Administering Avaya IP Office™ Platform with Web Manager

Release 11.0 FP4
February 2019

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 mediums which may include product information, 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. Refer to your sales agreement 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 You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You 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 SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Cluster License (CL). End User may install and use each copy or an Instance of the Software only up to the number of Clusters as indicated on the order with a default of one (1) Cluster if not stated. “Cluster” means a group of Servers and other resources that act as a single system.

Enterprise License (EN). End User may install and use each copy or an Instance of the Software only for enterprise-wide use of an unlimited number of Instances of the Software as indicated on the order or as authorized by Avaya in writing.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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, and 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

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

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 for complying 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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

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).

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 Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted 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.

Trademarks

Contents

Chapter 1: Introduction

Related links

Purpose on page 21
New in Release 11.0 FP4 on page 21

Purpose

This document contains descriptions of the configuration fields and the configuration procedures for administering Avaya IP Office Platform using the IP Office Web Manager application. This document principally covers Release 11.0 Feature Pack 4 of those products.

Intended audience

The primary audience for the Administering Avaya IP Office using IP Office Web Manager is the customer system administrator. Implementation engineers and support and services personnel may also find this information helpful, however, they are not the primary audience.

Related links

Introduction on page 21

New in Release 11.0 FP4

Default extension password

The default extension password or PIN is different than the user password and is much stronger with a minimum of nine digits. IP Office R11.0 FP4 deployments provide for an auto-generated default extension PIN of 10 digits, which can be viewed and modified later using the **System** > **VoIP** > **VoIP Security** page. The eye icon next to the **Default Extension Password** field in the user interface can be used to view the existing default extension password. The feature is available in R11.0 FP4 deployments including new installs and upgrades.

Fallback twinning

With this feature, IP Office redirects calls to the users twinned mobile number when the primary extensions are unreachable even if mobile twinning is disabled. The settings can be located at

User > **Mobility** page. 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

IP Office Media Manager enhancements

The following features have been added to IP Office Media Manager:

- Delete recordings
- Audit trail: Administrators can keep track of the usage of recording files in IP Office Media Manager. The following type of usage of a recording can be tracked using this feature:
  - Delete
  - Download
  - Replay
  - Search

The audit trail displays the User name, Timestamp, User Action, and Details. The audit trail can be stored up to a duration of one year. The settings are available in Web Manager at **Applications** > **Media Manager**.

Security enhancements for registration of SIP devices

The new 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 settings in **System** > **VoIP** > **Access Contro Lists** 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** drop-down menu in **System** > **LAN1** > **VoIP** can be used to select which SIP User Agents are allowed for registering with IP Office.

Automatic user synchronization with Avaya Spaces

IP Office R 11.0 FP4 system users and user details created for Avaya Equinox™ can be automatically synchronized with Avaya Spaces server. To use and receive additional Avaya Spaces features, the details of users configured for Avaya Equinox™ need matching users configured on the Avaya Spaces server. The synchronization can be done manually or automatically. The settings are located at **System** > **Avaya Cloud Services**.

Avaya Equinox™ support on Avaya Vantage™

Avaya Equinox™ is supported on Avaya Vantage™ phones in IP Office R 11.0 FP4 deployments. The option to select an application on Avaya Vantage™ is available at **System** > **Telephony** > **TUI**. The following applications are available to select:

- Avaya Equinox™
- Vantage Basic/Vantage Connect

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. The feature can be enabled from **Line** > **SIP Line** > **SIP Advanced**

SIP and H.323 Registrars disabled by default

To secure IP Office R 11.0 FP4 from vulnerabilities, the **H.323 Gatekeeper Enable** and **SIP Registrar Enable** fields in **System** > **LAN1/LAN2** > **VoIP** are disabled by default. Whenever a new H,323 or SIP extension is being added and the corresponding registrar is not enabled, IP Office system displays the following error message:

```
System is configured with IP extensions. Registration requires the
corresponding registrar to be enabled
```

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 the following error message:

```
System is configured to support resiliency. Registration of IP
extensions in failover requires the corresponding registrar to be
enabled
```

Avaya Equinox™ shared control

Avaya Equinox™ can now be used in shared control mode with desk phones. The shared control feature is available even when the Avaya Equinox™ client and desk phones are registered on different systems within the same network.

Join two Conferences

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.

JEM 24 button module support on Avaya J169/J179 IP Phone

Avaya J169/J179 IP Phone can support up to three JEM24 button modules. Each JEM24 has 24 dual-LED buttons with adjacent button label display. The button LEDs are used to indicate the status of the button feature whilst pressing the button is used to access the feature. A single JEM24 supports 72 programmable button slots. These are arranged in 3-pages, with pages accessed using the module's page scroll button. When multiple modules are connected to a phone, each module only supports a single page of 24 programmable button slots.

The modules automatically match the display settings of the phone to which they are connected - color with Avaya J179 IP Phone or greyscale with Avaya J169 IP Phone, font size, background image, screen saver. The button modules are powered though the phone. For more information, see the *IP Office Platform R11.0 J100 Series Telephone User Guide*.

Avaya J139 IP Phone

IP Office support for Avaya J139 IP Phone. Avaya J139 IP Phone is an advanced SIP desk phone that supports IP Office interactive menus and button programming. For more information, see the *IP Office Platform R11.0 J100 Series Telephone User Guide*.

