Session Manager 109
Avaya Aura® Communication Manager 109
Chapter 21: Avaya Contact Center Select overview 110
Part 4: Miscellaneous 112
Chapter 22: Standards 113
Regulatory standards 113
Networking protocol standards 115
Part 5: Further Help 120
Chapter 23: Additional Help and Documentation 121
Additional Manuals and User Guides 121
Getting Help 121
Finding an Avaya Business Partner 122
Additional IP Office resources 122
Training 123
Glossary 124

Part 1: Introduction

Chapter 1: Avaya IP Office™ Platform overview

The Avaya IP Office™ Platform is a cost-effective telephony system that supports a mobile, distributed workforce with voice and video on virtually any device. IP Office is an modular communications solution that scales up to 3000 extensions and 150 sites in a multi-site network with resiliency.

Match a deployment model to infrastructure needs from simple appliances to virtualized software in a data center with options in between. Improve customer experience and contact center agent efficiency with powerful, affordable multichannel functionality for voice, email and web chat. The solution combines collaboration software plus multichannel contact centers, networking, security and video.

IP Office provides a hybrid PBX with both Time Division Multiplexing (TDM) and IP telephony with trunk support, used in either mode or both concurrently. IP Office has data capabilities built-in, providing IP routing, switching and firewall protection, between LAN and WAN (LAN2).

In addition to basic telephony services and voicemail, IP Office offers both hard phone and soft phone options. Soft phone applications are designed to provide flexibility for remote workers and to allow workers to access telephony services, such as making and receiving calls, voicemail, and call forwarding from their computer or mobile device.

Related links

IP Office editions on page 10

IP Office editions

IP Office also offers advanced features such as audio and video conferencing and voice over IP to meet the evolving needs of small, medium, and large enterprises.

IP Office is available in many deployment models based on the size of the enterprise and the features required using one or all the following elements:

- IP Office 500 V2 (IP500 V2) control unit.
- Dedicated server PC running a Linux-based suite of IP Office software.
- Virtual servers running the Linux-based suite of IP Office software.

Edition	Platform	Business size (users)	Addresses business needs
Basic Edition	IP500 V2	Less than 25	Simple telephony and messaging capabilities only. SIP trunks but no IP telephones or applications.
Essential Edition	IP500 V2 Multiple servers can be networked to support different locations.	20 – 99	Simple telephony and messaging capabilities plus IP telephony.
Preferred Edition		21– 250	Essential Edition capabilities plus unified communications and advanced voicemail (Voicemail Pro).
Server Edition	Uses a Linux-based primary server to which additional servers can be added including virtualized servers and IP500 V2.	100 – 2000	Software based Preferred Edition.
IP Office Select		100 – 3000	Server Edition with increased scale and resiliency.
IP Office Subscription	IP500 V2	21– 250	Preferred Edition using per-month subscriptions rather than permanent licenses.
	Linux Server, IP500 V2 and Linux Expansion	100 – 3000	IP Office Select using per-month subscriptions rather than permanent licenses.

Related links

Avaya IP Office™ Platform overview on page 10

Chapter 2: What's New

This section describes the major changes and new features supported by IP Office.

Related links

New in IP Office Release 12.0 on page 12
New in IP Office Release 12.1 on page 13
New in IP Office Release 12.1 SP1 on page 15

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

What's New on page 12

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

What's New on page 12

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

What's New on page 12

Part 2: Features

Chapter 3: Basic Call Handling

This section lists some of the basic call handling features supported.

Related links

Automatic Callback on page 17
Distinctive ringing on page 17
Call screening on page 18
Hold on page 20
Personalized ringing on page 21
Tones on page 21
Transfer on page 22
Ring tone on transfer on page 22

Automatic Callback

A user can set an automatic callback two ways:

- When calling an extension that is busy, request a call when the extension becomes free.
- When calling an extension that only rings, request a call when the extension is next used.

Depending on the type of phone a user has, request a call back when free by dialing a short code if an internal busy tone is heard, selecting an option from an interactive menu or pressing a programmed DSS/BLF key. A user can also set a callback when free or a callback when next used using a short code without attempting a call.

This feature is available across both multisite and small community networks.

Related links

Basic Call Handling on page 17

Distinctive ringing

The system uses various ringing sequences to indicate call types. For example, internal and external calls can have different rings, called distinctive ringing.

On analog phones, the distinctive ringing sequences are adjustable. On digital and IP phones, distinctive ringing is fixed as follows:

- Internal call: Repeated single-ring
- External call: Repeated double-ring
- Ringback call: Single ring followed by two short rings

Ringing sequences work with the following call types:

- Calls returning from park
- Calls returning from hold
- Transferring calls
- Call back when free calls
- Voicemail ringback calls

This feature is available across both multisite and small community networks.

Related links

Basic Call Handling on page 17

Call screening

Users can screen for important calls and decide to answer a call or let it go to voice mail.

Users can screen incoming calls while the phone is in an idle state and listen to incoming calls transferred to voicemail. When an incoming call arrives at a phone and is directed to and answered by the voicemail system, the user automatically hears the caller on his or her phone speaker, but the caller cannot hear the user. Users can decide whether to answer the call or drop from the call and let the voicemail system continue to handle the call. A user cannot screen a call while he or she is on another call.

Related links

Basic Call Handling on page 17

Forwarding

Users can forward calls to another extension or external number including mobile devices.

Users can forward calls in a number of ways and if the call is not answered at the forward destination it will go to voicemail if enabled for the user and call supervision is available. Once the numbers have been entered, the user can toggle the forwarding to be active or not as required without having to reenter the numbers.

If the user is a member of a hunt group, some types of hunt group calls can also forward unconditionally. Users can select if forwarding is applied to external calls only, or all calls. Call forwarding is processed after do not disturb and follow-me conditions are tested.

Coverage to Operator

Administrators can configure an operator or a group of operators to provide coverage for external calls that would otherwise go to voicemail.

Unanswered calls are routed to an operator or a group of operators. For example, local government offices prefer to provide a personal service rather than voicemail.

Related links

Call administration features on page 33

Follow Me

Follow Me enables all the features that a user has set on their phone to follow them to another phone. Forwarding only forwards calls only, not phone settings.

When users are away from their desk at another work area, they can forward call settings from their main phone for calls that follow the user including Forward On Busy or No Answer.

User can set Follow Me either from their primary phone (Follow Me To) or from the phone where they want calls to be received (Follow Me From). Several people can have their phones forwarded to a one destination and if the phone has a display it will indicate who the call is for.

Related links

Basic Call Handling on page 17

Forward Hunt Group

Users can forward a hunt group to forward calls for a group. For example, in a sales or support environments where a number of people may be out of the office using mobile phones, this feature allows them to participate in the hunt group as if they are in the office.

Calls for a hunt group that the user belongs to can also follow forward unconditional. The hunt group must be set for either sequential or rotary ring type and if the call is not answered at the forward destination it will follow the hunt group call handling instead of going to voicemail.

Related links

Basic Call Handling on page 17

Forward On Busy

If enabled, this forward occurs when a user is busy and another call is routed to them, but the system does not forward calls for a hunt group that they may be a member of.

Users are considered to be busy when they are on a call, but depending on call waiting settings and key and lamp features, this may not be the case.

Related links

Basic Call Handling on page 17

Forward On No Answer

If a call rings for a user but the user doesn’t answer it within the configured answer time, the system forwards the call that has been indicating call waiting if enabled.

Related links

Basic Call Handling on page 17

Forward Unconditional

The system forwards all calls for the user to a number, but if a call is not answered within the configured answer time, the system sends the call to voicemail if enabled.

Related links

Basic Call Handling on page 17

Unconditional Forward To Voicemail

Users can divert all calls to voicemail even when a user's voicemail is not activated.

Related links

Basic Call Handling on page 17

Hold

Users can place calls on hold with optional hold music. A held call is presented back to the extension after a time out, set by the system administrator, so that held calls cannot be forgotten.

Related links

Basic Call Handling on page 17
Toggle Calls on page 20
Hold Call Waiting on page 21
Park on page 21

Toggle Calls

The system cycles each call that the user has on hold to their extension, presenting them one at a time to the user.

Related links

Hold on page 20

Hold Call Waiting

Combine hold and answer to hold an existing call and answer a waiting call through a one button press.

Related links

Hold on page 20

Park

As an alternative to placing calls on hold, users can park calls to be picked by another user.

Park is available on the user's phone, Avaya one-X® Portal for IP Office, Phone Manager and SoftConsole.

The system parks a call using a park slot number which can be announced over a paging system. The designated user can go to any phone and take the call by dialing the park slot number.

Phone Manager has 4 predefined Park buttons. On digital phones with DSS/BLF keys, it is possible to program park keys to indicate when there is a call in a particular park slot and allow calls to be parked or retrieved.

Administrators can determine how long a call remains parked before it is presented to the extension that originally parked the call.

Related links

Hold on page 20

Personalized ringing

Users can change the sound or tone of a phone’s ring.

On many digital phones, users can personalize the ringer sound. Changing the ringer sound does not alter the ring sequence used for distinctive ringing. This feature is local to the phone and not supported on all types of phones.

Related links

Basic Call Handling on page 17

Tones

The system generates the correct tones for the geography. These tones are generated for all extension types: analog, digital and IP.

Supported tones are:

- Normal, alternate, and secondary
- Busy
- Unobtainable
- Re-order
- Conferencing

Related links

Basic Call Handling on page 17

Transfer

Users can transfer a call in progress to either an internal extension or an external public number. The system places the caller on hold while it performs the transfer.

If the transferring user hangs up before the destination user answers, the system automatically transfers the call, called an unsupervised or blind transfer. Alternatively, a user can wait for the destination to be answered and announce the transfer before hanging up to complete the transfer, called a supervised transfer.

Unless restricted by the administrator, the system does not differentiate between internal or external call transfers.

Related links

Basic Call Handling on page 17

Ring tone on transfer

The transfer enquiry calls are presented to the recipient with an internal ring tone. If the user transferring the call completes the call when the call is still ringing, the ring tone changes as per the call being transferred. Customers have the choice of not using this configurable option and continue to operate as in Release 10 and prior releases.

Related links

Basic Call Handling on page 17

Chapter 4: Advanced Call Handling

This section lists some of the advanced call handling features supported.

Related links

Absence text on page 23
Call recording on page 24
Call tagging on page 25
Call waiting on page 25
Coaching intrusion on page 25
Conferencing on page 26
Conference Join on page 28
Dial On Pickup on page 28
Delayed Dial On Pickup on page 28
Do Not Disturb on page 28
Emergency 911 call on page 29
Hunt Group Enable/Disable on page 29
Inclusion on page 29
Off Hook Station on page 30
Pickup on page 30
User Privacy on page 30
Reclaim Call on page 31
Relay On/Off/Pulse on page 31
Restrict Network Interconnect on page 31

Absence text

Users can set absence text on their phone to inform other internal users of their current status and likely availability.

Absence text is also available for users of standard analog phones, but it can only be displayed on selected display phones, Phone Manager and SoftConsole. Most supported feature phones give the option of adding text.

When a user has an absence text message set, call processing is not affected to the user and they still have the choice of using features like do not disturb and forwarding. Telephones that

support the interactive setting of absence text also display it on the users own phone for the benefit of people who come to their desk. There are 10 predefined strings and 1 custom string for absence text:

1. On vacation until
2. Will be back
3. At lunch until
4. Meeting until
5. Please call
6. Don't disturb until
7. With visitors until
8. With customer until
9. Back soon
10. Back tomorrow
11. Custom

All message text include the option to add a time, for example, message 4 plus `10:00` displays **Meeting until 10:00**. Text strings are localized to the system language.

This feature is available across both multisite and small community networks.

Related links

Advanced Call Handling on page 23

Call recording

Users can record a call and save the recording to the a voicemail mailbox, a group mailbox or the voice recording library.

When a caller provides detailed information like an address or phone number, the caller hears a warning message or tone that the call is being recorded in some countries. Where call recording is required for quality assurance, administrators can configure IP Office to automatically record a percentage of calls for later review.

Any call on any phone type can be recorded. Where notification of recording needs to be played, the system ignores voicemail port licensing if an insufficient number of voicemail channels have been licensed.

Related links

Advanced Call Handling on page 23

Call tagging

Call tagging displays a text message to provide additional information about the call on a user's phone or soft client when a call is presented to it.

Users tag calls when transferring calls from Soft Console to provide caller information they are not able to announce the call.

Users can add a tag to a call automatically using CTI and Voicemail Pro based on the incoming call route.

Note:

On some phones, displaying the tag may mean that it is not possible to display the usual call source and target information.

Related links

Advanced Call Handling on page 23

Call waiting

Users may not want callers to receive busy tone if they are on another call. Instead, callers hear a normal ring tone. Users hear an alert that there is a call waiting.

Users can decide to finish or hold the current call and answer the one that is waiting. The amount of information that is available about the call that is waiting depends on the type of phone the user has, or if they are using Avaya one-X® Portal for IP Office or a soft client.

Because the call waiting tone can be disruptive, for example during conference calls. Users can turn the feature on or off and even suspend it for a single call.

Related links

Advanced Call Handling on page 23

Coaching intrusion

Designated users can join an existing conversation on internal or external calls. This features also allows a user to interrupt a call to without the caller hearing the conversation.

Administrators and supervisors designate users with the Can Intrude setting. Users can join calls on any extension on the system, however, administrators can also designate users with the Cannot be Intruded setting, which prevents others from intruding on their calls.

On Essential and Preferred Edition systems, Silent Intrusion or Whisper Page can be effective in a scenario where a user intrudes into a call to whisper that a very important customer is waiting. The user hears the whisper while talking to the caller but the caller will not be able to hear the whisper.

Used in call center scenarios and with other applications between employees. Supports the interruption or inclusion of a supervisor on a live call to talk to an agent without the far-end caller listening to the conversation. This is useful when the agent needs coaching support/training or when the supervisor needs to intrude to give instructions to an agent. The caller may still talk to the agent, but the caller will not hear what the supervisor is saying. The agent will be able to hear both the caller and the supervisor.

The feature enables users on a call to “intrude” and listen depending on the configuration of the end users if Coaching Intrusion or Whisper Page is used. Coaching Intrusion and Whisper Page cannot be done on and idle user. It may be done for internal calls or with external calls. This feature is enable through the IP Office Manager for each user. Only authorized users can use the coach/whisper feature. The default setting is off.

Related links

Advanced Call Handling on page 23

Conferencing

Users can place calls on hold and a create a conference using either the telephone or desktop applications. Additional conference members may be added.

For ad-hoc conferencing, the system requires as many digital trunks/VoIP channels as external participants (as well as Preferred Edition for Meet-Me conferences).

Meet-Me capabilities require Preferred Edition for direct dial into a conference bridge with PIN code security. In an SCN network, only one centralized Preferred Edition license is required to host Meet-Me conferences at any of the sites. Conference IDs are also shared across the SCN sites.

Primary/Secondary Server

Each Primary and Secondary supports a local audio conference capability with the following capacities:

System Mode	Primary/Secondary server	Total Conference Channels	Maximum conference size	Total Conference Channels with ACCS
IP Office Server Edition	**Dell R240**	128	128	414
	HP DL360	256	256	825
	Dell R640	256	256	1650
	OVA	256	256	1650
IP Office Select	**Dell R640**	512	256	1650
IP Office Subscription	**OVA**	512	256	1650

IP500 V2 and Linux Expansion System

Each IP500 V2 and Linux Expansion System supports a local audio conference capability with the following capacities:

Expansion Platform	Total Conference Channels	Maximum conference size	Total Conference Channels with ACCS
Linux/OVA	128	128	128
IP500 V2	128	64	128

To initiate a conference, users dial the direct number allocated to the conference bridge, type in the PIN (require Preferred Edition and Voicemail Pro) if required. For ad-hoc conferences with a few participants, users can easily set up immediate conferences by calling all parties and bringing them to the conference bridge. With Avaya one-X® Portal for IP Office, the originator of the conference can keep control: the Caller ID number (and the associated name if recognized) of each participant is displayed. If required, they can selectively hang-up a specific participant. The system plays a single beep on entry and a double beep on exit. The owner of the conference may use their extension number as the conference ID. The owner of the conference has control of the conference with the ability to mute and drop calls of participants. All participants will hear the system Music on Hold (MOH) until the owner joins, and will hear MOH when the owner drops. Note that any internal party has the option to view and drop participants (not just the conference originator).

Users can record a personalized greeting for a conference (requires Preferred Edition and Voicemail Pro).

Users can record the conference using Avaya one-X® Portal for IP Office, digital or IP display phone or a short code (requires Preferred Edition and Voicemail Pro). To prevent unauthorized access to the conference bridge, PIN codes, Caller ID number screening as well as time and date profiles can be set-up using Voicemail Pro. One user can manage the conferencing bridge facility from any location.

Conference Restrictions

Conferencing has the following restrictions:

- Only two calls connecting through analog trunks are permitted in any single conference.
- Each external caller requires a digital trunk/VoIP channel (for example 1 T1 allows 23/24 external parties, 1 E1 allows 30 parties and a fully licensed VCM-64 allows 64 parties).
- There are no limits on the mix of internal and external calls in conference, but if all internal participants disconnect from the conference bridge, the external participants can be disconnected automatically by the system for added security (configurable system setting).
- System features such as call intrusion, call recording and silent monitoring all use conference resources, as does automatic recording if enabled. When any of these features are active the number of slots available for conference parties is reduced. For example, a conference call between 3 parties and being recorded will use 4 conference slots.

Related links

Advanced Call Handling on page 23

Conference Join

Conference Join feature allows two separate conferences to be joined into one single conference that contains all the previous participants of both the earlier conferences. Once the conferences have been joined it is not possible to revert to the two separate conferences again.

Related links

Advanced Call Handling on page 23

Dial On Pickup

By taking the phone off hook, users can automatically dial a specified extension.

Use this feature in unmanned reception areas or for door entry systems to allow visitors to easily gain assistance. This feature is also known as “Hotline”.

Related links

Advanced Call Handling on page 23

Delayed Dial On Pickup

If a phone is off-hook or the phone speaker is enabled and nothing is dialed for a configured time period in seconds, a defined extension is automatically dialled.

Use this feature in unmanned reception areas or for door-entry systems to allow visitors to easily gain assistance – visitors who know the desired number have the option to dial it, while other visitors can be routed to assistance after a short time-out. This feature can also be used as an emergency alert in a health care environment, for example, when a handset is lifted but no digits are dialed.

Related links

Advanced Call Handling on page 23

Do Not Disturb

Users can temporarily stop incoming calls ringing at a their phones.

This feature prevents users from receiving hunt group calls and gives direct callers either voicemail, if enabled, or a busy signal. Users can enable and disable Do Not Disturb (DND) from their phone or soft client.

Users can allow some calls to bypass the DND setting and ring the phone. For example a manager can add their assistant's extension number to the DND exceptions list. Both internal and external numbers can be on the exception list.

Related links

Advanced Call Handling on page 23

Emergency 911 call

Calls to numbers configured as emergency numbers override any call barring that would otherwise apply to the user making the call.

Related links

Advanced Call Handling on page 23

Hunt Group Enable/Disable

User can temporarily join or leave individual hunt groups, for example, to assist during call peaks.