Related links

Introduction on page 21

Chapter 2: IP Office Web Manager

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

A version of IP Office Web Manager is available for each type of IP Office operating mode. See below for a description of IP Office operating modes. Web Manager provides access to most, but not all, configuration settings.

Related links

Supported Web Browsers on page 24
IP Office operational modes on page 24
Getting started with Web Manager on page 25

Supported Web Browsers

IP Office Web Manager is currently supported with the following browser applications.

- Internet Explorer 10 and 11.
- Edge
- Firefox
- Chrome
- Safari 8 and 9

Related links

IP Office Web Manager on page 24

IP Office operational modes

IP Office systems can run in one of a number of modes depending on the capacity required and the licenses purchased.

Standard Mode

Standard Mode systems can be standalone or multiple systems can be linked in a Small Community Network (SCN). The base license is an Essential Edition license. Additional features are enabled with Preferred Edition and Advanced Edition licenses.

Server Edition

IP Office Server Edition is a scalable solution. A Server Edition solution can consist of only a Primary Server. Additional components are an optional secondary server and optional expansion systems. The primary server runs on the Linux operating system.

Shell Server Mode

An IP Office Shell Server is a single installation of selected IP Office applications running on Linux. You can use Manager to configure and administer a Shell Server. Application Servers and Unified Communications Modules (UCM) run on an IP Office Shell Server.

Since a Shell Server does not provide telephony, when you open a Shell Server configuration in Manager, all telephony functions are disabled. The following Manager functions are supported for Shell Servers:

- Discovery
- Initial configuration utility.
- System status.
- Load, edit and save security settings.
- Load, edit, and save the configuration.
- Erase configuration and security settings.
- Audit trail display.
- Web Control.

For more information on the management of an IP Office Shell Server, see *Installing and Maintaining Avaya IP Office™ Platform Application Server* and *Installing Avaya IP Office™ Platform Unified Communications Module*.

Related links

IP Office Web Manager on page 24

Getting started with Web Manager

Related links

Offline Mode on page 29
User Preferences on page 34

Importing a certificate into the Firefox browser

Importing a common certificate into the browser's trusted store provides additional security. If you do not install a certificate, you receive a message that the site is not trusted when logging in to Web Manager. Web Manager is supported on Firefox 16+.

This procedure only needs to be preformed once.

Procedure

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

   The index page for the server opens.
2. Click on **IP Office Web Manager**.

   A page opens with the statement "This connection is untrusted".
3. Click **I understand the risks**.
4. Click **Add Exception**.
5. Ensure that **Permanently store this exception** is checked and then click **Confirm Security Exception**.
6. Continue to the log in procedure.

Related links

Getting started with Web Manager on page 25

Importing a certificate into the Internet Explorer browser

Importing a common certificate into the browser's trusted store provides additional security. If you do not install a certificate, you receive a message that the site is not trusted when logging in to Web Manager. Web Manager is supported on Internet Explorer (IE) 10 and higher.

This procedure only needs to be preformed once.

Procedure

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

   The index page for the server opens.
2. Click on **IP Office Web Manager**.

A page opens with the statement “There is a problem with this website’s security certificate”.

3. Click on **Continue to this website (not recommended)**.

   The Web Manager log in page opens.

4. At the top of the browser, the right hand side of the address field contains a **Certificate Error** button. Click on **Certificate Error** to open the security report.
5. At the bottom of the security report, click **View Certificates**.
6. In the Certificate window, click **Install Certificate**.
7. In the Certificate Import Wizard, click **Next**.
8. Select Place all certificates in the following store and then click **Browse**.
9. In the Select Certificate Store window, select **Trusted Root Certification Authorities**.
10. Click **Next** and then **Finish**.
11. In the Certificate window, click **OK** to close.
12. In the browser window, on the menu bar, select **Tools** and then **Internet Options**.
13. In the Internet Options window, select the **Advanced** tab.
14. Uncheck **Warn about certificate address mismatch**.
15. Click **OK**.
16. Continue to the log in procedure.

Related links

Getting started with Web Manager on page 25

Logging in to Web Manager

Use this procedure to log in to Web Manager.

The first time you log in to an IP Office Server Edition server using Web Manager, the system displays the Ignition menu. Use the ignition menu to configure the initial settings for the server. For procedures and information on the ignition process, see *Deploying IP Office Server Edition Solution*.

Note:

When you first log in to an IP Office system (with Web Manager or Manager), you must change the default passwords for the Administrator, Security Administrator, and System accounts.

Note:

In order to open a client application (for example Manager), you must log into Web Manager using the IP Office LAN 1 IP address.

Note:

In order to open the **Platform** page, you must log into Web Manager using the IP Office LAN 1 IP address or for other IP addresses, open a separate browser window and enter `https://<ip_address>:7071`.

Before you begin

- You must know the IP address of the IP Office system.
- You must have a user ID and password.

Procedure

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

   The index page for the server opens.
2. Click on **IP Office Web Manager**.
3. On the login page, enter a user name and password and click **Login**.

   IP Office allows five concurrent sessions using one administrator account. If five sessions are already on, logging in for the sixth session fails and Web Manager displays an error message `Limit of concurrent sessions per user exceeded`. Note that the following are also considered as a session:

   - If Manager is connected with IP Office Server Edition through SE Central Access.
   - If the same administrator account is used to log in to any of the IP Office third party applications developed using the Management SDK client.

Related links

Getting started with Web Manager on page 25

Logging out of Web Manager

Use this procedure to log out of Web Manager.