Supervisors or administrators don't usually take calls but at times of high call traffic they can join a group to take calls and when the peak is over, leave the group to resume their regular tasks. Administrators configure users as members of hunt groups. A user can not arbitrarily join a hunt group that they have not been identified as a member of.

Related links

Advanced Call Handling on page 23

Inclusion

Selected users can intrude on calls that are already in progress.

When the intruding user joins a call, all parties hear a tone. The speech path is enabled between the intruding party and the called user; the other party is forced onto hold and will not hear the conversation. On completion of the intrusion, the called party speech path is reconnected to the original connected party. Administrators enable or disable Inclusion on a per user basis through the Manager.

Related links

Advanced Call Handling on page 23

Off Hook Station

Off-Hook Station is designed for users who want their analog phone to operate like digital or IP feature phone, to isolate the user's phone idle state from the Hook state. This is a useful feature when using Avaya one-X® Mobile or SoftConsole to control the phone state when using a headset on an analog phone and with call control and dialing from Avaya one-X® Mobile, or SoftConsole.

Related links

Advanced Call Handling on page 23

Pickup

Users can answer a call presented to another extension.

Call pickup scenarios include:

- Pick up any call ringing on another extension.
- Pick up a hunt group call ringing on another extension, where the user must be a member of that hunt group.
- Pick up a ringing call at a specified extension.
- Pick up any call ringing on another extension that is a member of the hunt group specified.

This feature is available across both multisite and small community networks.

Related links

Advanced Call Handling on page 23

User Privacy

Certain users need to be assured of confidential communication. These users must be protected from other users being able to see who is calling them and must be able to prevent their calls being picked-up. The Privacy Override Group field in user records, if enabled, bars other users from seeing call details or picking up the calls

User button privacy

When a User button is pressed to see who is connected to the user or to answer an alerting call, the system checks the Privacy Override Group configuration setting of the user. If the group is not configured or the user is in the list (Enabled/Disabled status is not checked), then DSS status will be shown.

Pickup protection

When a user tries to pick up another user's call then the Privacy Override Group setting is checked on the targeted user. If the group is not configured or the user is in the list then the pickup is allowed. The Enabled/Disabled status in group is not checked.

Related links

Advanced Call Handling on page 23

Reclaim Call

Users can recover, or reclaim, the last call at their phone that is ringing or is connected elsewhere.

If users miss a call that goes to voicemail or call coverage, they can get the call back while it is still being presented or connected through the system. This is a version of the Acquire Call feature that only applies to the last call at an extension.

Related links

Advanced Call Handling on page 23

Relay On/Off/Pulse

IP500 V2 systems have 2 independent switch outputs for controlling external equipment such as door entry systems.

Control switches using allocated handsets to open, close or pulse switches as required. Users can also control switches with Receptionist, SoftConsole and Voicemail Pro.

Related links

Advanced Call Handling on page 23

Restrict Network Interconnect

The Restrict Network Interconnect feature bars calls from being connected between private and public trunk interface groups.

India Toll Bypass Prevention

Indian telecom regulation states that the VoIP call should not be mixed with PSTN call if the call origination location and call targeting location are in different toll areas.

The India Toll Bypass Prevention feature ensures that the system is compliant with this regulation and allow calls to and from IP phones to connect to local PSTN public trunks only if the IP phone’s location is the same as the system location. The feature is enabled by default for the India locale and disabled by default for all other locales. This feature is available for Branch and SCN

deployments on IP500 V2 in Essential, Preferred and Select editions. No additional licenses are required.

Related links

Advanced Call Handling on page 23

Chapter 5: Call administration features

Related links

Coverage to Operator on page 19
Dial Emergency on page 33
Dial plan on page 34
Direct Inward Dialing on page 34
Maximum call length on page 34
Paging on page 35
Transferable dial out privilege on page 35

Coverage to Operator

Administrators can configure an operator or a group of operators to provide coverage for external calls that would otherwise go to voicemail.

Unanswered calls are routed to an operator or a group of operators. For example, local government offices prefer to provide a personal service rather than voicemail.

Related links

Call administration features on page 33

Dial Emergency

Dial Emergency is a short code and permits specific numbers to be dialed regardless of call barring or a logged out phone.

Related links

Call administration features on page 33

Dial plan

IP Office has a very flexible numbering scheme for extensions, hunt groups and feature commands. While the system has default numbering for feature codes and extensions, they can all be redefined. Default extensions and hunt groups have 3 digit numbers starting at 200 but these can be changed from 2 to 9 digits through the IP Office Manager. There is a default set of feature access short codes, but these can be changed to whatever the end user requires, within limits. This is useful for example if IP Office is replacing a system where DND was accessed by dialing *21, it is possible to change the short code to mimic the code of the replaced system.

In certain countries IP Office can support a secondary dial tone when an access digit is dialed, though this limits some functionality like Alternate Route Selection (ARS). IP Office can also be configured to work without line access digits, by analyzing digits as they are dialed and determining if they are for an internal number or should be sent out on a line - this is valuable in SOHO installations where users will not necessarily be used to dialing an access digit for an outside line.

Related links

Call administration features on page 33

Direct Inward Dialing

Direct Inward Dialing (DID/DDI) relies on the local phone exchange passing all or part of the dialed number to IP Office.

Call routing software routes the call to an individual phone or a group of phones. Use this feature to reduce the workload on a receptionist by giving staff members or departments individual numbers for direct calls. Typically, the extension or group number is the same as the digits supplied from the network, but IP Office can convert the number to another number as needed within limits.

In North America, T1 circuits are required for DID.

Related links

Call administration features on page 33

Maximum call length

Maximum call length allows the system to control the maximum duration of any call based on the dialed number. Use this feature to control calls to cellular networks or data calls made over the public network to ISPs.

Related links

Call administration features on page 33

Paging

Supervisors and administrators can broadcast audio messages to digital and IP phones with loudspeakers without having to install a separate paging system. Paging can be to individual phones or groups of phones.

Implementation engineers can configure analog extension ports to an external overhead paging system, usually through an adapter, so that a port can be included in a paging group to permit mixed phone and overhead paging.

Some digital and IP phones can answer a page by pressing a key while the page is going on, this terminates the page and turns it into a normal call.

Paging limits

System Mode	Platform	Maximum Paging Group Size
IP Office Server Edition	Dell R240	128
	Dell R640	512
	OVA[1]	512
IP Office Select	Dell R640	512
IP Office Subscription	OVA[1]	512
All	IP500 V2/V2A	64

- Paging groups that include users on a V2 Expansion are limited to 64 members.
- For paging groups that include SRTP endpoints, reduce the maximum size by 50%.

Related links

Call administration features on page 33

Transferable dial out privilege

Administrators and supervisors can grant outside line access to restricted phones, for example phones in public areas or conference rooms, to control external calls.

A privileged user, such as a supervisor, can transfer an outside line (secondary dial tone) to a user that does not have external dial out privileges.

Related links

Call administration features on page 33

Chapter 6: Contact center features

Related links

Account codes on page 36
Acquire Call on page 37
Hold music on page 37
Agent login on page 38
Monitor calls on page 38

Account codes

Through the call records, supervisors and administrators can group calls by account code for the purpose of call costing and tracking. Supervisors and administrators can also restrict outgoing calls by requiring users to enter valid account codes.

The system stores a list of valid account code numbers. When making a call or during the call, a user can enter the account code they want associated with that call. The system checks the account code against the list of valid codes and requests the user to reenter the code if it is not valid. For incoming calls, the Caller ID can be used to match it with an account code from the list of valid codes and report the account code with the call for billing.

Supervisors and administrators can designate users to use a forced account code requiring them to enter a valid account code before making external calls. Using short codes it is possible to identify certain numbers or call types as requiring a valid account code before permitting the call to proceed, for example long distance or international numbers. Analog phone users can only enter account codes before making a call or in response to an audible system prompt to enter a code when making the call.

Account codes can also be entered through the Avaya one-X™ Portal for IP Office and Phone Manager. A system wide setting determines whether Phone Manager will display a list of account codes from which the user can select the code required or will hide the account code list.

In all the cases above, the account code entered is included with the call details in the IP Office's call record output. (SMDR).

Related links

Contact center features on page 36

Acquire Call

The Acquire Call feature allows users to take over a call connected to another extension. This feature is also known as Call Steal.

Administrators can set Acquire Call as a short code or assign it to a button on a digital or IP phone with programmable buttons. This feature is affected by intrusion control settings: the user acquiring a call must be set to be able to intrude and the user whose call is being acquired must be set so it can be intruded.

Acquire Call works in two ways:

Without a number	Allows a user to reclaim a call that was ringing on their phone but has now gone elsewhere, for example to voicemail or a Forward No Answer destination. The Intrude settings are not checked. The user can reclaim the call even if it has been answered. If the last call to ring this user is no longer ringing or connected on the system, the feature will fail.
With a number	Where the number is the phone number of a user who currently has the call to be acquired. If the user has a call ringing or waiting Acquire Call will act like the Call Pickup Extension short code and the user executing Acquire Call will be connected to the oldest ringing/waiting call. If the user has a connected call with no call waiting and the Intrude settings of the two users allow it, the call will be connected to the user executing the Acquire Call and the other user will be disconnected. If the user does not have a call the feature will fail.

Related links

Contact center features on page 36

Hold music

Administrators can access up to 32 sources for music on hold (4 on IP500 V2 systems). A wide range of sources are supported, including on Linux systems up to four USB sources are supported.

A music source can be a locally stored single WAV file (default) or a local directory of WAV files. You can configure playback to start every time from the beginning of the file or directory, or to start from where it left off the last time.

Alternate music sources can be located on Server Edition Primary, Secondary, and expansion systems. Server Edition also supports centralized music on hold, where the Primary Server streams music to the Secondary Server and all expansion servers.

Related links

Contact center features on page 36

Agent login

Contact center agents must log in before they can make or receive calls.

Administrators and supervisors can set a login idle period to determine how long an extension can be idle before the user is automatically logged out, ensuring that an extension is not left logged in with calls going unanswered.

Related links

Contact center features on page 36

Monitor calls

Users can monitor another user's call by listening in.

This feature is not available by default; implementation engineers must enable it during system configuration. This feature includes an option to have a tone indicate when monitoring is in use. The user is only able to listen; they cannot speak during the conversation.

Related links

Contact center features on page 36

Chapter 7: Outbound calling

Depending on the type of business, calls need to be treated in a specific way, such as recorded against a project or client through the use of account codes.

A business may have several sites linked through a private network but certain users, like customer service agents, may need to be able to call colleagues in other offices when the network is busy, while other users wait for a line to come free. Least cost routes can automatically translate the internal number to a direct dial call over the public network while other users wait.

Authorization codes

Authorization codes allow a user to go to another extension on the system and make calls using their personal toll restrictions; this may grant the user greater or fewer privileges than the normal owner of the extension they use.

Authorization codes are independent of account codes, so the user has to enter both if the required by the system configuration. All entered codes are logged in SMDR.

Call barring

Supervisors and administrators can prevent or allow calls to certain numbers such as international numbers or premium rate numbers for individual users or on a system-wide basis.

The system supports call barring at many levels. Short codes can be used at the system or individual user level to block the external routing of specific numbers or types of numbers. Typically the barring short codes are set to return busy tone, however they could route the call to an alternate number or to a Voicemail service that returns a 'barred dialing message'.

Users can allocate short codes to a user rights template. The users can then apply the template to the users whose calls need restriction. Administrators can also bar the forwarding of calls to external numbers on a per user basis.

Idle line preference

Idle line preference allows the user to select a specific external line for companies that prefer to work in key system mode.

Going off hook selects the first idle line appearance and the user connects to an outside line.

Override call barring

Override Barring can allow numbers dialed from the directory, using redial, call log, button programming, short codes, and numbers manually entered to external numbers present in the public directory (System Directory, LDAP, HTTP) even though a barred short code has been matched against dialed digits.

Private Call

Users can set Private Call status using short codes or a programmed button.

Private calls cannot be recorded, intruded on, bridged into or monitored.

Chapter 8: Inbound calling

Related links

[Incoming call routing](#) on page 41
[Time profiles](#) on page 42

Incoming call routing

Intelligent call routing makes routing decisions based on any or all of the following criteria:

- Digits from the exchange such as DDI/DID or ISDN MSN
- Calling phone number or Caller ID or part of the number received such as an area code
- ISDN sub-address
- ISDN/PRI service type such as Voice Call or Data Call

For example, a DDI/DID call to a sales group can be handled differently depending on which part of the country the call is originating from.

Each incoming Call Route supports a secondary destination Night Service that can provide alternative routing for an incoming call based on time of day and day of week criteria, as well as calendar-based routing for specific dates.

Calls that cannot be routed to the configured destination are rerouted to a user-defined Fall Back destination. This can be particularly useful where calls are normally answered by an auto-attendant and a network fault occurs.

Where multiple call routes are set up to the same destination, a priority level can be associated with the call. The priority level determines a call's queue position in place of simple arrival time.

Note:

Calls already ringing a free extension are not considered queuing and are not affected by a high priority call joining a queue (unless the option Assign Call On Agent Answer is selected for that hunt group).

Supervisors can configure a Priority Promotion Timer to increase the priority of calls which have been in the queue for more than a defined time and add and optional tag to calls on the Incoming Call Route, which can be displayed on the alerting phone.

Related links

Inbound calling on page 41

Time profiles

Time profiles set the operational times for service. For example, a time profile could be set up to make Internet access available to staff only during lunch times.

Using time profiles it is also possible to define an alternative service to operate outside the operational hours of the main service. This option may be used to take advantage of alternative tariffs at off peak periods. Switching to this fallback service can also be controlled manually by dialing a secure short code from a handset. This can be particularly useful in allowing quick restoration of service in the event of an ISP failure. This feature also applies to days of the week or specific calendar dates.

Related links

Inbound calling on page 41

Chapter 9: Hunt groups

A hunt group is a collection of users, typically users handling similar types of calls, for example a sales department. An incoming caller wishing to speak to someone in a group can call one number and the call can be answered by any number of extensions that are members of the hunt group.

There are four ways a hunt group can process calls:

Sequential	One extension at a time sequentially, always starting at the top of the list.
Collective	All extensions in the hunt group simultaneously.
Rotary	Start with the extension in the list immediately following the extension that answered the last hunt group call.
Longest Waiting	Start with the extension that has been free for the longest time period.

Announcements

Use voicemail in conjunction with hunt groups to:

- Record all group related messages.
- Play an announcement when the hunt group is in Night Service or Out of Service mode.
- Play announcements while a call is held in a queue.

A broadcast option is available for internal voicemail. This feature changes the voicemail box operation so that the message notification will only be turned off for each hunt group member when they retrieve their own copy of the message. Hunt group announcements are separated from hunt group queuing and can be used when queuing is off. Hunt group announcements are supported by Embedded Voicemail and Voicemail Pro. Administrators and supervisors can set times for the first announcement, second announcement, and between repeated announcements.

Hunt groups in a small community network can include members located on other systems within the network.

Assign Call On Agent Answer

Supervisors can set the Assign Call On Agent Answer hunt group option to enable CTI applications to correctly report the details for the call that is alerting and ensures that the call at the head of the queue is always answered first.

Night Service and Out of Service modes

Outside normal operation a hunt group can be put into two special modes: Night Service and Out of Service.

Night Service mode

Users can switch in or out of Night Service mode by dialing the appropriate short code. Calls are presented to a Night Service group. This can be controlled automatically by setting a time profile which defines the hours of operation of the main group or manually using a phone feature code. During Night Service mode, the original hunt group is temporarily disabled. You can design callers to the hunt group to do any of the following actions:

- Pass to a Night Service Fallback group passing calls to a manned extension or external number.
- Be played the Out of Hours greeting if set in voicemail.
- Receive a busy tone.

Out of Service mode

Users control Out of Service mode manually from a phone. While in this mode, calls are presented to the Out of Service group. Night service fallback using a time profile is not applied to a hunt group set to Out of Service.

Overflow groups

Supervisors can designate an overflow group to take calls if all extensions in the hunt group are busy or not answered.

Supervisors can also set overflow time to stipulate how long a call will queue before passing to the Overflow Group. Overflow time can be set for individual calls and for all calls in the group. The system can change the status of users who do not answer a hunt group call presented to them. The user status can be set to Busy Wrap-up, Busy Not Available or Logged Out. The change of status can be set per user and per hunt group.

Queuing

Queuing allows calls to a hunt group to be held in a queue when all extensions in the group extension List are busy. When an extension becomes free the queued call is then presented. The definition of queued calls now includes ringing calls and calls waiting to be presented for ringing. The queue limit can be set to control the maximum number of calls to wait against a hunt group.

While queuing, if Voicemail is operational, the caller will be played the announcements for this hunt group.

Queue threshold alert

Supervisors and administrators can set an alert to occur at a selected analog extension port when the number of calls queued against a hunt group exceeds a threshold.

Typically the alert is a loud ringer or other alerting device. The alert does not present a call.

Voicemail operation

The system supports voicemail for hunt groups in addition to individual user voicemail mailboxes. 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.

Previously the unanswered calls to a hunt group were sent to voicemail when reached the group's no answer time. From 11.1FP1 onwards the unanswered calls are forwarded to the group's fallback destination, by configuring to an extension number, system short code or voicemail. The configuration is done through the **Group** > **Fallback** tab.

- **Voicemail On** is configured through **Group No Answer Destination** through **Group** > **Fallback**.
- **Voicemail Answer Time** is configured through **Group No Answer Time** through **Group** > **Fallback**.

Chapter 10: IP Telephony features

Related links

Auto-create extensions on page 46
Avaya cloud authorization on page 46
Direct media path on page 47
Early media and PRACK support on page 47
Fast start on page 47
Fax transport on page 48
Inbound call directory name display on page 48
Out of band DTMF on page 49
PAI and privacy headers on page 49
Silence suppression on page 49
SIP features on page 50
Voice compression on page 53

Auto-create extensions

Implementation engineers can configure IP Office to create extension entries for new IP phones added onto the local area network.

This feature should only be used when installing a new system or a large number of phones. It is automatically disabled 24-hours after being enabled.

Related links

IP Telephony features on page 46

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.

Related links

IP Telephony features on page 46

Direct media path

Direct media path allows the speech path between two IP extensions (after call setup) to be routed directly to each other. This allows the system to free up voice compression resources after establishing the end to end connection, allowing the resources to be used in the most efficient way.

Related links

IP Telephony features on page 46

Early media and PRACK support

IP Office supports in-band announcements such as:

- Branding from discount or bulk long distance providers
- Progress indications when extraordinary wait times are inherent in the call scenario, for example when trying to locate a cell phone
- Country-specific ring back and other progress tones
- Conferencing in the IP domain before call answer, for example, in call recording scenarios or for automatic dialers' conferencing in agents

Implementation engineers can configure SIP trunks to support early media by adding the **100rel to Supported** header in the **INVITE** parameter.

Related links

IP Telephony features on page 46

Fast start

Implementation engineers can configure fast start on an IP extension to reduce the protocol overhead allowing an audio path to be established more quickly.

Related links

IP Telephony features on page 46

Fax transport

IP Office supports Avaya proprietary and T.38 fax transport protocols.

Avaya proprietary fax transport protocol

Fax calls route over VoIP trunks between IP Office systems on an IP network using a proprietary Avaya transport protocol.