Procedure

1. In the upper right corner of the Web Manager interface, click **Logout**.
2. You receive a prompt to confirm the log out. Click **OK**.

   You are logged out of the current session. If the browser window remains open, you are returned to the login screen.

Related links

Getting started with Web Manager on page 25

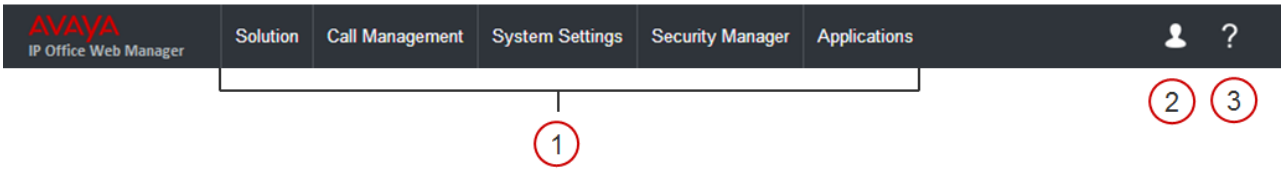
Granular access for Service Users

IP Office provides the option to restrict the Web Manager user interface access to Service Users. Administrators can provide granular Read/Write configuration access to Service Users depending on the Service user role. The Avaya IP Office Manager has provision for creating Rights group for Web Services and assigning the Service users to a a Rights group depending on the role the Service user performs. For more information on assigning Web Services configuration access to Service users, see *Administering Avaya IP Office Platform with Manager* guide.

Related links

Getting started with Web Manager on page 25

Web Manager User Interface



1	Menu bar selections. Use these options to navigate to Web Manager pages.
2	Current user. This menu displays the current user name. It also contains: • a link to the **Preferences** page for the current user • **Logout**
3	The help menu contains: • a link to the **Documentation** • The **About** command that opens a window to display version information and in service details.

Related links

Getting started with Web Manager on page 25

Offline Mode

Navigation: **Menu Bar Current User Icon** > **Offline Mode**

By default, Web Manager operates in real time and configuration changes are applied to the IP Office system immediately. When you select **Menu Bar Current User Icon** > **Offline Mode**, Web Manager changes to an offline management mode. In this mode, you can make multiple changes to the configuration and then apply them with one **Save** action.

Once you are in **Offline Mode**, the **Menu Bar Current User Icon** > **Offline Mode** changes to **Save to IP Office**. The **Save to IP Office** option is also available above the menu bar.

Important:

Once you have entered the offline management mode, you must log out and log back in again to return to real time operation.

Settings that must be edited in Offline Mode

The following table lists the configuration settings and indicates which settings must be edited in **Offline Mode**.

Configuration Setting	Offline Editing Required	Notes
Call Management > **Users** > **Add/Edit Users**		
User	No	
Voicemail	No	
Button Programming	No	
Call Management > **Users** > **Add/Edit Users** > **Telephony**		
Call Settings	No	
Supervisor Settings	No	
Multi-line Options	No	
Call Log	No	
TUI	No	
Call Management > **Users** > **Add/Edit Users**		
Short Codes	No	
Forwarding	No	
Mobility	No	
Group Membership	No	
Voicemail Recording	No	
Do Not Disturb	No	
Announcements	No	
Personal Directory	No	
SIP	No	
Call Management > **Users** > **Add/Edit Users** > **Menu Programming**		
T3 Telephony	No	
Hunt Group	No	
4400/6400	No	
Call Management > **Users** > **Add/Edit Users**		

Table continues…

Configuration Setting	Offline Editing Required	Notes
Dial In	No	
Self Administration	No	
Call Management > **Extensions** > **Edit Extension**		
Common	Yes	These settings must be edited offline.
H323	Yes	These settings must be edited offline.
SIP VoIP	Yes	These settings must be edited offline.
SIP T38 Fax	Yes	These settings must be edited offline.
IP DECT	Yes	These settings can be edited online with the exception of the **Reserve License** setting. The **Reserve License** setting must be edited offline and requires a reboot of the system.
Call Management > **Group** > **Add/Edit Group**		
Group	No	
Queuing	No	
Overflow	No	
Fallback	No	
Voicemail	No	
Voicemail Recording	No	
Announcements	No	
SIP	No	
Call Management > **Auto Attendant** > **Add Auto Attendant**		
Auto Attendant	No	
Actions	No	
System Settings		
Short Codes	No	
Incoming Call Route	No	
Time Profile	No	
System Directory	No	
Locations > **Locations**	No	
Locations > **Address**	No	
Licenses > **Licenses**	No	
Licenses > **Remote Server**	Yes	The **Reserved Licenses** setting can be edited online. The remaining settings must be edited offline. Changes to these settings requires a reboot of the system.
System Settings > **System**		