T.38 fax transport protocol

IP Office supports the T.38 protocol for fax messages transmission between IP Office and SIP trunks and SIP extensions.

Platforms	IP500 V2 with a VCM32 or VCM64 module. Linux based Server Edition servers.
Trunk types	SIP
Extensions	SIP
Transport layers	UDPTL with optional redundancy error correction
Versions	0–3
Call types	Voice calls with transition to fax relay on detection of fax tones and calls which are negotiated as fax-only.
Fax fallback	SIP Trunks and SIP Extensions can now configure the Fax Transport Support to T38 Fallback so that outgoing fax calls use T.38 fax, but when the called destination doesn't support T.38 and rejects the call, a re-invite is sent for fax transport over G.711. Incoming audio calls that detect fax tones also initiate fax transport using T.38 Fallback. This allows IP Office to support additional deployments where T.38 fax may not be universally available.

Related links

IP Telephony features on page 46

Inbound call directory name display

Administrators can select either the CLID or directory name as the default display for inbound calls.

Related links

IP Telephony features on page 46

Out of band DTMF

Implementation engineers can configure out of band DTMF on IP extensions to signal to the other end of a connection the digits to be regenerated by a local DTMF generator on behalf of the sending IP extension. This is useful when navigating external voicemail systems and auto-attendant systems.

Related links

IP Telephony features on page 46

PAI and privacy headers

PAI and privacy header defaults allow callers and calling parties to have anonymity while still providing necessary billing and traceability information, and emergency 911 information to the network. This feature satisfies the functionality with implementation guidelines outlined in the SIPconnect 1.1 Technical Recommendation.

Related links

IP Telephony features on page 46

Silence suppression

Silence suppression makes the best use of available bandwidth, such as the connection over which the caller is listening, not speaking. Silence suppression works by sending descriptions of the background noise, rather than the actual noise itself, during gaps in conversation, thereby reducing the number and frequency of voice packets sent on the network. Background noise is very important during a phone call. Without noise the call will feel very unnatural and give a perception of poor quality. Ensure that silence suppression configuration matches at both ends of the SCN trunk for correct operation and also for improved sound quality.

Related links

IP Telephony features on page 46

SIP features

SIP endpoints are supported on IP Office audio (voice) and T.38 fax communication using SIP terminal adapters. Users can use standards-compliant IP phones using the open SIP standard, offering a choice of endpoints including special purpose devices such as conference phones, hotel phones and terminal adapters.

IP Office supports Avaya 1100 and 1200 series phones using the SIP protocol. The phone user interface can vary when used on BCM with UNIStim. For example, with SIP, the 1100 and 1200 series IP phones only support a single call appearance although multiple calls are supported by the 1100 and 1200 series phones.

Note:

These phones are only supported on IP500 V2 control units.

In pure SIP systems, IP Office expands the feature set beyond the SIP standard offering features on SIP endpoints delivering features consistently between SIP and Avaya digital and IP endpoints.

Note:

In order to use a non-Avaya SIP endpoint with IP Office, obtain a Third-party IP Endpoint license from Avaya. This license supports endpoints based on the H.323 standard and is required for generic SIP endpoints on IP Office. Avaya IP Office SIP phones use the Avaya IP Endpoint license.

PSTN toll bypass

Toll bypass allows each system to leverage the trunk connections of the other system in the network to avoid international and long distance charges.

Standard call features

- Basic Call Completion
- Handling of busy called party
- DTMF and ring-back tone
- Hold and Retrieve
- Transfer
- Call Waiting presentation
- Called Number display
- Calling number and name display
- Abandoned call
- Single call appearance

Advanced call features

SIP endpoints support a number of extended features according to the SIP service samples, also referred to as “Sipping-19”. Features include:

- Calling line identification

- Hold/Consultation Hold
- Attended/Unattended Transfer
- Message waiting
- Do not disturb
- Conference Add
- From in Clear when privacy is requested
- User agent header (configurable) included to identify call in SIP trunks for troubleshooting
- Busy lamp keys with speed-dial, status indication, and pickup
- Self-labeling feature keys for softkey support including a Special feature key. The supported features are also available pressing a feature key plus the appropriate feature code. The feature codes are identical to the features codes from BCM

Feature activation key features

A large number of additional features are supported on IP Office using feature activation keys. These features include but are not limited to:

- Call forward: Unconditional/Busy/no Answer
- Follow me
- Park/Unpark
- Music on Hold
- Meet me conferencing
- Conference join
- Ring back when free
- Multiple call appearances

Note:

Does not include bridged appearances or outside-line appearances.

CTI features

The new centralized CTI web service API provides a more open platform to allow third parties add value and build solutions. Support is provided for distributed (IP Office Server Edition and SCN) environment – not limited to nodal as per current TAPI. Centralized CTI web service API is dependent on Avaya one-X® Portal access for the users. Creating a new user in IP Office with the new API does not require a reboot. SIP endpoints support the following CTI-based features using the TAPI interface:

- Outgoing call (without remote activation of speakerphone/headset)
- Hang up
- Hold
- Attended/Unattended transfer
- Conferencing

- Voicemail collect
- Set forwarding/DND (IP Office based)
- Park/Ride (IP Office based)

Video conferencing

Video conferencing is supported in the following configurations:

- Local system
- Small community network
- Video-ready SIP trunk such as Avaya Aura®

All video communication is end-to-end; IP Office does not natively manage or perform video conferencing.

The softphone application handles video conferencing. IP Office video conference supports the following features using feature access codes:

- Make calls to all phones and trunk lines as audio only
- Receive audio calls
- Call forwarding
- Forward to voicemail recording audio streams, not video.
- Application sharing
- Accept several video calls in parallel to leverage the Multi-Conference Unit (MCU) functionality, for example, the Avaya 1040 system

Video requires high network bandwidth, depending on codec video quality it can be up to 1 Mbit/sec. IP Office supports with H.263 and H.264 codecs. During planning, a network assessment identifies the bandwidth requirements. Refer to product details for video requirements. Typical bandwidth requirements for HD video are:

- 1010: 1 Mbps for 720p/30fps
- 1040:
  - 768 Kbps for 720p 30fps
  - 1.1 Mbps for 720p 60fps
  - 1.7 Mbps for 1080p 30fps

Parameters for passing User to User Information (UUI)

IP Office passes on the received UUI information element back to the public network in case of a transit call. This feature is supported only on SIP trunks and the UUI information element is not passed internally to other elements in the solution such as IP Office Contact Center, , and so on. The UUI information is not mapped to any other trunks types such as ISDN or H.323. IP Office carries the UUI information using a proprietary IP Office field.

Two new parameters are added in the SIP Advanced tab, Identity group, called Add UUI header and Add UUI header to redirected calls. The Add UUI header to redirected calls field is dependent on the Add UUI header field and can be selected only when Add UUI header is selected.
The default value for the field is false. These configuration items are a mergeable feature and applicable to Standard and Server Edition mode on all supported IP Office platforms.

SIP Line Appearances

Trunk line selection enables the familiar line appearance operation on Powered by Avaya (Release 3.0) or IP Office Essential Edition, Server Edition, and IP Office Select. The feature provides easier migration from familiar analog line appearances to SIP line appearances. Line appearance buttons for SIP URIs looks and operates in the same way as the analog trunk appearances. SIP trunk appearances is supported on all phones that support line appearances.

Route incoming SIP trunk calls based on an optional SIP header

This feature enables IP Office to route incoming SIP trunk calls based on optional SIP header P-Called-Party. IP Office reads the P-Called-Party ID header in the SIP message and routes the incoming SIP calls based on it. As P-Called-Party-ID is an optional header it is not parsed by default and it has to be explicitly configured. IP Office uses it for call routing only when the configuration option is selected and the header is present in the incoming SIP call. If the configuration item is checked and the header is not present IP Office uses the header configured in Call Routing Method for Incoming Call Route. P-Called-Party-ID is not used for SM trunks and SIP phones and IP Office does include this header in any outgoing messages.

Security enhancements for registration of SIP devices

This security enhancements enable administrators to allow or disallow registration of SIP devices in IP Office based on their User Agent strings. Administrators can use the configuration settings to add, modify, or remove SIP User Agent strings to SIP UA Blacklist, SIP UA Whitelist, and IP Whitelist. Subsequently, the **Allowed SIP User Agents** setting can be used to select which SIP User Agents are allowed for registering with IP Office. A default blacklist comes preconfigured with some known malicious user agent strings and can be updated as required. The lists can be configured using Web Manager and Manager.

SIP and H.323 Registrars disabled by default

For enhanced security with IP Office R 11.0 FP4, the H.323 and SIP Registrars are disabled by default. Whenever a new H,323 or SIP extension is added and the corresponding registrar is not enabled, IP Office system displays a warning message and prompts administrators to enable the Registrars. When resiliency support is enabled on an IP Office Line in systems having IP extensions and the systems do not have the corresponding registrars enabled, IP Office system displays a warning message and prompts administrators to enable the corresponding registrars.

Related links

IP Telephony features on page 46

Voice compression

IP Office supports a wide range of voice compression standards including G.711, G.722 and Opus. The method of compression can be either automatically established on a call-by-call basis or configured on an individual extension basis.

Voice compression

G.722 is supported on the following types of Avaya phones:

- J100 Series

- 9600 Series
- B179 conference phones
- 1100/1200 IP phones

Opus is supported on the following:

- J100 Series
- Avaya Workplace Client

Related links

IP Telephony features on page 46

Chapter 11: Branch telephony

Related links

Telephony services on page 55
Survivability for centralized users on page 56
Messaging on page 58

Telephony services

The Branch solution provides telephony services to centralized users and IP Office users.

IP Office users obtain telephony services from the local IP Office. The Branch solution supports all hard and softIP Office endpoints. For a list of IP Office endpoints, see “Phones” in *IP500/IP500 V2 Installation* (15-601042).

Centralized users register to the Avaya Aura® Session Manager and obtain telephony services from the Avaya Aura® Communication Manager Feature Server or Evolution Server in the enterprise core. Centralized users can use one of the following supported centralized endpoints:

- 9620 SIP
- 9630 SIP
- 9640 SIP
- 9650 SIP
- 9601 SIP
- 9608 SIP
- 9611G SIP
- 9621G SIP
- 9641G SIP
- 1120E
- 1140E
- 1220
- 1230

- Avaya B179
- Avaya J129 IP Phone
- Avaya J139 IP Phone
- Avaya J159 IP Phone
- Avaya J169 IP Phone
- Avaya J179 IP Phone
- Avaya J189 IP Phone
- Avaya Workplace Client for Windows

Note:

Avaya Workplace Client and Avaya Vantage™ are not supported for centralized users on branch solution.

Related links

Branch telephony on page 55

Survivability for centralized users

If WAN connectivity to the Avaya Aura® Session Manager is lost or if all deployed Avaya Aura® Session Manager servers are down, centralized users automatically get basic telephony services from the local IP Office with survivability or rainy day mode. The telephony features provided by the IP Office in rainy day mode are limited compared to the features that are normally provided to the centralized phone.

The following features are available on Centralized SIP phones when registered to IP Office in Rainy day mode:

- Make or receive calls to or from other endpoints in the branch and to or from any type of local PSTN trunk
- Caller ID
- Multiple call appearances but not bridged appearances
- Call hold and consultative hold
- Music on hold
- Attended call transfer
- Unattended call transfer
- Three-party ad-hoc conferencing done locally on the phone, as well as capability to dial into Meet-Me conferencing on IP Office up to 64-party conference
- Centralized voice mail coverage and access over PSTN, but no Message Waiting Indication (MWI)

- Automated Attendant
- Survivability mode indication on the phone screen
- Local telephone features: redial, mute, audio selection (speaker / headset / handset), Call Logs, Volume Control, local contacts, speed-dials, auto dials
- Station Message Detail Recording (SMDR) records stored on the IP Office for retrieval after WAN recovery
- Hunt groups

  IP Office can be configured with Centralized hunt groups for which IP Office processing is in effect only in the Rainy day mode. The IP Office administrator must configure the hunt groups on the IP Office consistent with the configuration on the central Avaya Aura® Communication Manager for the Sunny day mode.
- Call Management

  IP Office can be configured with short codes using the Barred feature to restrict in the Rainy day mode what calls the Centralized user can make. The IP Office administrator must configure this consistent with the Class of Restriction (CoR) configured on Communication Manager, which is applied to the same user in the Sunny day mode.
- Send call to mobile phone

  IP Office can be configured with Mobile Twinning to send calls for the Centralized user in the Rainy day mode to a mobile number. The IP Office administrator must configure this on the IP Office consistent with the EC500 configuration on the central Communication Manager for the same Centralized user.
- Call forwarding

  Local Call Forwarding on the phone in the Rainy day mode can be configured. The Call Forwarding set on Communication Manager in the Sunny day mode has no impact on the local behavior of the phone or on the IP Office behavior in the Rainy day mode. Also, the local Call Forwarding set on the phone works only in the Rainy day mode after failback.
- Authorization codes

  IP Officecan be configured to support authorization codes that Centralized users can use in the Rainy day mode. The IP Office administrator must configure authorization codes consistent with the authorization codes configured on Communication Manager, which are available to the same Centralized users in the Sunny day mode. Centralized SIP phone users in Sunny day will hear 3 beeps to indicate that an authorization code is required. In the Rainy day mode, the Centralized SIP phone users will hear 1 beep that repeats approximately every 5 seconds.

Related links

Branch telephony on page 55

Messaging

The IP Office Branch solution supports IP Office voice mail systems and centralized voice mail systems.

The following centralized voice mail systems are supported:

- Avaya Aura® Messaging
- Avaya Modular Messaging
- Avaya CallPilot®: Only supported in distributed branch environments connected to CS 1000.

The following IP Office voice mail systems are supported:

- Embedded Voicemail: Default IP Office voice mail system
- Voicemail Pro: Available with IP Office Preferred and Advanced editions

For information about the configuration requirements of each voice mail system, see *Reference Configuration for Avaya IP Office in a Branch Environment* (15–604253).

In a stand-alone branch environment, the enterprise branch can only use an IP Office voice mail system.

In a distributed branch environment, the enterprise branch can choose an IP Office voice mail system or a centralized voice mail system for users. If the distributed environment is connected to CS 1000, users can also use Avaya CallPilot® as their voice mail system.

In a mixed or centralized branch environment, the enterprise branch can only use a centralized voice mail system.

Related links

Branch telephony on page 55

Chapter 12: Messaging features

Messaging enables users to manage all of their messages, both emails and voicemails, in one place. Since the main messaging platform is typically email, IP Office enables users to manage voicemails through the email system in order to keep all messages synchronized through one user interface. IP Office offers two voicemail options: Embedded Voicemail and Voicemail Pro.

Voicemail in general provides a phone answering machine with a personalized greeting on every employee's desk and allows callers to leave spoken messages when the user cannot answer a phone call. Voicemail messages are retrieved either locally or remotely via any phone (users are prompted for a PIN if they are using any phone other than their allocated extension or a trusted location e.g. mobile phone).

The voicemail server is multilingual and can offer different prompts depending on the user's preferred language, independently of the default system setup. Similarly, external callers can hear prompts in their own language depending on their incoming call route (for example, based on caller ID).

Voicemail options available are:

- IP Office Essential Edition Embedded Voicemail enables some basic messaging through the ability to forward voicemail messages to the user's email inbox.
- IP Office Preferred Edition
  - Voicemail Pro - for single site use but use in an SCN from remote users
  - Distributed Voicemail Pro - for multisite use in an SCN
  - Centralized Modular Messaging - for use with Avaya Aura® Communication Manager

Related links

Messaging feature comparison on page 59

Messaging feature comparison

The following table summarizes the operational and functional differences between the messaging applications IP Office supports on the IP500 V2 control unit.

Capacities

Capacity	Voicemail Pro	Embedded Voicemail
Number of mailboxes	No Limit - Limited only by IP Office configuration.	Limited only by IP Office configuration.
Concurrent calls (ports)	Up to 40 dependent on license	6 simultaneous calls
Message Capacity	64MB per mailbox	2 ports: Up to 15 hours 4 ports: Up to 20 hours 6 ports: Up to 25 hours

Features

Feature	Voicemail Pro	Embedded Voicemail
Runs as a service	Yes	No
Multilingual support	Yes	Yes
Voicemail for individual users	Yes	Yes
Voicemail for virtual users	Yes	Yes
Voicemail for hunt groups	Yes	Yes
Group broadcast	Yes	No
Unified Messaging Service (UMS)	Option	No
Integration with Microsoft Exchange Server	Option	No
Capable to interact with Blackberry solution	Option[1]	No
Resilience and Backup	Option	No
Small Community Network operation	Yes	No
Centralized voicemail services	Yes	No
Distributed voicemail servers in an SCN	Yes	No
Voicemail Ringback	Internal and external	Yes
Voicemail Help TUI	Yes	No
Message Waiting Indication	Yes	Yes
Visual Voice (interactive menu on phone display)	Yes	Yes
Integration with Phone Manager Pro	Yes	No
Personalized greetings	Yes	Yes

Table continues…

[1] Requires UMS (enabled through the Power User, Office Worker and the Teleworker licenses) and MS Exchange Server 2007/2010 with a mobility solution (for example a Blackberry) - not provided by Avaya.

Feature	Voicemail Pro	Embedded Voicemail
Extended personal greetings	Yes[2]	No
Continuous Loop Greeting	Yes	No
Forward to email	Yes	Yes
Copy to email	Yes	Yes
Listen to email (Text-To-Speech)	Yes[2]	No
Send email notification	Yes	Yes
Save message	Yes	Yes
Delete message	Yes	Yes
Forward Message to another mailbox	Yes	Yes
Forward to multiple mailboxes	Yes	Yes
Forward with a header message	Yes	Yes
Repeat message	Yes	Yes
Rewind message	Yes	Yes
Fast forward message	Yes	Yes
Pause message	Yes	No
Skip message	Yes	Yes
Oldest message first/newest message first Message Playback Option	Yes	No
Set message priority	Yes[2]	No
Set automatic message deletion time frame	Yes	No
Alphanumeric Data Collection	Yes[2]	No
Callers Caller ID, time and date announced	Yes	Yes
Call Back Sender (if Caller ID available)	Yes	Yes
Remote Access to Mailbox	Yes	Yes
User Definable PIN Code	Yes	Yes
Known Caller ID PIN Code By-Pass	Yes	Yes
Breakout to Reception	Internal and external.	Internal and external.

[2] Intuity mode only.

In queue announcements

Feature	Voicemail Pro	Embedded Voicemail
Queue Entry Announcement	Yes	Yes
Queue Update Announcement	Yes	Yes
Queue Position Announcement	Yes	No
Time in Queue Announcement	Yes	No
Time in System Announcement	Yes	No
Estimated Time to Answer (ETA)	Yes	No
Exit Queue to alternative answer point	Yes	No

Auto-Attendant/Audiotex

Feature	Voicemail Pro	Embedded Voicemail
Multi-Level Tree Structure	Yes	Yes
Message Announcements	Yes	No
Whisper Announce	Yes	No
Alarm Calls	Yes	No
Assisted Transfers	Yes	No
Dial by Name	Yes	Yes
Direct Dial by Number	Yes	Yes

Other features

Feature	Voicemail Pro	Embedded Voicemail
Call Recording	Yes	No
Tamper proofed/verified Call Recording	Yes	No
Test Conditions	Yes	No
Personal Numbering	Yes	No
Speaking Clock	Yes	No
Campaign Manager	Yes	No
Voicemail Pro Manager	Yes	No
Customized voicemail	Yes	No
Intuity TUI emulation mode	Yes	No
Forward Emails to external systems (VPIM)	Yes	Yes
Third-party database Access (IVR)	Yes	No
Text-To-Speech within call flows	Yes	No
Support for Visual Basic Scripts	Yes	No

Related links

Messaging features on page 59

Chapter 13: Mobility features

Related links

Hot Desking on page 64
Remote access features on page 65
Remote hot desking on page 65
Remote Worker on page 66
Telecommuter mode on page 69
Twinning on page 69
Fallback Twinning on page 70
Simplified Mobile Access on page 71
VPN Phone on page 71

Hot Desking

Hot desking allows users nonexclusive use of the a single extension.

Users log with their own identity so they can receive calls and can access their voicemail and other facilities. For example, sales personnel who visit the office infrequently can be provided with telephony and voicemail services without being permanently assigned a physical extension. When finished, they simply log out to make the extension available to others or if users log in at another phone, they are automatically logged out of the original extension.

Support for Hot desking on SIP function phones such as J129 and H175 are not available from IP Office Release 10.1. This includes Hot desking through CTI or the standard short codes; *35 and *36 by default. The SIP function phones on IP Office do not support clearing of user contacts and call history when a new user logs in to those phones through Hot desking. This can result in one user having visibility to another user's contacts and call history information.

Related links

Mobility features on page 64

Remote access features

IP Office's integral firewall, service quotas and timebands all apply to remote access calls. Remote access security can be supplemented by CHAP (encrypted passwords) to verify the end users, or PAP which does not support encryption. Timebands can control the hours within which the remote access service is available.

A trusted location can be set for dial in. These are locations that the system will allow either data access, for example, a user dialing in from home, or access to voicemail without a voicemail code for a user collecting their voicemail messages from a mobile. The trusted location is also the location the voicemail server will call to inform the user of a new message.

Conversely a specified location can be set which restricts remote access from only that location, this specified location can also be a designated dial back number thereby minimizing the threat of unauthorized remote access.

IP Office can also incorporate remote access dial back services so that if a user always remotely accesses the office from a single location, for example, their home, then after login verification, the system disconnects their call and dials them back. In addition to the added level of security dial back provides, it can also be an excellent method of consolidating remote access charges onto the central office phone bill.

In addition to remote access from phone adaptors, all ATM4 trunk cards (including the IP500 V2 Combination Card ATM) support switching of the first analog trunk to an integral V.32 modem for remote access.

Related links

Mobility features on page 64

Remote hot desking

Users can make and receive calls from any office as if using the phone on their own desk. Users have access to the centralized system and personal directory as well as their call logs (available on digital, analog and IP phones).

When a user logs in to a remote IP Office system, all their user settings are transferred to that system.

- The user's incoming calls are rerouted across the SCN.
- The user's outgoing calls use the settings of the remote IP Office.
- However some settings may become unusable or may operate differently. For example, if the user uses a time profile for some features, those feature will only work if a time profile of the same name also exists on the remote IP Office.

IP Office supports remote hot desking between IP Office systems within an SCN. The system on which the user configured is termed their “home” IP Office, all other systems are “remote” IP Offices. No additional licenses are required to support remote hot desking other than the Voice

Networking license on each IP500 V2 within the SCN. A single number provides improved mobility and easy access to familiar features. For example consultants, managers, and lawyers can use their phone services at different offices on different days.

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. 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 SCN but is of significant use to remote hot deskers.

Note:

Remote hot desking is not supported for use with contact center. Features handled by the phone itself are not affected by hot desking, for example, call log and phone speed dials)

Related links

Mobility features on page 64

Remote Worker

Remote Worker allows the connection of supported IP phones and client applications remotely from IP Office, without requiring any VPN concentrator equipment with IP Office.

With the Remote Worker feature enabled, remote 9600 H.323 or SIP J100 IP Phones can connect to IP Office even if it is located behind a NAT router. The same applies to supported client applications, see supported SIP endpoints on page 66. The sets or applications are authenticated on IP Office in the same way as if in the private network. The IP Office determines that the user is located outside the private network and relays the VoIP RTP traffic to ensure it transverses the NAT router.

The following 9600 phones are supported:

- 9620, 9630, 9640, 9650

  Note:

  The H.323 signaling and the media traffic is not encrypted however the proprietary binary format adds a basic level of encryption.

- 9608, 9611, 9621, 9641

  Note:

  The H.323 signaling and media traffic may be encrypted using TLS and SRTP respectively.

The following SIP endpoints are supported:

- Avaya J100 Series IP Phones:
  - J129 (Standard SIP phone)

  - J139, J159,J169,J179, J189 (SIP Feature phones)
- Avaya Vantage™ 2.2 version: K165, K175 and K155
- Avaya Vantage™ 3.0 version and above: K175 and K155
- Avaya Workplace Client platforms:
  - Avaya Workplace Client for Windows
  - Avaya Workplace Client for Android
  - Avaya Workplace Client for Mac
  - Avaya Workplace Client for iOS
- B179
- B199

To reach the IP Office from the remote private network, remote IP phones or client applications need to be configured to point to the public IP address of the NAT router hosting IP Office. Configurable ports need to be forwarded to IP Office. IP Office requires a valid public IP address configured for the feature to function. The public IP address can be statically configured or dynamically discovered via a STUN server.

Administrators enable Remote Worker feature using IP Office Manager. To use the Remote Worker feature, you require the Essential Edition license. The Essential Edition license provides 4 remote workers.

Additional Remote Workers can be configured if those additional users are licensed and configured with either Teleworker or Power User user profiles

Note:

On Server Edition systems, the Remote Worker is supported for all user profiles (Basic User, Office Worker and Power User)

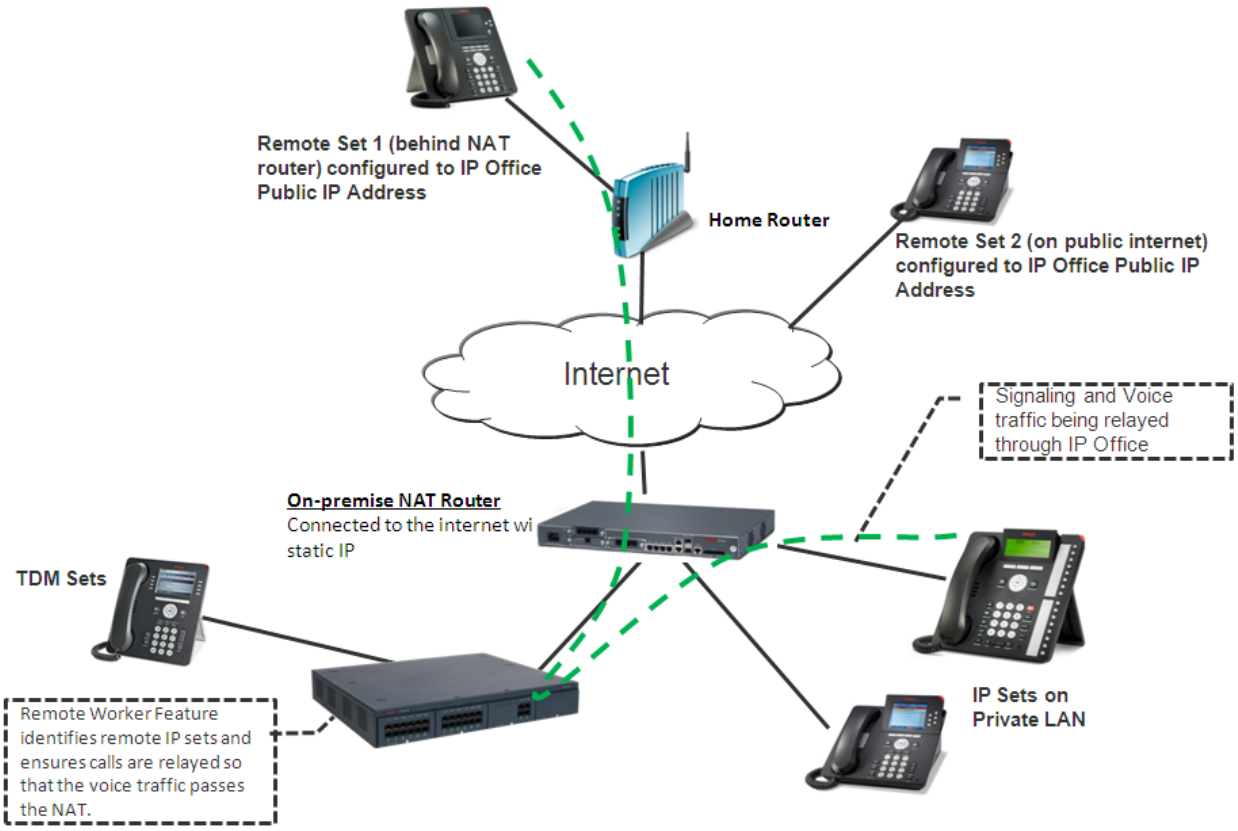


Figure 1: Remote Worker interactions

SIP phones using Avaya SBC

The Avaya Session Border Controller (Avaya SBC) sits on the edge of customer's network with both internal and external IP interfaces. Using these IP interfaces, Avaya SBC functions as the gateway for SIP traffic into and out of the network. When used internally, SIP clients register to the IP Office directly. When used externally, the SIP clients connect to the Avaya SBC. This is achieved using Split DNS, which automatically resolves the FQDNs to the internal IP address of the IP Office or the public IP address of the Avaya SBC depending on where the clients are currently located. Apart from acting as a gateway, Avaya SBC also provides protection against any external SIP-based attacks. For privacy over the public internet, the public side of the Avaya SBC facing the remote workers must be configured to use the recommended values of TLS for signaling and SRTP for media encryption, as long as they are supported by the endpoints.

The following endpoints are supported as IP Office Remote Workers with Avaya SBC.

- Avaya J100 Series IP Phones:
  - J129 (Standard SIP phone)
  - J139, J159, J169, J179, J189 (SIP Feature phones)
- Avaya Vantage™ 2.2 version: K165, K175 and K155

  Avaya Vantage™ 3.0 version and above K175 and K155

- Avaya Workplace Client platforms:
  - Avaya Workplace Client for Windows
  - Avaya Workplace Client for Android
  - Avaya Workplace Client for Mac
  - Avaya Workplace Client for iOS

Related links

Mobility features on page 64

Telecommuter mode

Users can make and receive calls and the retrieve voicemails from an external phone number as if they were in the office, with the server providing the call control.

The typical scenario is the remote worker that occasionally works from home or from a hotel room. This feature also provides billing convenience and potential cost savings for remote workers and mobile work force as all the calls are established by IP Office. There is no need to check bills or to pay for expensive hotel calls.

Related links

Mobility features on page 64

Twinning

Twinning allows a primary extension and a secondary number (extension or external) to operate together as a single phone.

Twinning allows calls to a user main extension number to alert at both that extension and a secondary extension. This feature is aimed primarily at users who have both a desk phone and a wireless extension. Calls from the secondary twinned extension are presented as if from the user's main extension. Presentation of call waiting and busy is based on whether either of the twinned extensions is in use.

When a call is presented to the primary phone the secondary will ring. If the primary phone does not ring, for example in Do Not Disturb, the secondary phone will not ring.

This is typically used in scenarios like workshops or warehouses where team supervisors may have a desk with a fixed phone but also have a wireless extension (e.g. DECT). When a call is made from either twinned phone, the call will appear to have come from the primary phone. Other users of the system need not know that the supervisor has two different phones. The supervisor’s Coverage Timer and No Answer Time are started for the call and if the call is not answered within that time, the call will be delivered to available coverage buttons and then voicemail.

The following features are supported with twinning:

- Follow Me To
- Follow Me Here
- Forwarding
- Do Not Disturb (including exceptions)
- Context less hunt group actions: Membership/Service Status/Fallback Group configuration
- Voicemail On/Off/Access
- Call Log (Central Call Log 1600 phones only)
- Redial (Central Call Log 1600 phones only)
- Personal Directory Entries (for 1600 phones only)

Mobility features include:

- Mobile (external) Twinning
- Mobile Call Control
- Mobility Callback

Related links

Mobility features on page 64

Fallback Twinning

IP Office redirects calls to the users twinned external phone numbers when the primary extensions are unreachable even when the Mobile Twinning is disabled. This feature provides a mechanism for failing over to an external device such as mobile and PSTN if a customer site supporting IP Office phones loses connectivity with the Cloud data center.

The following two short codes are available for disabling and enabling mobile Fallback Twinning:

- Set Fallback Twinning Off: To disable Fallback twinning
- Set Fallback Twinning On: To enable Fallback twinning

When Fallback Twinning feature is enabled:

- If Mobile Twinning is enabled – the only change will be to ignore the Mobile Dial Delay setting if the user's devices are unreachable.
- If Mobile Twinning is disabled – and if the user has no reachable devices, the normal evaluation of all Mobile Twinning conditions is performed, and if met, calls are redirected to the twinned mobile number immediately, that is, ignoring the Mobile Dial Delay setting.

Related links

Mobility features on page 64

Simplified Mobile Access

The standard behavior of the Mobile Call Control feature gives a Mobile Worker fresh dial-tone if a call recipient clears its call. This is intended operation as it prevents the Mobile Worker from dialing in again to make any further calls. Simplified Mobile Access introduces a new set of FNEs (FNE35, FNE36, and FNE 37) to clear the call on call completion; no dial-tone is provided after the call ends.

Related links

Mobility features on page 64

VPN Phone

VPN Phone is a full-featured IP telephony solution that provides secure communication over public ISP networks to IP Office at the company headquarters. VPN phones provide full telephony features available at the user's desktop to a remote location like a home-office. There is no restriction on VPN phone usage.

VPN Phone is a software-only feature on the standard 5610/5620/5621 or 4610/21 IP phones. In combination with one of these phones and the most popular VPN gateway products, the software extends enterprise telephony to remote locations. VPN functionality is supported on 9600 IP phones and does not require additional software.

VPN Phone works in the following situations:

- Virtual Office workers
- Remote workers
- Remote call center
- Business continuity support
- Very small locations that require a single phone only
- Temporary installations such as conferences, off-site meetings, and trade shows

Note:

J100 phones with SIP do not support VPN phone.

VPN Phone has been tested with a number of VPN-gateways from major vendors like Cisco or Juniper as well as with smaller VPN-access devices from companies like Adtran, Kentrox, Netgear, and SonicWall. Refer to the support pages (support.avaya.com) for a list of available application notes on VPN-gateways tested with each line of phones.

Related links

Mobility features on page 64

Chapter 14: Network features

Related links

Alternate Route Selection on page 72
Auto Connect on page 73
Callback on page 73
Firewall on page 73
Internet Access on page 74
Network Numbering Schemes on page 75
Service Quotas on page 75
Time Profiles on page 75
Multisite networking on page 76
Networking services on page 78

Alternate Route Selection

If a primary trunk is unavailable, then Alternate Route Selection (ARS) provides automatic fallback to an available trunk, for example, analog trunk fallback if a T1 or SIP trunk fails, or use PSTN for SCN fallback.

By configuring ARS, the system can route calls through the optimum carrier. You can also use time profiles to take advantage of less expensive rates or better quality at specific times of day.

Multiple carriers are supported. For example, local calls are to go through one carrier between specific hours and international calls through an alternative carrier. Carrier selection using two-stage call set up through in-band DTMF is possible. It is possible to assign specific routes on a per user basis to only allow expensive routes to be used by critical staff.

Related links

Network features on page 72

Auto Connect

If a service is idle, that is no one is using the internet, Auto Connect allows the system to periodically connect to a service. This is ideal for mail polling to retrieve email from an internet service provider. An Auto Connect Time Profile controls the time period during which automatic calls are made, for example not at weekends or during the middle of the night.

Related links

Network features on page 72

Callback

Three types of call back are supported:

Link Control Protocol (LCP)	After authentication the incoming call is dropped and an outgoing call is made to a predefined number to reestablish the link.
Microsoft Callback Control Protocol (CP)	After authentication from both ends, the incoming call is dropped and an outgoing call to a predefined number made to reestablish the link.
Extended Callback Control Protocol (CBCP)	Similar to Callback CP however, the Microsoft application at the remote end will prompt for a phone number. An outgoing call will then be made to that number to reestablish the link.

Related links

Network features on page 72

Firewall

IP Office integrated firewall provides packet filtering of the most common IP protocols including File Transfer Protocol (FTP) and Internet browsing (HTTP). Each protocol passing through the firewall can be restricted/allowed access in four different ways:

Drop	No sessions using this protocol will be allowed through the firewall.
In	An incoming session can get through the firewall to allow traffic in both directions.
Out	An outgoing session can get through the firewall to allow traffic in both directions.
Bothway	An incoming or outgoing sessions can get through the firewall to allow traffic in both directions.

In cases where a protocol is not supported by default, the firewall can be customized to control packets based on their content.

IP Office allows the configuration of as many firewalls as needed through IP Office Manager. This permits different security regulations to be applied to individual dial-in users and data services.

Related links

Network features on page 72

Internet Access

IP Office provides shared, secure, high-speed access to the internet via exchange lines (Central Office), digital leased lines or IP VPN services.

IP Office handles internet security with an integrated firewall removing the need for a standalone firewall. System administrators can configure the firewall to accommodate a variety of situations and to control who can access external resources and when.

The firewall isolates private networks from the internet, ensuring that the network remains beyond the reach of hackers, while allowing service quotas to be set against a remote access service to ensure authorized users can gain access. Service Quotas place a time limit on outgoing calls to a particular IP Service so limiting costs.

Each service can be configured with an alternative fall back, for example, to connect to an ISP during working hours and at other times take advantage of varying call charges from an alternative ISP. Or, set up one service to connect during peak times and another to act as fallback during the cheaper period.

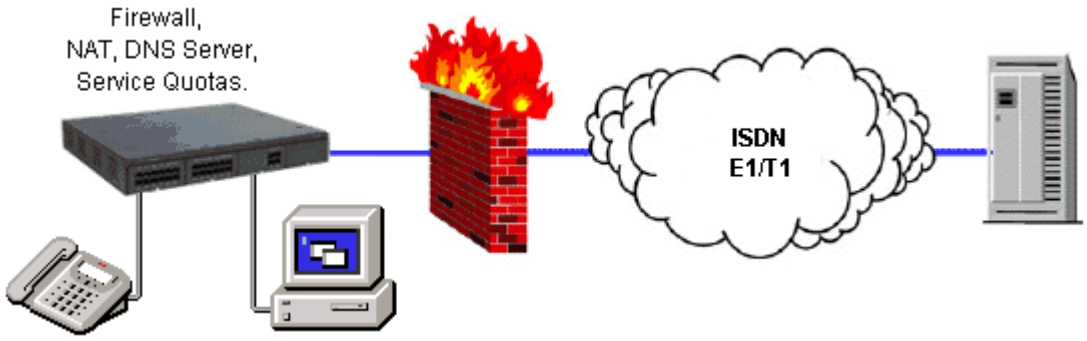


Figure 2: Internet access

Related links

Network features on page 72

Network Numbering Schemes

IP Office provides flexible network numbering options. The system can manipulate dialed digits adding or removing digits and access codes to fit into any numbering scheme. Two types of numbering schemes are commonly deployed: linked numbering and node numbering.