Table continues…

Configuration Setting	Offline Editing Required	Notes
System	Yes	These settings can be edited online with the exception of **Locale** and **Favor RIP Routes over Static Routes**. These settings must be edited offline and requires a reboot of the system.
Voicemail	Yes	These settings can be edited online with the exception of **Voicemail Type** and **Voicemail IP Address**. These settings must be edited offline and requires a reboot of the system.
System Events	Yes	These settings must be edited offline.
SMTP	Yes	These settings must be edited offline.
DNS	Yes	These settings must be edited offline.
SMDR	No	
LAN > **Settings**	Yes	These settings must be edited offline.
LAN > **VoIP**	Yes	These settings must be edited offline.
LAN > **Network Topology**	Yes	These settings must be edited offline.
LAN > **DHCP Pools**	Yes	These settings must be edited offline.
VoIP	Yes	These settings must be edited offline.
VoIP Security	Yes	These settings must be edited offline.
Directory Services > **LDAP**	No	
Directory Services > **HTTP**	No	
Firewall Profile	No	
Authorization Code	No	
RAS	No	
WAN Port	Yes	These settings must be edited offline.
User Rights	No	
System Settings > **System** > **Telephony**		
Telephony	Yes	These settings can be edited online with the exception of **Companding LAW** and **Media Connection Preservation**. These settings must be edited offline and requires a reboot of the system.
Park and Page	No	
Tones and Music	Yes	These settings must be edited offline.
Ring Tones	No	
SM	Yes	These settings must be edited offline.
Call Log	No	
TUI	No	

Table continues…

Configuration Setting	Offline Editing Required	Notes
Contact Center	No	
System Settings		
IP Route	No	
Services > **Normal / WAN / Internet**	No	
Services > **SSL VPN**	No	
Add/Edit Alternate Route	No	
Account Code	No	
System Settings > **Line**		
SIP Line > **SIP Line**	No	
SIP Line > **Transport**	No	
SIP Line > **URI**	No	
SIP Line > **VoIP**	No	
SIP Line > **Credentials**	No	
SIP Line > **Advanced**	No	
SIP Line > **Engineering**	No	
H.323 Line > **VoIP Line**	No	
H.323 Line > **Short Codes**	No	
H.323 Line > **VoIP Settings**	No	
IP Office Line > **Line**	No	
IP Office Line > **Short Codes**	No	
IP Office Line > **VoIP Settings**	No	
SIP DECT Line > **SIP DECT Base**	Yes	These settings must be edited offline.
SIP DECT Line > **SIP DECT VoIP**	Yes	These settings must be edited offline.
IP DECT LIne > **Line**	No	When creating an IP DECT line, these settings are mergeable. You can also remove an IP DECT line without rebooting. Changing an IP DECT line that has been imported into the configuration is not mergeable.
IP DECT LIne > **Gateway**	No	
IP DECT LIne > **VoIP**	No	
SM Line > **Session Manager**	No	
SM Line > **VoIP**	No	
SM Line > **T38 Fax**	No	
Analog Line > **Line Settings**	Yes	The settings can be edited on line with the exception of the **Network Type** setting. This setting must be edited offline and requires a reboot of the system.

Table continues…

Configuration Setting	Offline Editing Required	Notes
Analog Line > Line Options	Yes	These settings must be edited offline.
BRI Line > Line Settings	Yes	The following settings must be edited offline. Changes to these settings requires a reboot of the system. • **Line Sub Type** • **Network Type** • **TEI** • **Add 'Not-end-to-end ISDN' Information Element** • **Progress Replacement** • **Clock Quality** • **Force Number Plan to ISDN** Decreasing the **Number of Channels** setting requires a a “merge with service disruption”. When the configuration file is sent to the system, active calls on the deleted channels are cleared.
BRI Line > Channels	No	
E1 PRI Line	Yes	These settings must be edited offline.
E1 PRI Channels	Yes	These settings must be edited offline.
E1–R2 Options	Yes	These settings must be edited offline.
E1 R2 MFC Group	Yes	These settings must be edited offline.
E1-R2 Advanced	Yes	These settings must be edited offline.
US T1 Line	Yes	These settings must be edited offline.
T1 Channels	Yes	These settings must be edited offline.
T1 ISDN	Yes	These settings must be edited offline.
T1 ISDN Channels	Yes	These settings must be edited offline.
T1 ISDN TNS	Yes	These settings must be edited offline.
T1 ISDN Special	Yes	These settings must be edited offline.
T1 ISDN Call By Call	Yes	These settings must be edited offline.

Related links

Getting started with Web Manager on page 25

User Preferences

Navigation: **Menu Bar Current User Icon** > **Preferences**

Field	Description
Password / Confirm Password	Change the password of the currently logged in user.
Accessibility	Enables accessibility features.
Opt for Google Analytics	Default = No. When set to Yes, the Google Analytics application captures usage details and sends them to Google. The Avaya IP Office team uses this information to improve the user experience.
Application Preferences	
Inactivity Timeout	Default = 30 minutes. If no activity is detected, the time in minutes after which the Web Manager interface will close and return to the login screen. The minimum time is 5 minutes.
Web Manager Logging Level	Default = INFO. The level of logging information written to the Web Manager log file. The options are: • INFO • DEBUG • ERROR
Set current user for configuration synchronization	Sets the current logged in user for all the background configuration synchronization tasks.
Server User / System Password Synchronization	Default = Yes. When set to Yes, the service user password and the system password are synchronized.
Use Proxy	Default = No. Enables communication with expansion systems using the Primary Server's proxy. Only set to Yes for expansion systems: • in a cloud deployment • behind a NAT router
IP Address	If **Use Proxy** is enabled and an IP address is specified, then the IP address is used during the upgrade of expansion systems.
Consolidate Objects	Default = No. When enabled, global objects are formed. Global objects are common across all systems in the Server Edition solution.

Table continues…

Field	Description
Minimum Protocol Version	Default = TLS 1.2 This updates the supported TLS version of the Solution Management Application (SMA) server and does not affect the TLS version of the IP Office system. SMA uses port 7070 for integrating management API SDK client applications through TLS connections. The TLS servers allow connections that meet the specified minimum requirement of the selected protocol version and connections from a lower TLS version fail. The available options are: • TLS 1.0 • TLS 1.2

Related links

Getting started with Web Manager on page 25

Chapter 3: Configuration dashboard

IP Office provides a Configuration dashboard that guides you with tasks that are necessary for setting up a functioning single-node IP Office system. The tasks are categorized under separate widgets with each widget representing a simplified IP Office configuration page. On your fist login of the IP Office configuration, you are presented with the Configuration dashboard with the System widget enabled and all other widgets disabled. You can click the widget to access the simplified System configuration page where you can perform the initial configuration. The next widget is enabled when you complete the configuration of the page corresponding to the current widget. Since many of the configuration tasks in the System page requires a reboot, the page has been designed to be configured in Offline mode. After you configure a page in offline mode, you must **Save to IP Office** to enable the configuration. Configuring and saving the System page is a must on your first login. You can come back to the system and configure rest of the pages later.

On your subsequent logins, you can carry on with your configuration if you have configured at least the System configuration. After you configure the pages, each widget displays the highlights of the existing configuration on the dashboard. You can click the desired widget anytime afterwards to access the simplified pages to modify the existing IP Office configurations.

Navigation

IP500 V2: The landing page is the Dashboard page that appears when you log on.

IP Office Server Edition:

- The Dashboard page appears when you log in after the system has been installed and ignited.
- Anytime afterwards when at least the System has been set up: **Solution** > **Server Menu** > **Dashboard**

The widgets

The widgets on the Dashboard are displayed depending on the IP Office system you are setting up.

Widget	Server Edition Primary	On Avaya/ Powered By Avaya	Standard Mode	Branch	Basic Mode	Server Edition Expansion[1]
System	✓	✗	✓	✓	✓	✓
VoIP	✓	✓	✓	✗	✗	✗
Voicemail	✓	✓	✓	✗	✗	✗
Licensing	✓	✗	✓	✗	✗	✗

Table continues…

[1] The System widget appears when the expansion system has been installed and ignited.

Widget	Server Edition Primary	On Avaya/ Powered By Avaya	Standard Mode	Branch	Basic Mode	Server Edition Expansion[1]
Users and Extensions	✓	✓	✓	✗	✗	✗
Groups	✓	✓	✓	✗	✗	✗
Trunks	✓	✓	✓	✗	✗	✗
Incoming Call Routing	✓	✓	✓	✗	✗	✗
Outgoing Call Routing	✓	✓	✓	✗	✗	✗

Related links

Configuring IP Office using the Dashboard on page 38
System configuration on page 39
VoIP configuration on page 44
Voicemail configuration on page 49
Incoming Call Routes configuration on page 52
Outgoing Call Routes configuration on page 53
Configuring IP Office using the Dashboard on page 38
System configuration on page 39
VoIP configuration on page 44
Voicemail configuration on page 49
Licenses on page 215
Users on page 99
Group settings on page 167
Lines on page 307
Incoming Call Routes configuration on page 52
Outgoing Call Routes configuration on page 53

Configuring IP Office using the Dashboard

About this task

Configuring IP Office using the Dashboard is simple and intuitive. Widgets are enabled sequentially for configuration starting with the System settings page. Clicking each widget takes you to the relevant Configuration page where you can add or modify the configuration.

Before you begin

Ensure that your Server Edition Primary system has been installed and ignited.

[1] The System widget appears when the expansion system has been installed and ignited.

Procedure

1. Log on to **Web Manager**.

   On an IP500 V2, the Dashboard page appears when you log on to **Web Manager**.
2. On a Server Edition system, select **Solution** > **Server Menu** > **Dashboard**. On an IP500 V2, click **Solution**.

   The Dashboard page appears.
3. Click the **System** widget.
4. Type appropriate information in the fields.

   For information on the fields, see the field descriptions for each of the page.
5. Click **Apply** to save the page.

   The System page can be updated in **Offline Mode** only.
6. Click **Back** to go back to the Dashboard.
7. Follow steps 3 to 5 for each widget you want to configure.

Related links

Configuration dashboard on page 37
Configuration dashboard on page 37
System configuration on page 39
VoIP configuration on page 44
Voicemail configuration on page 49
Licenses on page 215
Users on page 99
Group settings on page 167
Lines on page 307
Incoming Call Routes configuration on page 52
Outgoing Call Routes configuration on page 53

System configuration

You must configure this page in Offline mode and save configuration to IP Office before you set up any other configuration. This is the only mandatory configuration page in the Dashboard. The Configuration page on a IP500 V2 provides you with the option to select a System mode where as in a Server Edition system the System mode selected at ignition is applied on the system.