In linked numbering schemes each site within the network has a unique range of extension numbers and users simply dial the extension number of the called party. Often, linked numbering schemes are used in very small networks (less than 5 sites) with less than 500 extensions.

With node numbering schemes, each site is given a node ID and this is prefixed by the user when dialing extensions at other sites. In this way extension numbers can be replicated across sites while still appearing unique across the network. Node numbering schemes are common in larger networks.

Linked numbering schemes and node numbering schemes are sometimes both used within the same network with node numbering used at the large offices and linked numbering employed at clusters of satellite offices.

Related links

Network features on page 72

Service Quotas

IP Office can be configured to limit the maximum number of minutes that a service, such as Internet Access, is available for each user. This is the sum total of calls made and does not include periods of inactivity. Once the quota has been used the service is no longer available. The quota can be either automatically refreshed daily, weekly or monthly or manually refreshed by dialing a secure feature code on a handset.

Related links

Network features on page 72

Time Profiles

Time Profiles can be used to define when a Service, Hunt Group, Least Cost Route, Conference Bridge or a user's dial-in facility are operational. For example, a time profile can be used to route hunt group calls to a manned extension or voicemail outside of office hours, or be used to apply different Least Cost Routes at varying times of day to take advantage of cheaper call rates. Multiple Time Entries can be created so that a Time Profile can be used to define specific hours in the day e.g. 09:00-12:00 and 13:00-17:00. Outside of a Time Profile, voice calls would be re-routed according to the configuration but any currently connected calls at the time the Time Profile changes would not get cut off as the change only affects the routing. Data calls will get cut

off as the time profile goes out of service but a new data call will start immediately if specified. Time Profiles can also be based on specific calendar dates to make allowance for public holidays or other events.

Related links

Network features on page 72

Multisite networking

When connecting IP Office systems together over IP or packet-based networks, Small Community Networks (SCNs) enhance feature transparency. These networks can support up to a maximum of 1000 users across 32 sites.

IP Office supports the following features in an SCN environment:

Basic call setup (voice)	Supported by H.323 and SIP on IP trunks
Call Hold (local)	Supported by H.323 and SIP on IP trunks
Call Transfer (local)	Supported by H.323 and SIP on IP trunks
Called/Calling Name	Supported by H.323 and SIP on IP trunks
Called/Calling Number	Supported by H.323 and SIP on IP trunks
Busy Lamp Field (BLF)	
Camp-on	
Call Back When Free	
Paging	
Pickup	
Location based time zones	Different times zones for group of extensions based on locations. For 9600, 160, 1100/1200, D100 phones
Centralized Personal Directory	For 1400, 1600, 9600 phones and Avaya one-X® Portal for IP Office
Centralized System Directory	For 1400, 1600, 9600 phones and Avaya one-X® Portal for IP Office
Centralized Call Log	For 1400, 1600, 9600 phones and Avaya one-X® Portal for IP Office

Centralized Voicemail	Preferred Edition. Support for mailboxes, call recording, dial by name and auto attendants. Remote queuing on remote systems is also supported.
Distributed/Backup Voice Messaging	
Internal Directory	
Absence Text	
Anti-Tromboning	
Distributed Hunt Groups	Hunt groups can include users located on other IP Office systems within the network.
Remote Hot Desking	Users can hot desk between IP Office systems within the network. The system on which the user configured is termed their home IP Office; all other systems are remote IP Office systems.
Breakout Dialing	This feature allows the user to select an IP Office system in the network from a displayed list and then dial a subsequent number as if dialing locally on the chosen system. This feature is triggered either by a programmable button or short code.

Resiliency

As an example, in an SCN configuration of System A and System B where the centralized voicemail is connected to System B, and a number of IP phones are connected to either System A or System B. If System B fails then:

- System A will automatically take over from System B and support IP phones, hunt groups, and DHCP if required.
- Voicemail Pro will reregister to System A.
- For users in an SCN, when they hot desk to another IP Office system, they retain their licensed profile setting as configured on their home system.
- All System B users' personal contacts and call logs will continue to be available (96x1, 9600, and 1600 phones).

For multisite networks, VCM modules are required in all systems being connected. The IP lines may be configured in a start or a meshed configuration. One of the advantages of a meshed configuration is that it removes the risk of a single point of failure within the network. Also the names and numbers (groups, line, services, etc.) on the separate IP Office systems should be unique to reduce potential maintenance confusion.

EachIP Office system broadcasts UDP messages on Port 50795. These broadcasts typically recur every 30 seconds but BLF updates are potentially more frequent. There are no updates if there is no activity and the overall level of traffic is very low - typically less than 1 kbps per system.

Multisite networking is supported between IP Office systems with differing software levels but network features will be based on the lowest level of software within the network. This option

is intended to allow the phased upgrading of sites within a multisite network and it is still recommended that all systems within a network are upgraded to the same level where possible.

If larger networks are required Q.SIG can be used to link multiple SCNs together. Functionality between the communities is governed by the Q.SIG feature set.

Voice networking licenses

On IP500 V2 systems, multisite networking (with SCN) requires one or more additional licenses. Server Edition Expansion (V2) systems do not require voice networking licenses.

Q.SIG, H.323 and SCN capabilities are not enabled by default on IP500 V2. An additional license is required to enable this functionality with 4 simultaneous networking channels (no channel limit for Q.SIG). Additional channels can then be licensed in increments of 4. A Voice Networking license is still required to enable TDM Q.SIG, even though there is no limit to the number of TDM Q.SIG calls that can be made or received once licensed.

Related links

Network features on page 72

Networking services

Related links

Network features on page 72
Dial-Up Circuit Support on page 78
DHCP Server on page 79
Domain Name Service (DNS) Proxy on page 79
LAN/WAN Services on page 79
LAN to LAN Routing on page 80
Integral 10/100 Mbit Layer 3 Ethernet Switch on page 80
Leased Line Support on page 80
Remote Access Server on page 80
SSL/VPN Remote Access on page 81

Dial-Up Circuit Support

Where the amount of traffic does not justify the cost of a dedicated leased line, the system can provide data connectivity via ISDN dial-up circuits using its E1/T1 or Basic Rate trunks. Where data speeds greater than a single channel are required (64K/56K), additional channels can be added to the call as and when they are needed.

Related links

Networking services on page 78

DHCP Server

IP Office can manage your IP Network for you through its integral DHCP Server. IP Office can be configured to hold a pool of IP addresses for users on the Local Area Network. When a user powers up their PC, the system will allocate them an IP address for the duration of their session. The DHCP server also provides the user's PC with the address of the Domain Name Service (DNS) server and the Windows Name Service (WINS) server. Alternatively, for customers who have a separate DHCP Server, IP Office can be configured to obtain its address from that DHCP server or be set with its own static IP address. IP500 V2 has two independent DHCP servers, each one dedicated to Layer 3 switched LANs.

Related links

Networking services on page 78

Domain Name Service (DNS) Proxy

Domain Name Service servers provide the translation of names such as www.avaya.com to the domain's IP address required to establish a connection. IP Office provides this service to PCs on the network by proxy.

Related links

Networking services on page 78

LAN/WAN Services

The IP500 V2 supports a firewalled 2 port Layer 3 Ethernet Switch.

When computers on the LAN communicate they do not care where the destination is, they just send messages with the address of the destination. These messages are likely to be received at all other computers on the same network but only one - the target destination - will act on the message. Where the destination is on another network, the router is needed to be the "gateway" to the rest of the world and find the optimum route to send the message on to the destination. The router alleviates the need to establish and hold a call for the duration of a communication session (when messages or IP packets are being sent between source and destination) by automatically establishing a connection only when data is to be passed. Routers may be connected together using WAN (Wide Area Network) links that could be point-to-point leased lines, managed IP networks, Frame Relay networks or exchange lines (Central Office). The IP Office system supports all of these types of network connections.

IP Office has an integral router with support for bandwidth on demand that allows the negotiation of extra bandwidth dynamically over time. Where connection is over ISDN, IP Office initiates extra data connections between sites only when there is data to be sent or sufficient data to warrant additional channels. It then drops the extra channels when they are no longer needed. The calls are made automatically, without the users being aware of when calls begin or end. The rules for making calls, how long to keep calls up etc, are configurable within IP Office.

It is possible to have several different routing destinations or paths active at any time linking the office to other offices and the Internet simultaneously.

Related links

Networking services on page 78

LAN to LAN Routing

All businesses now have a need for data routing whether it's a requirement to share resources such as email servers, file servers and internet gateways, or seamlessly transport data between sites or network to and from their customers and suppliers. This is why each IP Office platform offers IP routing as standard.

Embedding a router within IP Office removes the costs, complexity and additional points of failure of external WAN multiplexers by allowing data and voice traffic to converge and share the network resources of IP Office. These network resources can range from dial up ISDN connections, point-to-point leased circuits, managed IP networks or Frame Relay as IP Office supports all these types of network connections.

Related links

Networking services on page 78

Integral 10/100 Mbit Layer 3 Ethernet Switch

Layer 3 switching is particularly useful in situations where it is desirable to have a 'trusted' and 'unsecured' network, where the 'unsecured' network is uncontrolled and carries public traffic on it.

It is possible to set up a firewall between two LAN segments using the IP Office layer 3 switch. IP500 V2 supports a two-port Layer 3 Ethernet switch with the firewall between them. Both of these switched ports have their own IP addresses (LAN1 and LAN2) and in order for traffic to pass from one port to the other, a route is configured in the system's routing tables.

Related links

Networking services on page 78

Leased Line Support

IP Office is capable of connecting to leased line services.

IP Office WAN services are supported over E1/T1 PRI trunks and BRI trunks. E1/T1 trunks can be configured to operate in a fractional mode for 'point to multi-point' applications i.e. a single 2M interface could be treated as 3 x 512K and 8 x 64K going to 11 different locations. When using T1 as a Leased Line it is possible to use the same circuit for switched circuit services. Not all types of leased line are available in all territories, check for availability.

Related links

Networking services on page 78

Remote Access Server

IP Office provides Remote Access Server (RAS) functionality allowing external users to dial in to the local area network from modems, phone adaptors and routers.

Several of the previously described features and services can be applied to the dial-in users to create RAS capabilities. Dial-in users can be authenticated using either PAP or CHAP. Once authenticated the DHCP server can automatically assign the user an IP address to use while connected to the LAN. Individual time profiles and firewalls can be applied to the user restricting what they have access to and when they have access. For further security and accounting ease, IP Office can automatically call a user back. This keeps the cost of the phone call on the company phone bill removing the need to process individual expense claims.

Related links

Networking services on page 78

SSL/VPN Remote Access

SSL/VPN remote access provides Avaya and Avaya partners with reliable remote access that enhances service delivery while reducing the cost associated with truck rolls. The solution enables partners of any size to create an infrastructure that automates management and maintenance of IP Office systems.

IP Office software includes an embedded SSL/VPN client. On the server side (should the partner decide to host the server side), the partner will need to install a server (VM) and install the Avaya VPN Gateway (AVG) software. The Partner will establish the SSL/VPN Gateway configuration on the IP Office so that the IP Office can trigger a secure tunnel back to the Gateway.

A username/password is setup during the configuration step for security purposes. A second level of security is also provided with a server-side certificate authentication. A radius server will then validate the username/password upon connection request initiated from the IP Office. Once the credentials are validated, the secure remote access is established.

At a minimum, the partner needs to ensure that a broadband connection is available at the customer site. A partner deciding to host the server side can purchase (scale as you go) the SSL/VPN licenses based on how many simultaneous connections are required. The AVG software is installed on a VM server software (the partner can choose the server of their choice) and set up a radius server for username/password authentication. The same VM server can also act as a radius server or the partner can use a separate radius server or reuse an existing radius server based on their IT department's recommendations and security policy.

Partners wanting to host the server side gateway should refer to the Avaya enterprise portal for more detailed information about the Avaya VPN gateway solution (see https://enterpriseportal.avaya.com/ptlWeb/gs/products/P0623/AllCollateral).

SSL/VPN remote access provides the following functionality:

- Secure remote access at broadband speeds for enhanced support
- Simple configuration and deployment
- Scaling to accommodate future growth requirements
- Networking expertise not required at the customer site (No IT admin required at the customer site)
- No requirement to open holes in the firewall (Firewall-agnostic as the connection is initiated from the customers' site to the Gateway)

- Connection can be “Always-ON” or can be initiated via Dial-Up or Phone.
- Facilitation of remote configuration, management, monitoring, diagnostics, and upgrades.

Related links

Networking services on page 78

Chapter 15: Phone features

Related links

Alerting/ring tone for covered calls on page 83
Call history on page 83
Caller ID on page 84
Centralized Personal Directory on page 84
Language on page 85
On Hook Dialing on page 85
Self-Administration on page 85
Visual voice on page 85

Alerting/ring tone for covered calls

Users can choose how the covered call will alert and set the alert noise to low in open floor plan offices.

Users can set the alert signal (ring tone) for incoming calls for covered phones to the following values:

- Ring (default)
- Abbreviated ring
- No ring

Related links

Phone features on page 83

Call history

IP Office keeps a record of calls made and received, including unanswered calls. Details are store for both users (maximum 30 entries) and hunt groups (maximum 10 entries). The method of operation varies according to the phone type but in all cases the call records can be used for return calls.

Call history can display data for all calls, missed calls, inbound calls and outbound calls. Entries in the call history can be used for return calls, sorted and added to the local directory or speed dials. Call log data is retained even after power down and a system reset. A centralized call log is supported in the SCN when using hotdesking maintaining consistency between desktop phones and user productivity applications. Call log entries can be added to the personal directory.

Related links

Phone features on page 83

Caller ID

If the service provider supplies a caller ID, IP Office can pass it to the answering phone or application and is includes it in any call log or history supported by the phone or application. If the caller ID matches a number in the directory, IP Office displays the matching directory name.

If IP Office Phone Manager or TAPI service links to a database, IP Office performs an automatic query on the supplied Caller ID and displays the caller's record to the user before the call is answered.

For outgoing calls, IP Office can insert a system wide caller ID or set a flag to have caller ID withheld. For users with a direct dial number routed to their extension, IP Office uses that number as their caller ID for outgoing calls. Alternatively, IP Office can use short codes to specify the caller ID that should be sent with outgoing calls.

Note:

Sending and receiving the caller ID is subject to the service provider supporting that service. The service provider may also restrict which numbers can be used for outgoing caller ID.

Related links

Phone features on page 83

Centralized Personal Directory

The Personal Directory is a list of up to 100 numbers and associated names stored centrally in the system for a specific user. A directory entry can be used to label an incoming call on a caller display telephone or on a PC application. The directory also gives a system wide list of frequently used numbers for speed dialing.

For example “Mr. Smith” can be displayed when a known Caller ID is received. A user can also select **Mr. Smith** in the Directory List in Phone Manager, or on a display phone to speed dial this number. All entries may be added, deleted or modified by Manager, , a telephone, or an external service. The personal directory data is sent/updated whenever the user is logged in a SCN.

Related links

Phone features on page 83

Language

Avaya digital and IP phone menus and displays are available in many languages and usually the system default setting will be applicable to all phones, however it is possible to have language set on an extension by extension basis, this will also change the language of menus for IP Office Voicemail.

Related links

Phone features on page 83

On Hook Dialing

Avaya digital and IP telephones allow the user to make calls by just dialing the number on the keypad, without having to lift the handset or pressing a speaker button. Usually the call progress can be monitored using the speaker in the phone On phones that support hands free usage, the conversation can be had without having to lift the handset.

Related links

Phone features on page 83

Self-Administration

The IP Office administrator may give select users the ability to change some of the phone settings themselves. The range of changes that the user can make depends on the phone.

Related links

Phone features on page 83

Visual voice

Users can access and control voice messages through the digital or IP phone display. Visual Voice works on Preferred or Essential Edition, and can only be used with large-display phones such as Avaya J100 Series IP Phones.

On phones that have a display but do not support visual voice, mailbox access using voice prompts and direct to voicemail transfer during a call is supported.

Visual voice allows users to perform the following tasks:

- Access new, old and saved messages for personal and hunt group mailboxes
- Next and previous message
- Fast forward and rewind
- Pause message
- Save, delete and copy a message to other users of the system
- Change default greeting
- Change password
- Change email settings (Preferred Edition only)

Related links

Phone features on page 83

Chapter 16: Appearance buttons

Many Avaya digital and IP phones have programmable buttons. These buttons can be assigned to appearance functions that allow the handling of calls.

Use the programmable buttons available on Avaya digital and IP phones to represent individual calls. Answer, originate and join calls by pressing the appropriate appearance buttons. The appearance buttons on the phone indicate calls connected and calls waiting. This allows the user to handle multiple calls from a single phone.

Related links

Line appearance buttons on page 87
Call appearance buttons on page 87
Bridged appearance buttons on page 88
Call coverage buttons on page 88
Multiple Access Directory Number buttons on page 89

Line appearance buttons

Line appearance indicate users making and answering calls on a specific external trunk.

Line appearance buttons show the use of a trunk line on the system and tracks the activity on the line. Only external calls can be answered or made on line appearances. Line appearances can be used with Analog, E1 PRI, T1 PRI and BRI trunks PSTN trunks. They cannot be used with E1R2, Q.SIG and IP trunks.

Related links

Appearance buttons on page 87

Call appearance buttons

Call appearance buttons allow a user to make, answer and switch between multiple calls by pressing the appropriate call appearance button for each call.

On digital and IP phones that have programmable buttons, you can be set them as call appearance buttons using IP Office Manager. The number of call appearance buttons set for

a user determines the number of simultaneous calls they can make and answer. When call appearance buttons are used, a minimum of three call appearance buttons is recommended where possible, although some phones are restricted to two call appearance buttons by the number or design of their programmable buttons. Where possible, the status of the calls (ringing, connected or held) is indicated by the button indicator.

Note:

Note that the use of call appearance buttons overrides call waiting features. It is only when all call appearances are in use that subsequent callers receive either busy tone, voicemail or follow a forward on busy action.

Related links

Appearance buttons on page 87

Bridged appearance buttons

Bridged appearance buttons allow the user to have an appearance button that matches another user's call appearance button.

A bridged appearance button allows a user to answer and make calls on behalf of another user. An audible indication of calls is presented to the bridged user where programmed. The button provides a visual indication of when the other user has calls presented, held or connected. A user can join and exchange calls using the paired call appearance and bridged appearance buttons.

For example, when one user’s call appearance button shows a ringing call, the bridged appearance button on another user’s phone also shows the ringing call and that user can use it to answer the call. Similarly, if a user uses the bridged appearance button to make a call, the call activity shows on the matching call appearance button. The user can join or takeover the call using their call appearance button.

Bridged appearance buttons allow paired “manager/secretary” style operation between two users, and are only supported for users who have call appearance buttons.

Related links

Appearance buttons on page 87

Call coverage buttons

Call coverage buttons allow unanswered calls to alert at other user extensions and be answered there before being forwarded or going to voicemail.