Name	Description
System Name	A name to identify this system. This is typically used to identify the configuration by the location or customer's company name. Some features such as Gatekeeper require the system to have a name. This field is case sensitive and within any network of systems must be unique. Do not use <, >, |, \0, :, *, ?, . or /.
Retain Configuration	This option is shown for IP500 V2 units being converted to become Expansion System (V2)s in a Server Edition solution. If left unselected, the default, the existing configuration of the system is defaulted as per a standard Server Edition expansion system. If selected, the existing configuration is retained. However, some elements of that configuration may be invalid or ignored in a Server Edition solution. It is the installers responsibility to ensure that the final configuration is valid for use in the solution. For more information on IP500 V2 conversion, see *Deploying Avaya IP Office™ Platform Server Edition*.
Activate Avaya IP Office Select Mode	This option is to change the IP Office mode to IP Office Select mode.
Hosted Deployment	The option to select when deploying IP Office in a hosted environment. Selecting this option sets HTTP directory to HTTPS. The default is unchecked.
Services Device ID	Set a Device ID for the system. This ID is displayed on the Solution View and System Inventory pages and on the System | System tab in the configuration. The value can be changed using the **Device ID** field on the System | System Events | Configuration tab. If an SSL VPN is configured, , Avaya recommends that the Device ID match an SSL VPN service Account Name. Each SSL VPN service account name has an associated SSL VPN tunnel IP address. Having the displayed Device ID match an SSL VPN service account name helps identify a particular SSL VPN tunnel IP address to use for remotely managing IP Office.
DNS Server	This is the IP address of a DNS Server. If this field is left blank, the system uses its own address as the DNS server for DHCP client and forwards DNS requests to the service provider when **Request DNS** is selected in the service being used (Service | IP).
Locale	This setting sets default telephony and language settings based on the selection. It also sets various external line settings and so must be set correctly to ensure correct operation of the system. See *Avaya IP Office™ Platform Locale Settings*. For individual users the system settings can be overridden through their own locale setting (**User | User | Locale**).
LAN Interface	This IP Address, IP Mask, Gateway and DHCP Mode settings can be set for the systems two LANs, LAN1 and LAN2. These radio buttons are used to switch between displaying the LAN1 details or the LAN2 details.
IP Address	LAN1 Default = 192.168.42.1. LAN2 Default = 192.168.43.1. This is the IP address of the Control Unit on LAN1. If the control unit is also acting as a DHCP server on the LAN, this address is the starting address for the DHCP address range.

Table continues…

Name	Description
IP Mask	Default = 255.255.255.0. This is the IP subnet mask used with the IP address.
DHCP Mode:	Default = Server. This controls the control unit's DHCP mode for the LAN. When doing DHCP: • LAN devices are allocated addresses from the bottom of the available address range upwards. • Dial In users are allocated addresses from the top of the available range downwards. • If the control unit is acting as a DHCP server on LAN1 and LAN2, Dial in users are allocated their address from the LAN1 pool of addresses first. • **Server** When this option is selected, the system will act as a DHCP Server on this LAN, allocating address to other devices on the network and to PPP Dial in users. • **Disabled** When this option is selected, the system will not use DHCP. It will not act as a DHCP server and it will not request an IP address from a DHCP server on this LAN. • **Dial In** When this option is selected, the system will allocate DHCP addresses to PPP Dial In users only. On systems using DHCP pools, only addresses from a pool on the same subnet as the system's own LAN address will be used. • **Client** When this option is selected, the system will request its IP Address and IP Mask from a DHCP server on the LAN.
Enable NAT	Default = Off. This setting controls whether NAT should be used for IP traffic from LAN1 to LAN2. This setting should not be used on the same LAN interface as a connected WAN3 expansion module. **Note:** This field is applicable only for IP500 V2 systems.
Gateway	The address of the default gateway for routing traffic not in the same subnet address range of the **IP Address**/**IP Mask** set above. A default IP Route for this address is added to the systems configuration.
Server Edition Secondary Server	The IP address of the Secondary Server. This address is used to add an IP line to the Secondary Server to the configuration.
• **WebSocket Password** • **Confirm WebSocket Password**	Default = Blank. WebSockets are bi-directional HTTP or HTTPS communication pipes initiated from a client to a server. They permit clients behind local a firewall to traverse the internet to a server by using well known ports and protocols. A matching password must be set at each end of the line.

Table continues…

Name	Description
Activate Centralized Management and **Time Settings** **Note:** Activate Centralized Management and Time Settings are applicable only for IP500 V2 systems.	
Activate Centralized Management	This is a read-only field when accessed through Dashboard. The field indicates if IP Office system is being managed by Avaya Aura® System Manager. The field can be enabled using the Initial Configuration at **Solution** > **Actions** > **Initial Configuration**. If already enabled, the following fields provide more information on the System Manager configuration. • **System Manager IP Address** • **Secondary System Manager IP Address** • **SNMP Discovery Community** • **SNMP Trap Community** • **Device Certificate Name** • **Certificate Enrolment Password** • **Confirm Certificate Enrolment Password**