Call coverage buttons allow users to answer a colleague's unanswered call before it goes to voicemail. When a user has an unanswered call ringing, after a configurable delay, the call will also start alerting on any call coverage buttons associated with the user on other extensions. Another user can answer the call by pressing the call coverage button. If the call goes unanswered, the call is forwarded or goes to voicemail.

You can adjust the time a call rings before alerting on associated call coverage buttons.

Related links

Appearance buttons on page 87

Multiple Access Directory Number buttons

Multiple Access Directory Number (MADN) is a key and lamp style feature that permits a user to have multiple appearance of a directory number. Users can have up to thirty appearances of the same directory number. To use MADN features in IP Office environment, the MADN number must be configured as one of the user’s number.

MADN Single Call Arrangement (SCA)

- The directory number can be on 1 or more users.
- Calls alert on all buttons configured with the directory number and any user can answer the call on that button.
- A user can make an outgoing call when the directory number is Idle. The call party details will be the name and number of the selected button.
- When the directory number is in use, other users with the button appearance see the number as busy.
- Users can bridge into calls with privacy settings.

MADN Multiple Call Arrangement (MCA)

- The directory number can be on 1 or more users
- Calls alert on all buttons configured with that directory number and any user can answer the call on that button. After the call is answered, all other users see the number go Idle.
- When the directory number is Idle, the user can select the button to make an outgoing call. The calling party details will be the user’s name and the directory number of the selected button.

Note:

The MADN feature is supported on button sets only and not on analog and DECT phones.

Related links

Appearance buttons on page 87

Chapter 17: Buttons, keys and lamps

IP Office supports up to 10 buttons on each phone and 10 phones with the same line appearance.

The key and lamp features require a phone with buttons and indicators and on certain Avaya digital and IP phones. Key and lamp operation is not supported on analog phones. You can set a ring delay on each appearance button to allow time for the target number to answer before another extension rings, or set a visual alert only — without a ring.

Programmable buttons

Digital and IP phones have dedicated function buttons for mute, volume, hold, conference and transfer. On many digital and IP phones administrator users can program keys and buttons with a range of selected special functions.

These buttons are used for calling other extensions on the system or for other options such as speed dialing numbers and do not disturb. Many features use an indicator to show whether a feature is enabled. Implementation engineers can program buttons as part of the system configuration, although some phones allow users to program buttons and functions where given administration rights.

For more information see Administering Avaya IP Office™ Platform with Web Manager.

Busy lamp field indicators

Busy lamp field (BLF) indicators show when a button or associated feature is active.

Digital and IP phones have programmable buttons which can be assigned to various features. When those buttons include some form of BLF indicator, the button can also be used to indicate when the feature is active. For example, a button associated with another user will indicate when that user is active on a call. A button associated with a group will indicate when the group has calls waiting to be answered.

The directory entries in and the speed dial icons within the Phone Manager and SoftConsole applications also act as BLFs. When the icons are associated with internal users, the icons will change to indicate the current status of the users.

Avaya one-X® Portal for IP Office shows these conditions:

Text or icon	State	Description
available	Available	You are available and can be called.
	Busy	You have a call in progress.
	Do not disturb	You have enabled do not disturb on the phone system. Calls to you are redirected to voicemail if available. Otherwise, the callers receive a busy tone. The exception is calls from numbers that you have added to your list of do not disturb exceptions.
	Logged out	You have not logged into the extension on the phone system. Calls to you are redirected to voicemail if available. Otherwise, the callers receive a busy tone. You cannot make calls. However you can still use to alter your configuration settings.
	Ringing	The phone is ringing and you have an incoming call.
unknown	Unknown	Your presence on the phone system is unknown. The presence cannot be determined as the phone number is not an extension on the system.

External call lamps

Users can determine if covered calls are internal or external based on the indicator flash pattern.

Users can select the lamp flash pattern for external calls on bridged and call coverage appearance buttons.

Message waiting lamps

IP Office uses message waiting indication (MWI) to set a lamp or other indication on phones when a new message has been left for the user, either in a personal voice mailbox or in a group mailbox or call back message. After the system plays the message, it turns the lamp off.

All digital and IP phones have in-built message waiting lamps. Avaya one-X® Portal for IP Office provides message waiting indication on screen.

For analog phones, IP Office provides a variety of analog message waiting indication (MWI) methods:

- 51 V stepped
- 81 V
- 101 V
- Line reversal

The system administrator or installer selects the MWI method using IP Office Manager during configuration to match the properties of the analog phones.

Note:

101V signaling is only available on IP500 phone cards and expansion modules.

Part 3: Applications

Chapter 18: User applications

The following sections provide an overview of the applications intended for end users.

Related links

IP Office User Portal on page 94
Avaya Workplace Client on page 94
Avaya one-X Portal for IP Office on page 97
SoftConsole on page 98

IP Office User Portal

The IP Office user portal is a browser based application that allows users to view and change their settings and to make and answer calls. It is supported in all IP Office modes except Basic Edition.

The system administrator is able to configure which users can access the portal and which portal features they can use.

- Access various different settings such as forwarding numbers and personal contacts.
- Access voicemail messages and call recordings.
- Make and answer calls. This can be done in several ways:
  - Control of the users desk phone.
  - On systems that have been configured with a WebRTC gateway, make and answer calls using through the browser.

Related links

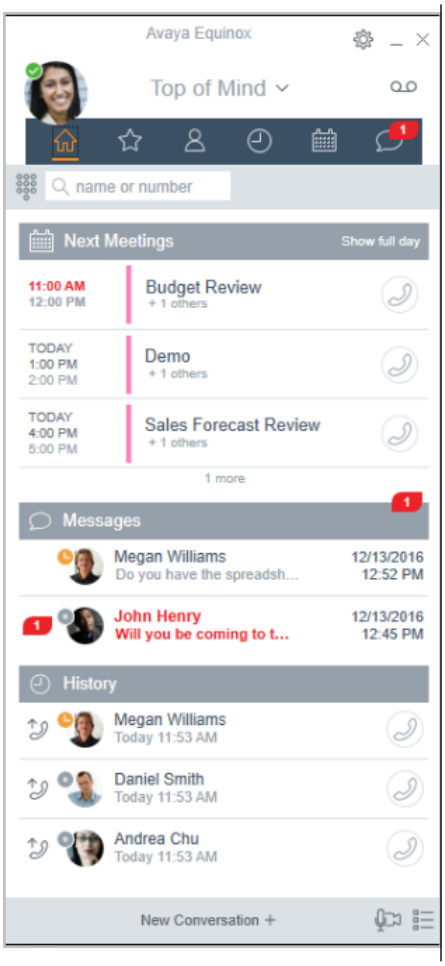
User applications on page 94

Avaya Workplace Client

Avaya Workplace Client is a SIP-based client that provides users with real time collaboration capabilities and enables business users to easily manage their day-to-day communications from a single interface. IP Office supports the following operating systems:

Device	Supported
Desktop PC	Windows and macOS
Mobile phone	Android and iOS. • IP Office iOS support is for iPhone and iPad devices only.
Avaya Vantage™	Yes

Avaya Workplace Client is a common cross-platform client. The client capabilities vary depending on the platform it is registered with. The supported features in Avaya Workplace Client for IP Office are:



- Top of Mind Home Screen
  - Next meetings showing local calendar schedule or Exchange Web Service/Office 365
  - Local Call History
  - Messages
  - Start Meetings/Launch Spaces dashboard
- IP Office directory and local contacts
- Instant messaging
- Presence
- Centralized call log.
- Dialpad with Redial
- Desktop integration with Microsoft Outlook and browsers
- Softphone client audio and video calls
- Shared control of an associated IP Office deskphone.

Avaya Workplace Client registers with IP Office server as a SIP softphone for audio and video calling, and telephony features. The following features are supported:

- Point to point audio and video calls (make, receive, and end)
- Multiple call handling (incoming and outgoing)
- Hold and retrieve (audio and video calls)
- Transfer (blind and consultative)
- Consult conferencing

- Escalate audio to video call
- Share control with supported desk phones in the Avaya Workplace Client desktop.
- CTI Control - Avaya Workplace Client for IP Office can be controlled through other applications such as Avaya Contact Center Select, IP Office Contact Center, IP Office SoftConsole, one-X Portal, Call assistance or Outlook plugin.

  CTI is supported with Avaya Workplace Client for Windows only.
- Apple push notification service- platform notification service created by Apple Inc. With this service, third-party application developers can send notification events to applications installed on Apple devices when the application is idle in the background or is in quit state.
- Avaya Workplace Client on Avaya Vantage™
- Presence and directory integration with Avaya Workplace Client on Avaya Vantage™
- Enter DTMFs during a call

Avaya Workplace Client on Avaya Vantage™ supports the following features:

- Making outgoing calls.
- Handling incoming calls.
- Putting call on hold and resuming the call.
- Muting and unmuting a call.
- Transferring a call.
- Escalating an audio call to video call and de-escalating video call to audio call.
- Entering DTMF digits using the keypad.
- Access your local contacts
- Access your IP Office contacts by using IP Office directory.
- Manage your presence status and presence status messages.

Avaya Workplace Client for IP Office limitations

- Branch worker - Avaya Workplace Client for IP Office does not support failover between Avaya Aura® core and IP Office Branch.
- For instant messaging, Avaya Workplace Client requires either one-X Portal or Avaya cloud services.
- CTI control - Avaya IP Office CTI applications supports mute/unmute control, however it will not visually appear in Avaya Workplace Client.

  IP Office does not support video call controls over CTI.
- The Avaya Workplace Client accesses Workplace Meetings Online using HTTPS, from within the Workplace Meetings tab of the client. The Avaya Workplace Client can access local on-premise Equinox Conferencing in the same way using HTTPS, that is, if the access URL is configured under Workplace Meetings. However, if the Avaya Workplace Client accesses local on-premise Equinox Conferencing through SIP trunks, audio and video will be available but not sharing or conference roster. The same applies for accessing Scopia over SIP trunks too. Even when Avaya Workplace Client accesses local on-premise IP Office Meet Me Conferencing, audio will be available but not sharing or conference roster.

- Apple Push Notification service (APNs) is a platform notification service created by Apple Inc. This service allows iOS users of Avaya Workplace Client to receive notification of new calls, voicemail messages, and other events. They receive these notifications regardless when the Avaya Workplace Client is idle in the background or is in quit state. However, if Avaya Workplace Client is on suspension, then Avaya Workplace Client automatically starts when a new call or instant message notification arrives.

  Unlike the rest of the world, due to the restriction of CallKit in Chinese applications, Avaya Workplace Client does not display incoming call screen using CallKit. However, an incoming call notification is displayed.

Related links

User applications on page 94

Avaya one-X® Portal for IP Office

Avaya one-X® Portal for IP Office provides users control of their telephone from a networked PC. Use this application with any extension; analog, digital or any IP telephone, wired or wireless, that is available as part of the Office Worker, Power User or Teleworker user licenses.

Avaya one-X® Portal for IP Office is a server-based application that the user accesses via web browser.

For Telecommuter mode, One-X applications require answer supervision and disconnect detection for proper functioning. As a result, the one-X applications will not work with trunks that do not support answer supervision and disconnect detection.

Note:

one-X applications function on trunk types such as PRI, BRI, and SIP, however, they will not function on E1R2, T1 RBS and analog loop start trunks.

System administrators can control if Avaya one-X® Portal for IP Office can be accessed over a secure protocol only, recommended for hosted deployments to provide “secure only” access. The other option is to allow users to access the client over a secure and unsecure protocol (HTTP/HTTPS). The client application forces users to change their passwords and voicemail passcodes to meet the complexity settings configured by the administrator.

Through gadgets, Avaya one-X® Portal for IP Office provides the following features:

- Call information
- Call and conference control
- Presence and instant messaging notifications, monitoring and archiving
- Contact import and export
- XMPP groups displayed in the **System Directory** tab
- Support for User Avatar on Avaya one-X® Portal web client **System Directory** tab

- Dial to user's own bridge and invite other users to join
- Conference call and other meeting scheduling including port reservations, email support and automatic report creation — available within the Outlook interface
- One-click web conferencing hosting and single sign-on joining web conferences as a participant
- Display number of **Logged in Sessions** on Avaya one-X® Portal administrator dashboard under User Details section. This shows the number of clients a user is currently logged in. Detailed information on the Logged in sessions is displayed on the Avaya one-X® Portal under Health/Active sessions tab.
- Option to block client versions under configuration.
- Option to clear all sessions for a user.
- Option to track repeated failed login attempts.

Related links

User applications on page 94

SoftConsole

SoftConsole is the PC-based Windows receptionist application for IP Office. It can be purchased with the Receptionist user license.

SoftConsole provides enterprise receptionists and operators with call information and call actions to simplify call handling and instant messaging. With SoftConsole, users see the status of other users and adjust basic telephony settings of other users, such as forwarding numbers. Avaya recommends using phones that support Auto Answer. Users can use instant messaging features provided by Avaya one-X® Portal, if available.

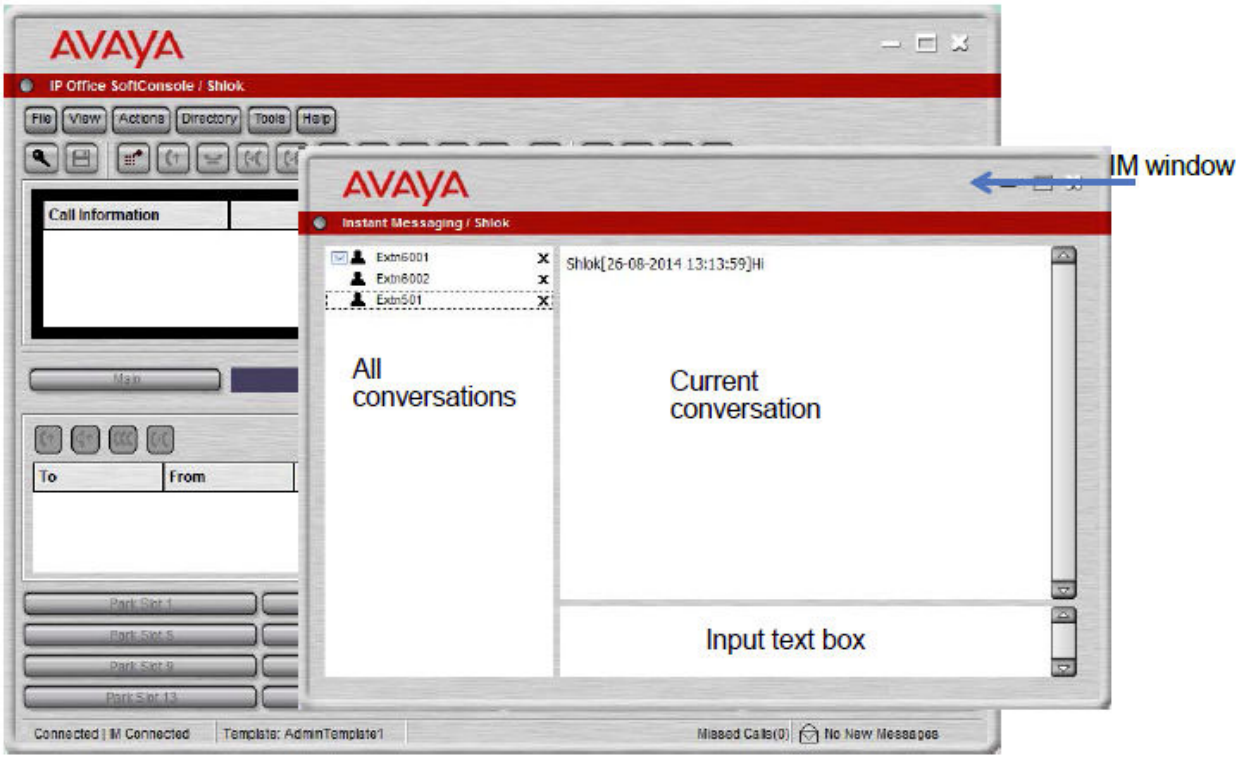


Figure 3: SoftConsole instant messaging window

WebSocket communication allows SoftConsole clients to communicate with IP Office and Avaya one-X® Portal. The WebSocket protocol is bidirectional between the client and the server. As the communication is done over port 80 or 443 (same port used for HTTP), there are no issues with firewall traversal. In a hosted environment, WebSocket communication provides security.

SoftConsole can be minimized in the Windows system tray when not in use, but will pop up on the screen when a call is received. Sound and media files can be associated with calls. If this feature is used, the PC requires a sound card and speakers.

SoftConsole supports the following features:

- Answering calls
- Making outgoing calls
- Supervised and unsupervised transfers
- Transfer calls to voicemail
- Hold and park calls
- Monitoring queues and answering queue calls
- Using and viewing conference rooms
- Conferencing held calls
- Adding users to a conference

- Adding text to a call
- Door release
- Intrude
- Sending text messages
- Paging
- Recording calls
- Sending email
- Using dial pad
- Multiple language support, users can select language

Related links

User applications on page 94

Chapter 19: Administration applications

The following sections provide an overview of the installation and administration related applications.

Related links

IP Office Manager on page 101
Server Edition Manager on page 102
Web Manager on page 104
System Status Application (SSA) on page 104
SysMonitor on page 105
Customer Operations Manager on page 106
SNMP Management Console on page 106

IP Office Manager

Use the Manager to manage IP Office standalone systems or systems in a small community network (SCN). Manager tracks system configuration changes, manages upgrades, and configuration imports and exports.

IP Office has a built-in audit trail that tracks changes to the system configuration, and who has made them. Manager can display the audit trail to assist with problem resolution. The audit trail records the last 15 changes in the configuration and records the following elements:

- Configuration Changed - For configuration changes, the log will report at a high level on all configuration categories (users, hunt group...) that have been changed.
- Configuration Erased
- Configuration merged
- Reboot - user instigated reboot
- Upgrade
- Cold Start
- Warm Start
- Write at HH:MM - This is when the administrator saved the configuration via the schedule option

- Write with Immediate Reboot
- Write with Reboot When Free

IP Office Manager is also used for maintenance functions such as:

- Upgrade to the IP Office system software
- Ability to send software over an IP network link to a system and have it validated before committing to the upgrade
- Backwards compatibility with systems from Release 2.1 onwards to allow a single management application
- Importing and Exporting IP Office configuration information in ACSII-CSV files.

Related links

Administration applications on page 101

Server Edition Manager

Server Edition Manager supports complete centralized administration for Server Edition Primary, Server Edition Secondary, and Server Edition Expansion Systems. Manager also provides IP Office telephony and Unified Communications features.

Manager enables management of all the components within the solution for activities such as:

- Single point of configuration for IP Office and voicemail
- Simple initial installation wizard
- Overview of the system with inventory and status
- Common settings consolidated to the Server Edition Primary
- Integrated Voicemail Proclient, System Status Application, and Linux Platform settings access
- Supports online, offline administration, and configuring a complete solution
- Template operations
- Centralized configuration and template storage
- Administrator account management utility
- Retains existing IP Office expertise
- Context sensitive help

Even though Manager is a Windows application, Manager can be installed directly from the Web administration portal of Server Edition Primary server. This enables you to use any Windows personal computer that has any IP Office Manager that is pre-installed immediately.

The configuration of an existing non-Server Edition system can be converted to a Server Edition configuration, and inturn for Server Edition (Non Select) or (Select) mode the conversion to Subscription mode can be achieved by rerunning **Initial Configuration** menu.