Table continues…

Name	Description
Time Setting Configuration Source	The time is either set manually (see Date and Time), obtained using Time protocol (RFC868) requests or obtained using Network Time Protocol (RFC958) request. This field is used to select which method is used and to apply ancillary settings based on the selected method. For Server Edition networks, the Primary Server is defaulted to use **SNTP** to **0.pool.ntp.org** to obtain its time and date. The Secondary Server and expansion servers are defaulted to use **SNTP** to obtain their time from the Primary Server. For other IP Office systems the default is **Voicemail Pro/Manager**. This option should not be used with Server Edition systems and systems with a Unified Communication Module as in those scenarios, the voicemail server is being hosted by and getting its time from the same server as the IP Office. • **None**, the system to not make any time requests. The system time and date needs to be set using a phone with System Phone Rights (User | User). The system can then automatically apply daylight saving settings to the manually set time. • **Voicemail Pro/Manager**, Both the Voicemail Pro service and the Manager program can act as RFC868 Time servers for the system. Use of other RFC868 server sources is not supported. They provide both the UTC time value and the local time as set on the PC. The system makes a request to the specified address following a reboot and every 8 hours afterwards. This option should not be used with Server Edition systems and systems with a Unified Communication Module as in those scenarios the voicemail server is being hosted by and getting its time from the same server as the IP Office. • **IP Address**: Default = 0.0.0.0 (Broadcast) The address to which the RFC868 request is sent. 0.0.0.0 means default operation. In this mode, following a reboot the control unit will send out a time request on its LAN interfaces. It first makes the request to the Voicemail Server IP address in its configuration if set and, if it receives no reply, it then makes a broadcast request. • **Time Offset**: Default = 00:00 This value is not normally set as any time changes, including daylight saving changes, that occur on the PC will be matched by the system. If you are running Manager when the voicemail server starts, voicemail does not start as a time server. It is therefore recommended that you have no copy of Manager running when you start or restart the voicemail server. Manager can be disabled from acting as a RFC868 time server by deselecting the Enable Time Server option (File | Preferences | Edit | Preferences). • **SNTP**: Use a list of SNTP servers to obtain the UTC time. The records in the list are used one at a time in order until there is a response. The system makes a request to the specified addresses following a reboot and every hour afterwards.

Table continues…

Name	Description
Time Zone	The option to select a time zone.
Local Time Offset from UTC	Default is based on the currently selected time zone. This setting is used to set the local time difference from the UTC time value provided by an SNTP server. For example, if the system is 5 hours behind UTC, this field should be configured with **-05:00** to make the adjustment. The time offset can be adjusted in 15 minute increments. If also using the daylight time saving settings below, use this offset to set the non-DST local time.
Automatic DST	Default = On. When set to On, the system automatically corrects for daylight saving time (DST) changes as configured in the **Clock Forward/Back Settings** field.
Clock Forward/ Back Settings (Start Date — End Date (DST Offset))	Default is based on the currently selected time zone. Click **Edit** to configure the time and date for DST clock corrections. In the Daylight Time Settings window, you can configure the following information: • **DST Offset**: the number of hours to shift for DST. • **Clock Forward/Back**: Select **Go Forward** to set the date when the clock will move forward. Select **Go Backwards** to set the date when the clock will move backward. • **Local Time To Go Forward**: The time of day to move the clock forward or backward. • **Date for Clock Forward/Back**: Set the year, month and day for moving the clock forwards and backwards. Once you click **OK**, the forward and back dates, plus the DST offset, are displayed using the format **(Start Date — End Date (DST Offset))**.

Related links

[Configuration dashboard](#) on page 37
[Configuring IP Office using the Dashboard](#) on page 38
[Configuration dashboard](#) on page 37

VoIP configuration

You can use this page to select a LAN and configure the H323 Gatekeeper and SIP Registrar for the selected LAN interface.

Field	Description
Select LAN	The option to select a LAN.

Table continues…

Field	Description
H.323 Gatekeeper Enable Default = Off This settings enables gatekeeper operation.	
H.323 Signalling over TLS	Default = Disabled. For hosted deployments, default = Preferred. When enabled, TLS is used to secure the registration and call signalling communication between IP Office and endpoints that support TLS. The H.323 phones that support TLS are 9608, 9611, 9621, and 9641running firmware version 6.6 or higher. When enabled, certificate information is configured in the `46xxSettings.txt` file on IP Office and automatically downloaded to the phone. When IP Office receives a request from the phone for an identity certificate, IP Office searches it's trusted certificate store and finds the root CA that issued it's identity certificate. IP Office then provides the root CA as an auto-generated certificate file named `Root-CA-xxxxxxxx.pem`. For information on IP Office certificates, see **Security Manager** > **Certificates**. The options are: • **Disabled**: TLS is not used. • **Preferred**: Use TLS when connecting to a phone that supports TLS. • **Enforced**: TLS must be used. If the phone does not support TLS, the connection is rejected. When set to **Enforced**, the **Remote Call Signalling Port** setting is disabled. If TLS security is enabled (**Enforced** or **Preferred**), it is recommended that you enable a matching level of media security on **System Settings** > **System** > **VoIP Security**.

Table continues…

Field	Description
Auto-create Extn	Default = Off The field to set up auto creation of extensions for H.323 phones registering themselves with the System as their gatekeeper. If selected, the system displays the **Auto Create Extension Password** window prompting you to type a Password and Confirm Password. This password is used for subsequent auto creation of extensions. A message `H.323 Auto-Create Extension option is active` is flashed next to the **Auto Create Extension** field till the option is cleared. SIP Extensions use a separate setting, see below. This setting is not supported on systems configured to use WebLM server licensing. If using resilience backup to support Avaya IP phones, **Auto-create Extn** and **Auto-create User** should not be left enabled after initial configuration or any subsequent addition of new extensions and users. Leaving auto-create options enabled on a system that is a failover target may cause duplicate extension/user records on the multi-site network under multiple failure scenarios. For security, any auto-create settings set to On are automatically set to Off after 24 hours.
H.323 Remote Extn Enable	Default = Off. The system can be configured to support remote H.323 extensions in the case where NAT is used in the connection path. This could be the case where the IP Office is located behind a corporate NAT/Firewall router and/or the H.323 phone is located behind residential NAT enable router. The use of this option and the interaction and configuration of external third party elements is beyond the scope this help file. In the case where the public IP address of the corporate router is unknown, the LAN's Network Topology settings should be used to configure a STUN Server. Enabling **H.323 Remote Extn Enable** allows configuration of the **RTP Port number Range (NAT)** settings. Currently, only 9600 Series phones are supported as H.323 remote extensions.