Using Manager, the administrator can create templates for many management items such as users, extensions, Hunt Groups, and Lines. The administrator can then create any new item using

the default settings or the template. You can create multiple users and extensions using one template.

Call Routing Support:

- Full IP Office ARS and dial plan support
- Default routing simplifies configuration
- Solution wide auto line group numbering
- Common incoming call routes provide resilience
- Resilient Hunt Groups

Offline Operation:

- Complete solution can be created and/or managed offline if required
- Can still manage when some deices offline
- On/offline configuration sync options to harmonize as required

Solution Management:

- Complete solution view with status and inventory
- Users and Hunt Groups are solution wide
- Centralized User Rights, feature short codes, Time Profiles, Incoming Call Routes, and Account Codes
- Permits advanced per-device configuration if desired
- All configurations stored on primary server
- Solution wide system directory
- Easy management of central and per-device licenses

Resilience management:

- You can manage every device locally for ‘rainy day’ events
- You can manage the solution through a secondary server when the primary server fails or in a split WAN setup
- On/Offline configuration sync options to harmonize as required

Add or Remove Devices:

- Single process for addition or removal of device
- Built-in Initial Configuration Utility (ICU) to simplify adding a new device
- Common configuration items from primary server is auto populated
- Can configure before you install a new device

Validation :

- Configuration validation on read and any change.
- Solution wide validations

Template:

- Create a local and centralized template from an existing Line, Extension, User, Hunt Group, Time Profile, Firewall Profile, IP Route and Service entries
- Recreate multiple Extension and Users from one template

Remote access:

- Supports access from service through SSL VPN

Security:

- Single Sign On to all except one-X Portal administration

Related links

Administration applications on page 101

Web Manager

Web Manager is a browser-based management tool designed to simplify the installation and maintenance process and provides access to most, but not all, IP Office configuration settings. Web Manager eliminates the need to have Windows PC for administration.

Granular access:

Web Manager provides service users with access to entire configuration objects if the service user has the configuration access. However, large customers who have multiple service users roles or customers having deployments in the cloud environment need to have granular configuration access for different service users. Hosting partners will be able to build an account for customer or re-seller with limited permissions. These permissions shall restrict the customer or re-seller from performing activities that affects service of the system.

Configuration dashboard:

The Dashboard is a simplified version of the existing IP Office Web Manager and is presented to the administrators when a fresh single-node IP Office system is installed. The Dashboard consists of minimum required set of configuration fields to set up the system. The full setup can be performed anytime afterwards.

Related links

Administration applications on page 101

System Status Application (SSA)

The System Status Application (SSA) is a diagnostic tool for system managers and administrators to monitor and check the status of IP Office systems locally or remotely. SSA shows both the

current state of an IP Office system and details of any problems that have occurred. SSA is not a configuration tool for IP Office systems.

The information reported is a combination of real-time events, historical events, status and configuration data to assist fault finding and diagnosis. SSA provides real-time status, historic utilization and alarm information for ports, modules and expansion cards on the system.

There can be up to two (2) SSA clients connected to an IP Office unit at one time.

SSA provides information on the following:

Item	Description
Alarms	SSA displays all alarms which are recorded within IP Office for each device in error. The number, date and time of the occurrence is recorded. The last 50 alarms are stored within IP Office to avoid need for local PC.
Call Details	Information on incoming and outgoing calls, including call length, call ID and routing information.
Extensions	SSA details all extensions (including device type and port location) on the IP Office system. Information on the current status of a device is also displayed. SSA shows IP Extensions that were registered but no longer available and IP extensions that are configured but have not been registered after last re-boot. This helps to spot phones that are Idle, disconnected, or are misconfigured. SSA also shows quarantined phones and blacklisted extensions and IP addresses.
Trunks	IP Office trunks and connections (VoIP, analog and digital) and their current status are displayed. For VoIP trunks, QoS information is also displayed (for example roundtrip delay, jitter and packet loss).
System Resources	IP Office includes central resources that are utilized to perform various functions. Diagnosing these resources is often critical to the successful operation of the system. This includes details on resources for VCM, Voicemail and conferencing.
QoS Monitoring	QoS Parameters from connected calls, such as jitter and roundtrip delay, are monitored.

Related links

Administration applications on page 101

SysMonitor

Use SysMonitor to troubleshoot IP Office from both local (LAN) and remote locations (WAN).

Select the protocols and interfaces to monitor and diagnose through a graphical interface. Capture traces directly to the screen or as a log file for later analysis. Color code different traces to improve the clarity in large files. The utility also captures system alarms and displays the activity log of the last 20 alarms that have occurred.

Related links

Administration applications on page 101

Customer Operations Manager

Customer Operations Manger is an administration tool that allows multi-customer management of subscription mode IP Office systems. It is accessed by browser from the same cloud-based servers that are providing the subscriptions for systems.

The tool enables management of IP Office Server Edition systems and provides the following capabilities:

- Dashboard that displays error conditions, ongoing system activities, and system health
- Grouping of systems based on versions and tags for accessing similar systems at the click of a button
- Displays all connected systems such as Primary, Secondary, Expansions, and open applications
- Ability to centrally manage IP Office software backup, restore and upgrade actions.
- Role-based administration. Customer Operations Manager has its own service users with access to complete or selective customers IP Office.
- Provides facility to launch Native IP Office Management applications. Uses need to log in to the applications separately after the application is launched.
- Alarms for Configuration, Services, Trunks, Link, and Security by Severity type
- Alarms for status of IP Office systems indicating whether they are online of offline
- Alarms indicating status of various applications

Related links

Administration applications on page 101

SNMP Management Console

Simple Network Management Protocol (SNMP) is an industry standard designed to allow the management of data equipment from different vendors using a single Network Manager application. The Network Manager periodically polls equipment to solicit a response, if no response is received an alarm is raised. In addition to responding to polls, IP Office monitors the state of its Extensions, Trunk cards, Expansion Modules and Media cards so that if an error is detected IP Office will notify the Network Manager.

As the IP Office platform comprises many applications, the core software notifies SNMP events from both Voicemail Pro and Embedded Voicemail to warn of approaching storage capacity limits.

IP Office sends email notifications directly to the email server; no additional PC client is needed.

On customer sites where SNMP management is not available, IP Office can email events using up to 3 email addresses each containing a different set of alarms.

The following system event categories can be chosen for email notification, if installed on the system:

- Generic
- Trunk lines
- Embedded Voicemail Card
- VCM
- Expansion modules
- Applications
- License
- Phone change
- CSU Loop-Back

IP Office has been tested against CastleRock's SNMPc-EE™ and HP's Network Node Manager (part of the OpenView application suite).

Related links

Administration applications on page 101

Chapter 20: Branch Systems

IP Office systems can be connected to other Avaya telephony systems in order to act as local branches.

Related links

Centralized management on page 108
Centralized licensing on page 108
Voice mail systems on page 109
Avaya Aura Session Manager on page 109
Avaya Aura Communication Manager on page 109

Centralized management

With the distributed, mixed, and centralized deployment models, you can use Avaya Aura® System Manager to centrally manage all components in the solution. System Manager manages the centralized applications and services included in the solution, IP Office systems in the branch, as well as centralized users and IP Office users. For certain capabilities that cannot be managed centrally, System Manager launches IP Office Manager in the appropriate mode where you can remotely administer individual IP Office systems.

Centralized management of components through Avaya Aura® System Manager is optional. For example, you can choose to directly manage IP Office systems through IP Office Manager.

With the stand-alone IP Office branch option, centralized management is not available. You must manage all IP Office systems directly though IP Office Manager.

Related links

Branch Systems on page 108

Centralized licensing

With a distributed, mixed, or centralized deployment connected to the Avaya Aura® network, you can access centralized licensing capabilities through the System Manager Avaya WebLM server. With centralized licensing, a single license file is generated in the Product Licensing and Delivery System (PLDS) for multiple branches.

To use centralized licensing, the enterprise must obtain a WebLM licence from PLDS for each IP Office branch. Centralized licensing is not available in stand-alone IP Office branch environments.

Related links

Branch Systems on page 108

Voice mail systems

The IP Office Branch solution supports IP Office voice mail systems and centralized voice mail systems.

The IP Office Embedded Voicemail system is included with the IP Office Essential Edition, and the IP Office Voicemail Pro system is included with the IP Office Preferred and Advanced Editions.

The Branch solution supports the following three centralized voice mail systems as additional components within the solution:

- Avaya Aura® Messaging
- Avaya Modular Messaging
- Avaya CallPilot®: Only supported in distributed branch environments connected to CS 1000.

Avaya Aura® Session Manager

Avaya Aura® Session Manager handles call admission control, call re-direction, digit analysis, dial plan management, internal network call accounting feeds, toll by-pass, inter-office routing and international least cost routing. All administration and management of the enterprise-wide private global dial plan network is handled by this communications appliance, and managed as a single enterprise with Avaya Aura® System Manager.

Session Manager plays a different role for centralized users and IP Office users in deployment environments connected to Avaya Aura®. For IP Office users, Avaya Aura® Session Manager acts as a SIP proxy to route SIP sessions to and from the SIP connections to the IP Office. For centralized users, Avaya Aura® Session Manager is also the main interface that handles user registration and call routing.

Avaya Aura® Communication Manager

Centralized users register to Avaya Aura® Session Manager and obtain telephony services from the Avaya Aura® Communication Manager Feature Server or Evolution Server in the enterprise core. Avaya Aura® Communication Manager does not provide any functionality to IP Office users.

Chapter 21: Avaya Contact Center Select overview

Avaya Contact Center Select is a context-sensitive, collaborative, voice and multimedia contact center solution that allows small to midsize enterprises to anticipate, accelerate, and enhance customer interactions. Avaya Contact Center Select uses the Avaya IP Office telephone system to provide a real-time telephony platform.

Avaya Contact Center Select uses industry-standard SIP and CTI interfaces to integrate with IP Office. This integration gives Avaya Contact Center Select access to and control of a wide range of IP Office phones and features. Customers integrating Avaya Contact Center Select with IP Office gain skill-based routing, call treatments, reporting, unified agent management, and the graphical Orchestration Designer utility.

Avaya Agent Desktop is a single-interface client application used by Avaya Contact Center Select agents to assist customers. Avaya Contact Center Select agents use Agent Desktop software to respond to customer voice and multimedia contacts. Agent Desktop supports a range of IP Office phones and a wide variety of multimedia contact types.

By default, Avaya Contact Center Select connections and Web Services use secure TLS communication. The Avaya Contact Center Select Certificate Management tool makes it easier to manage security certificates.

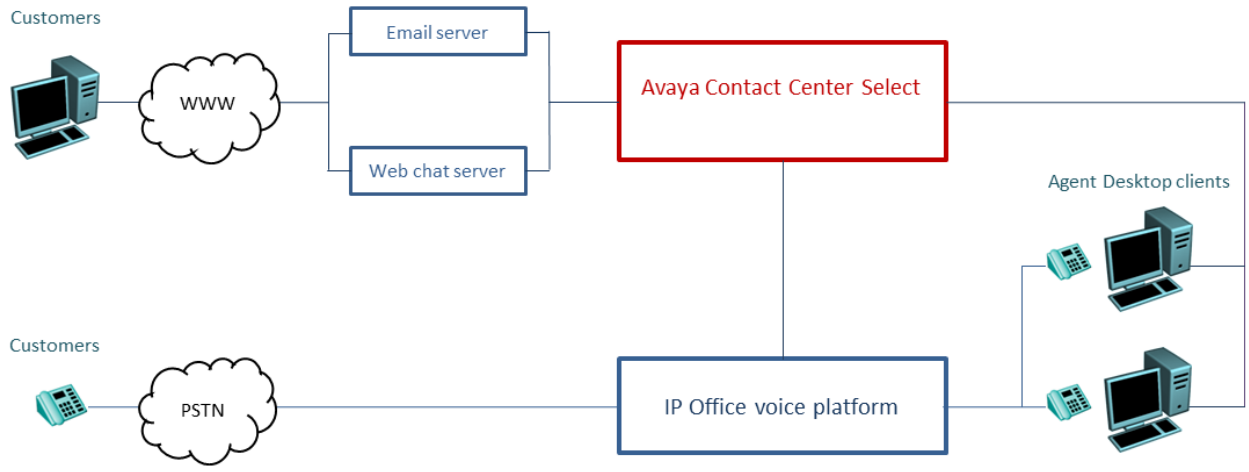


Figure 4: Typical contact center solution using voice and multimedia Avaya Contact Center Select and the Avaya IP Office voice phone system

Avaya Contact Center Select provides a feature-rich voice and multimedia solution with integrated routing and reporting for small to midsize enterprises. Avaya Contact Center Select provides unified contact center and IP Office phone user account management for agents and supervisors. Voice-enabled agents and supervisors created in Avaya Contact Center Select are automatically added to IP Office. Avaya Contact Center Select synchronizes user (agent and supervisor) information between Avaya Contact Center Select and IP Office.

Part 4: Miscellaneous

Chapter 22: Standards

Regulatory standards

Quality of Service standards

Every customer will have different expectations and different budgets to work to. Some will be willing to upgrade their networks to use the best possible equipment and practices. To others the additional expense may be viewed as unnecessary. Examples of standards based Quality of Service protocols include:

- 802.1Q (Layer 2)
- DiffServ (Layer 3)
- Port Range (Layer 4)
- 802.1X (MD-5)

Voice compression codecs

The bandwidth used varies depending on the compression method chosen. IP Office supports standards listed below. These will occupy approximately 10K and 13K of bandwidth respectively. Use the following chart to choose the most appropriate compression algorithm for your available bandwidth.

Audio Codec	RTP Voice Data Payload (bytes)	Packets per second	LAN (bps)	% overhead LAN	WAN (bps)	% overhead WAN	Algorithmic delay (ms)
G.723.1 (6.3K)	24	33.33	20,800	225%	9,867	54%	80
G.729a	20	50	29,600	270%	13,200	65%	40
G.711 (64K)	160	50	85,600	34%	69,200	8%	20
G.722 (64K)	160	50	85,600	34%	69,200	8%	20

VoIP standards

IP Office supports the following protocols and standards:

H.323 V2 (1998) Packet-based multimedia communications systems.

Q.931 ISDN user-network interface layer 3 specification for basic call control.

H.225.0 (1998) Call signaling protocols and media stream packetization for packet-based multimedia communication systems.

H.245 (1998) Control protocol for multimedia communication.

SIP Session Initiation Protocol

T.38 Fax standard

Internet standards (In addition to TCP/UDP/IP.)

Standard	Description
RFC 1889	Real Time Protocol (RTP) and Real Time Control Protocol (RTCP)
RFC 2507, 2508, 2509	Header compression
RFC 2474	DiffServ, Type of Service field configurable
RFC 1990	PPP fragmentation
RFC 1490	Encapsulation for Frame Relay
RFC 2686	Multiclass Extensions to Multilink PPP
RFC 3261	SIP
RFC 3489	STUN

Analog trunk standards

IP Office analog trunk cards conform to the standards:

TIA/EIA-646-B Loop Start

GR-188-CORE and GR-31-CORE Incoming Caller line identification (ICLID)

ANSI T1.401 and TIA/EIA-646-B Ground Start (not available in all localities)

Database interface standards

IP Office supports the ActiveX Data Object (ADO) interface standard.

PCI Security Standard Council standards

Leading credit card companies defined standards in the PCI Security Standard Council and one of these standards is not recording credit card numbers given by the customer.

Networking protocol standards

Protocol	RFC	Description
Point-to-Point Protocol (PPP)	RFC1661	WAN protocol that allows interworking with a wide range of third-party routers. PPP is used over leased line circuits where a single channel is used to connect the two locations together. For example, a single channel maybe a 64K channel on a dial-up circuit or a 256K leased line etc.
Link Control Protocol (LCP)	RFC1570	In PPP, LCP establishes, configures and tests data-link Internet connections.
Multi-Link Point-to-Point Protocol (ML-PPP)	RFC1990	Allows additional calls to be made where bandwidth greater than a single channel is required. The maximum number of channels available to data can be set on a service-by-service basis. When the available bandwidth reaches a user defined limit additional channels can be automatically added. Similarly, when traffic falls then the number of channels in use can be automatically reduced. If there is no data traffic on any of the channels in use then all lines can be cleared. Since most carriers have a minimum charge for calls, the period that a channel has to be idle before clearing is configurable. Through these mechanisms call costs can be effectively controlled while ensuring that bandwidth is available as and when it is needed.
Internet Protocol Control Protocol (IPCP)	RFC1332	A Network Control Protocol (NCP) for establishing and configuring IP over a PPP.
Internet Protocol Header Compression (IPHC)	-	Reduces the header size of the data packet to gain bandwidth efficiency over WANs, but adds to transmission latency.
Password Authentication Protocol (PAP)	RFC1334	A method of authenticating the remote end of a connection using unencrypted passwords.
Real-time Transport Protocol (RTP) Real-time Transport Control Protocol (RTCP)	RFC1889	RTP defines a standardized packet format for delivering audio and video over IP networks. RTCP works with RTP to send control packets to call participants to provide feedback on the quality of service.
Challenge Handshake Authentication Protocol (CHAP)	RFC1994	Allows an incoming data call to be authenticated using encrypted passwords. The system also provides the option to periodically reaffirm the authenticity of the caller during the data call.
Compression Control Protocol (CCP)	RFC1962	Configures, enables and disables data compression algorithms on both ends of the PPP link. Also used for signal a failure.

Table continues…

Protocol	RFC	Description
Light-weight Directory Access Protocol (LDAP)	RFC4510	Allows the telephone number directory (names and telephone numbers) held in IP Office to be synchronized with the information on an LDAP server (limited to 5000 entries). Although targeted for interoperation with Windows 2000 Server Active Directory, the feature is sufficiently configurable to interoperate with any server that supports LDAP version 2 or higher.
Microsoft Point-to-Point Compression (MPPC)	RFC2118	Data compression method for greater throughput on slow speed WAN links.
Bandwidth Allocation Control Protocol (BACP)	RFC2125	Allows the negotiation with the remote end of the data call to request additional calls to be made to improve aggregate data throughput.
User Datagram Protocol (UDP)	RFC768	A simple connectionless transmission model with a minimum of protocol mechanism used to allow applications to send messages (datagrams) to other hosts on an IP network without prior communications to set up special transmission channels or data paths.
Internet Protocol (IP)	RFC791	A set of rules governing the format of data sent over the Internet or other network.
Transmission Control Protocol (TCP)	RFC793	A connection is established an maintained until the application at each end have finished engaging messages.
Dynamic Host Configuration Protocol (DHCP)	RFC1533	Dynamically distributes network configuration parameters on and IP network such as IP addresses for interfaces and services.
Network Address Translation (NAT)	RFC1631	A mechanism that allows the use of different IP address on a private network behind a router with a public IP Address. When connecting to the Internet, ISPs typically want a customer to use an IP address they have allocated. Using NAT this is easily accommodated, eradicating the need for the customer to change their network numbering scheme and providing additional security to the internal users as their address in hidden to the public. Typically, a company maps its internal network addresses to a global external IP address and unmaps the global IP address on incoming packets back into internal IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process. This also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves the number of global IP addresses that a company needs.

Table continues…

Protocol	RFC	Description
Bootstrap Protocol (BOOTP)	RFC951	Automatically assigns an IP address to network devices from a configuration server on an IP network.
Trivial File Transfer Protocol (TFTP)	RFC1350	A simple protocol to transfer files implemented on top of the UDP using port number 69.
Network Time Protocol (NTP)	RFC868	Provides clock synchronization between computer systems over packet-switched, variable latency data networks.
Proxy Address Resolution Protocol (ARP)	-	Support for Proxy Address Resolution Protocol allows IP Office to respond on behalf of the IP address of a device connected to it when receiving an ARP request.
Simple Network Managment Protocol (SNMPv1)	RFC1157 RFC1155 RFC1212 RFC1215	Simple Network Management Protocol. (STD15) Structure and identification of management information for TCP/IP based internets. (STD16) Concise MIB Definitions. (STD16) A convention for defining traps for use with SNMP
Managment Information Base (MIB-II)	RFC1213	Management Information base for network management of TCP/IP based internets: MIB-II. (STD17)
ENTITY MIB	RFC2737	Entity MIB (Version 2)
Routing Information Protocol (RIP)	RFC1058 RFC2453 RFC1722	Adistance vector protocol that allows routers to determine the shortest route to a destination network. It does this by measuring the number of intermediary routers that need to be traversed to reach the destination network. If more than one route exists to the same destination the shortest route is used. If a fault occurs on the shortest route it will be remarked as being infinite and any alternative route will become the new shortest route. This behavior can be used to add resilience into a data network. Where a customer has an existing data network comprising of third party routers, IP Office added to the network can provide back up using its routing and dial-up capability. RIP enabled routers share their knowledge of the network with each other by advertising and listening to routing table changes. IP Office Supports both the RIP I and RIP II standards.

Table continues…

Protocol	RFC	Description
Internet Protocol Security (IPSec)	RFC2401 RFC2402 RFC2403 RFC2404 RFC2405 RFC2406 RFC2407 RFC2408 RFC2409 RFC2410 RFC2411	Security Architecture for the Internet Protocol IP Authentication Header The Use of HMAC-MD5-96 within ESP and AH The Use of HMAC-SHA-1-96 within ESP and AH The ESP DES-CBC Cipher Algorithm with Explicit IV IP Encapsulation Security Payload. (ESP) The Internet IP Security Domain of Interpolation for ISAKMP Internet Security Association and Key Management Protocol The Internet Key Exchange The NULL Encryption Algorithm and its Use with IPSec IP Security Document Roadmap
Layer 2 Tunneling Protocol (L2TP)	RFC2661 RFC3193	PPP authentication using PAP or CHAP takes place between directly connected routers only. When using a public IP Network to connect sites this authentication takes place between the customers router and the service provide router that it is connected to. In some circumstances it is desirable to authenticate between the customer owned routers, jumping over all the intermediary routers of the service provider's network. Layer 2 Tunneling Protocol allow this to happen by facilitating a two stage authentication, firstly with the service provider router then the customer router on the remote network. IPSec tunnels allow a company to pass data between locations over unsecured IP networks such as the public internet. The company data is secured using 3DES encryption making it unintelligible to other parties that might be 'eaves dropping' on the traffic. Tunneling can be applied to link offices together or provide workers access to the office over the internet. All IP Office systems support up to a total of 256K worth of encrypted traffic to multiple locations. Initially, inter-working is supported only between IP Offices that are connected either directly on a WAN port or via the LAN using a third-party router. IPSec is optional and enabled on IP Office through a License Key.
Differentiated Services (DiffServ)	RFC2474	Networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying and managing network traffic and providing quality of service (QoS) on IP networks.
Frame Relay Encapsulation	RFC 1490	Multi protocol Interconnect over Frame Relay

Session Initiation Protocol (SIP) standards

Rec. E.164 [2]	ITU-T Recommendation E.164: The international public telecommunication numbering plan
RFC 2833 [7]	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
RFC 3261 [8]	SIP: Session Initiation Protocol
RFC 3263 [10]	Session Initiation Protocol (SIP): Locating SIP Servers
RFC 3264 [11]	An Offer/Answer Model with Session Description Protocol (SDP)
RFC 3323 [14]	A Privacy Mechanism for the Session Initiation Protocol (SIP)
RFC 3489 [18]	STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
RFC 3824 [24]	Using E.164 numbers with the Session Initiation Protocol (SIP)
RFC 1889	RTP
RFC 1890	RTP Audio
RFC 4566	SDP
RFC 3265	Event Notification
RFC 3515	SIP Refer
RFC 3842	Message Waiting
RFC 3310	Authentication
RFC 2976	INFO
RFC 3323	Privacy for SIP (PAI) and draft-ietf-sip-privacy-04 (RPID)
RFC 3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
RFC 3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
RFC 3311	The Session Initiation Protocol (SIP) UPDATE Method

Part 5: Further Help

Chapter 23: Additional Help and Documentation

The following pages provide sources for additional help.

Related links

Additional Manuals and User Guides on page 121
Getting Help on page 121
Finding an Avaya Business Partner on page 122
Additional IP Office resources on page 122
Training on page 123

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 122).

Related links

Additional Help and Documentation on page 121

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 122.

Related links

Additional Help and Documentation on page 121

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 121

Additional IP Office resources

In addition to the documentation website (see Additional Manuals and User Guides on page 121), 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 121

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 121

Glossary

Automatic Route Selection	A feature of some telephone systems in which the system automatically chooses the most cost-effective way to send a toll call.
Busy Hour Call Completions	A measure of dynamic traffic calls that can be completed in an average busy hour.
Communication Manager	A key component of Avaya Aura®. It delivers rich voice and video capabilities and provides a resilient, distributed network for media gateways and analog, digital, and IP-based communication devices. It includes advanced mobility features, built-in conference calling, contact center applications and E911 capabilities.
Computer Supported Telecommunications Application (CSTA)	A standard interface for Computer Telephony Integration (CTI) applications, such as voice mail and auto-attendant, to interact with telephony equipment.
Digital Communications Protocol	A proprietary protocol that is used to transmit both digitized voice and digitized data over the same communications link. A Digital Communications Protocol (DCP) link consists of two 64-kbps information (I) channels, and one 8-kbps signaling (S) channel. The DCP protocol supports two information-bearing channels and two telephones or data modules.
Directory Enabled Management	An interface that uses Avaya Directory Server to facilitate administration of Modular Messaging from a centralized location.
Distributed Communications System	A proprietary inter-networking protocol from Avaya with which you can configure two or more Avaya-based private communication networks to operate as one, large network.
Domain Name System (DNS)	An Internet Engineering Task Force (IETF) standard for ASCII strings to represent IP addresses. The DNS is a distributed internal directory service used mostly to translate between domain names and IP addresses. Avaya 9600 Series IP Telephones can use DNS to resolve names into IP addresses. In DHCP, TFTP, and HTTP files, DNS names can be used whenever IP addresses are available as long as a valid DNS server is identified first.

Dynamic Data Exchange (DDE)	An interprocess communication (IPC) method.
Dynamic Host Configuration Protocol (DHCP)	An Internet Engineering Task Force (IETF) protocol used to automate IP address allocation and management.
Ethernet Routing Switch (ERS)	The Avaya stackable chassis system that provides high-performance, convergence-ready, secure, and resilient Ethernet switching connectivity.
Expansion Interface	A port circuit pack in a port network (PN) that provides the interface between a time-division multiplex (TDM) bus or a packet bus on the PN and a fiber-optic link. Expansion interface (EI) carries circuit-switched data, packet-switched data, network control, timing control, and digital signal-1 (DS1) control. EI in an expansion port network (EPN) also communicates with the master maintenance circuit pack to provide the environmental status and the alarm status of the EPN to the switch processing element (SPE).
Expansion port network	In Intuity Audix Server configurations, a port network (PN) that is connected to the time-division multiplex (TDM) bus and the packet bus of a processor port network (PPN). Control is achieved by indirect connection of the EPN to the PPN by way of a port network link (PNL).
Extension to Cellular access number	The phone number dialed to connect to the Avaya server that is running Communication Manager. The Extension to Cellular access number initiates the process of enabling or disabling Extension to Cellular or changing the station security code.
Federal Communications Commission (FCC)	A United States federal agency that regulates communications such as wire-line communications and the Internet.
Global Technical Services	An Avaya team that answers customer calls about products in Avaya Integrated Management.
Internet Protocol	A connectionless protocol that operates at Layer 3 of the Open Systems Interconnect (OSI) model. Internet Protocol (IP) is used for Internet addressing and routing packets over multiple networks to a final destination. IP works in conjunction with Transmission Control Protocol (TCP), and is identified as TCP/IP.
Local Survivable Processor	A configuration of the S8300 media server in which the server acts as an alternate server or gatekeeper for IP entities such as IP telephones and G700 media gateways. These IP entities use the Local Survivable Processor (LSP) when the IP entities lose connectivity with the primary server.

Media gateway	An application-enabling hardware element that is part of a family of such elements. This family includes intra-switch connectivity, control interfaces, port interfaces, and cabinets. Avaya media gateways support both bearer traffic and signaling traffic that is routed between packet-switched networks and circuit-switched networks to deliver data, voice, fax, and messaging capabilities. Media gateways provide protocol conversion, such as IP to ATM to TDM, conferencing, presence, such as on-hook or off-hook, connectivity to private networks and public networks, such as IP, ATM, TDM, and networking, such as QSIG, DCS, ISDN. Media gateways support optional form factors.
Network Address Port Translation	A network routing technique. Network Address Port Translation (NAPT) is used to access systems on the same subnet as an IP Office.
Network Routing Policy	An application for centrally managing SIP routing for Session Manager instances. A routing policy describes how a call is routed: where it comes from, where it's going, what its dial pattern is, what time of day it is routed, and its cost for a particular route.
OFCOM	The United Kingdom Office of Communication for the regulation of telecommunications.
Product Information Presentation System	The Product Information Presentation System (PIPS) reports provide data from the Product Information Expert (PIE), a data mining tool that extracts Avaya customer switch and adjunct configuration information and stores it in a database.
Product Licensing and Delivery System (PLDS)	The Avaya licensing and download website and management system. Avaya Business Partners and customers use this site to obtain ISO image files and other software downloads.
Public Switched Telephone Network (PSTN)	A telephone network that includes many communication technologies such as microwave transmission, satellites, and undersea cables.
Remote Feature Activation	A Web-based Avaya application to remotely activate features and increase capacities on the system of a customer by delivering a new license file.
System Manager	A common management framework for Avaya Aura® that provides centralized management functions for provisioning and administration to reduce management complexity. System Manager can also function as a self-signed Root Certificate Authority (CA) or as an intermediate CA. System Manager enables the Simple Certificate Enrollment Protocol (SCEP) application to sign certificates for Avaya deskphones.
System Status Application	An IP Office application that shows the status of things such as outgoing calls.

Telecommuter	The configuration where Communication Manager establishes the voice connection to a circuit-switched telephone. Requires two connections: a TCP/IP connection for signaling control and a circuit-switched connection for voice.
Telephony Application Program Interface (TAPI)	A Microsoft® Windows API that enables computers running Windows to use telephony services. TAPI is used for data, FAX, and voice communications. Applications can use TAPI to control telephony functions, such as dial, answer, and hang up.
Telephony Service Provider Interface (TSPI)	A Microsoft-defined interface to the telephony service provider (TSP). Microsoft® Windows comes with an H.323 TSP, an IP conference TSP, a kernel-mode device driver TSP, and a unimodem TSP.

Index

Numerics

1500 DECT extensions 15

A

absence text 23
account codes 36, 39
ACO persistent gateway 15
Acquire Call 37
addressing
    Domain Name Service 79
Administrator 85, 121
agent login 38
alerting 83
allocated 79
Alternate Route Selection 34, 72
announcements 43
Announcements 45
APIs 122
Applicable 85
Application Notes 122
ARS 34, 72
assign call on agent answer 44
assigning calls 44
authorization codes 39
Auto Connect 73
automatic callback 17
Avaya Contact Center Select
    overview 110
Avaya Workplace for IP Office 94

B

Base 80
Base Unit 80
Basic Rate 78, 80
BLF 90
blind transfers 22
bridged appearance buttons 87, 88
business partner locator 122
busy lamp field 90
buttons 90

C

call appearance buttons 87
call barring 33, 39, 40
call costing 36
call coverage buttons 87, 88
call handling
    outbound calls 39
call history 83
call intrude 25
call logs 36
call redirection 50
call screening 18
Call Steal 37
call tagging 25
call waiting 21, 25
callback 17, 73
Callback Control Protocol 73
caller ID 84
calls
    acquiring 37
    barring 39
    forwarding 18
    inbound directory name display 48
    incoming routing 41
    monitoring 38
CBCP 73
CDRs 39
Central Office 79
centralized licensing 108
centralized management 108
Centralized Personal Directory 84
centralized telephony 55
CHAP 80
Clock 80
cloud 46
    authorization 46
Communication Manager 109
compression 53
Conference Bridge 75
conference calls 26
conference join 28
conferencing 50
Control Protocol 73
courses 122
coverage to operator 19, 33
CP 73
customer operations manager 106

D

Data Call 75
DDI 34
DECT R5 15
default numbering 34
delayed dial on pickup 28
DHCP 79, 80
DHCP Server 79
dial emergency 33
dial out privileges 35
dial plan 34

Dial-Up Circuit Support 78
dialing in 80
DID 34
Direct Inward Dialing 34
direct media path 47
directory name display 48
distinctive ringing 17
DND 28, 34
DNS 79
do not disturb 28
Domain 79
Domain Name Service 79
DTMF 49

E

E1/T1 ..... 78, 80
early media 47
Email 80
emergency calling 29
End of support 12
end user applications 94
Ethernet 79, 80
Ethernet Ports 79
Ethernet Switch 79, 80
exception list 28
extensions
    auto-create 46
external call lamps 91

F

Fallback Twinning 70
fast start 47
fax transport 48
firewall
    Small Office Edition offers 80
firewalled 79
firewalled Layer 79
firewalls 73, 80
follow me 19
forced account codes 36
forums 122
forward hunt group 19
forward on busy 19
forward on no answer 20
forward unconditional 20
forwarding calls 18
Frame Relay 79, 80
framed 79, 80
FTP 73

G

Gateway 79, 80

H

Handset 75, 85
headset 30
Help 121
hold 20, 21, 29
Hold 79
hold music 37
hook 30
Hook 85
Hook Dialing 85
hot desking 64
hotline 28
Hunt Group Calls 75
Hunt Group Enable/Disable 29
hunt groups 43
    announcements 43
    Night Service mode 44
    overflow groups 44

I

idle line preference 40
incoming call routing 41
incoming calls
    ring tones 83
India toll bypass 31
indicators
    busy 90
Integral 10/100 Mbit Layer 80
internet access 74
Internet Access 75
internet access restrictions 42
intrude 25, 29
IP Office applications
    installation and administration applications 101
    user applications 94
IP Office editions 10
IP Phones 85
IP412 ..... 79, 80
IP500 ..... 79, 80
IPv6 13
ISDN 78–80

K

key and lamp operation 90
key system mode 40
keys 90

L

lamps 90
Language 85
LCP 73
Leased Line 78, 79

Leased Line *(continued)*
types ... 80
Leased Line Support ... 80
Least Cost ... 75
Least Cost Routes ... 75
least cost routing ... 72
licensing ... 108
line appearance buttons ... 87
Link Control Protocol ... 73
linked numbering ... 75
Local Area Network ... 79, 80

M

madn
buttons ... 89
management ... 108
Manager ... 101
Manuals ... 121
maximum call length ... 34
message waiting ... 91
message waiting lamps ... 91
messaging ... 58, 59
messaging feature comparison ... 59
Monitor ... 85
monitoring calls ... 38
Multiple Time Entries ... 75
multisite networking ... 76
music on hold ... 37
MWI ... 91

N

network numbering ... 75
network protocols ... 115
networking
multisite ... 76
SCN ... 76
new features ... 12
new in this release
R12.0 ... 12
R12.1 ... 13
R12.1 SP1 ... 15
night service ... 43
node numbering ... 75
numbering schemes ... 75

O

Off-Hook Station ... 30
one-X Portal for IP Office ... 97
out of service ... 43
Out of Service mode ... 44
outbound call handling ... 40
overflow groups ... 44
overview ... 10
overview *(continued)*
Avaya Contact Center Select ... 110

P

paging ... 35
PAI and privacy headers ... 49
PAP ... 80
park ... 21
persistent gateway ... 15
Personalized ringing ... 21
phones
appearance buttons ... 87
bridged appearance buttons ... 88
call appearance buttons ... 87
key and lamp operation ... 90
programming buttons ... 90
pickup ... 30
Point-to-Point ... 79, 80
Point-to-Point Protocol ... 79
PPP ... 79
PRACK ... 47
private calls ... 40
programmable buttons ... 90
protocols ... 115
PSTN toll bypass ... 50
Public ... 75, 80

Q

queue threshold alert ... 45
Quick Reference Guides ... 121
Quotas ... 75

R

R12.1 ... 13
R12.1 SP1 ... 15
rainy day ... 56
RAS ... 80
reclaim calls ... 31
redundancy ... 56
regulatory standards ... 113
relay ... 31
Release 4.1 ... 75, 80
remote access ... 65
Remote Access ... 80
Remote Access Server ... 80
remote hot desking ... 65
remote worker ... 66
Reseller ... 121
Rest ... 79
Restrict Network Interconnect ... 31
ring tone on transfer ... 22
ring tones ... 83
ringback ... 17

Rocky Linux 12
router alleviates 79

S

sales 122
SCN 76
screening calls 18
SDKs 122
Self-administration 94
Self-Administration 85
Server Edition Manager 102
servers provide 79
service 46
Session Manager 109
silence suppression 49
simplified mobile access 71
SIP 50
SIP endpoints 50
SIPconnect 1.1 49
Small Community Network 76
SMDR 36
SNMP Management Console 106
SoftConsole 30, 98
SOHO 34
Speaker button 85
specifications
    protocols 115
SSA 104
SSL/VPN 81
standard call features 50
supervised transfers 22
support 122
survivability 56
SysMonitor 105
System Administrator 121

T

T1 80
Technical Bulletins 122
telecommuters 69
telephones
    call coverage buttons 88
    external call lamps 91
    line appearance buttons 87
telephony 55
Time Entries 75
time linking
    office 79
Time Profile 75
time profiles 42
toggle calls 20
tones 21
training 122, 123
transferable dial out privileges 35
transfers 22
twinning 69

U

UCM 12
Unified Communications Module 12
unsecured' 80
unsupervised transfers 22
user
    privacy 30
User Guides 121
user portal 94

V

V.24 80
V.35 ..... 79, 80
V24 80
V35 80
visual voice 85
voice compression 53
voice mail 58
voice mail systems 109
voice recording 24
voice traffic 80
voicemail
    forwarding to 20
    operation 45
Voicemail 45, 75
VPN 71

W

WAN 79, 80
WAN link 79
WAN multiplexers 80
WAV file 37
Web Manager 104
websites 122
Wide Area 79
Wide Area Network 79
WINS 79
Wireless DECT R5 15
Workplace 94
World 79

X

X.21 ..... 79, 80