Table continues…

Field	Description
SIP Trunks Enable	Default = On. This settings enables support of SIP trunks. It also requires entry of **SIP Trunk Channels** licenses. Enabling **SIP Trunks Enable** allows configuration of the **RTP Port number Range (NAT)** settings.
SIP Registrar Enable Default = Off. Used to set the system parameters for the system acting as a SIP Registrar to which SIP endpoint devices can register. Separate SIP registrars can be configured on LAN1 and LAN2. Registration of a SIP endpoint requires an available **IP Endpoints** license. SIP endpoints are also still subject to the extension capacity limits of the system.	
Auto-create Extn	Default = Off The field to set up auto creation of extensions for H.323 phones registering themselves with the System as their gatekeeper. If selected, the system displays the **Auto Create Extension Password** window prompting you to type a Password and Confirm Password. This password is used for subsequent auto creation of extensions. A message `H.323 Auto-Create Extension option is active` is flashed next to the **Auto Create Extension** field till the option is cleared. SIP Extensions use a separate setting, see below. This setting is not supported on systems configured to use WebLM server licensing. If using resilience backup to support Avaya IP phones, **Auto-create Extn** and **Auto-create User** should not be left enabled after initial configuration or any subsequent addition of new extensions and users. Leaving auto-create options enabled on a system that is a failover target may cause duplicate extension/user records on the multi-site network under multiple failure scenarios. For security, any auto-create settings set to On are automatically set to Off after 24 hours.

Table continues…

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

Table continues…

Field	Description
SIP Registrar FQDN	Default = Blank This is the SIP registrar fully qualified domain name, for example, `server1.example.com`, to which the SIP endpoint should send its registration request. This address must be resolvable by DNS to the IP address of the IP Office system or to the IP address, such as that of an Avaya SBCE, through which the SIP endpoints reach the IP Office system.

Related links

Configuration dashboard on page 37
Configuring IP Office using the Dashboard on page 38
Configuration dashboard on page 37

Voicemail configuration

Name	Description
Voicemail Type	Defaults: • Non-Server Edition = Embedded Voicemail • Primary Server = Voicemail Pro • Server Edition Secondary Server with independent voicemail or for Outbound Contact Express = Voicemail Pro • Server Edition Others: Centralized Voicemail. Sets the type of voicemail system being used. For more information, see the description of Voicemail Type in the topic Voicemail.

Table continues…

Name	Description
Voicemail IP Address	Defaults: Non-Server Edition = 255.255.255.255, Primary Server = Primary Server IP Address. This setting is used when the **Voicemail Type** is set to **Voicemail Pro** or **Distributed Voicemail**. It is the IP address of the PC running the voicemail server that the system should use for its voicemail services. If set as 255.255.255.255, the control unit broadcasts on the LAN for a response from a voicemail server. If set to a specific IP address, the system connects only to the voicemail server running at that address. If the system is fitted with an Unified Communication Module hosting Voicemail Pro, the field should be set to 169.254.0.2.

Hold Music

This section is used to define the source for the system's music on hold source. You must ensure that any MOH source you use complies with copyright, performing rights and other local and national legal requirements.

Server Edition deployments support centralized music on hold, where the Primary Server streams music to the Secondary Server and all expansion servers.

The WAV file properties must be:

- PCM
- 8kHz 16-bit
- mono
- maximum length 90 seconds (30 seconds on non-IP500 V2 systems, 600 seconds on Linux based systems)

If the file downloaded is in the incorrect format, it will be discarded from memory after the download.

Caution:

Copying files in the incorrect format directly into the `opt/ipoffice/system/primary` directory can disable the music on hold function.

The first WAV file, for the system source, must be called `HoldMusic.wav`. Alternate source WAV files:

- can be up to 27 IA5 characters
- cannot contain spaces
- any extension is allowed
- case sensitive

Table continues…

Name	Description
Select a File	Use the option to select a `WAV` file to the system. The new file replaces the HoldMusic.wav file in the system. • **WAV File**: Use the WAV file `HoldMusic.wav`. This file is loaded via TFTP. Note that on Linux systems, the file name is case sensitive. • **External**: Applicable to IP500 V2 systems. Use the audio source connected to the back of the control unit. • **Tone**: The use of a double beep tone (425Hz, 02./0.2/0.2/3.4 seconds on/off) can be selected as the system source. The hold music tone is automatically used if the system source is set to WAV File but the `HoldMusic.wav` file has not yet been successfully downloaded. • **WAV (Restart)**: Identical to WAV except that for each new listener, the file plays from the beginning. Not supported on IP500 V2 systems. Cannot be used as a centralized source.
Upload	Click the button to upload the selected file.
Auto Attendant (is applicable only on IP500 V2 systems if the Voicemail Type is Embedded Voicemail)	
Name	Range = Up to 12 characters This field sets the name for the auto-attendant service. External calls can be routed to the auto attendant by entering AA:Name in the destination field of an Incoming Call Route.
Maximum Inactivity	Default = 8 seconds; Range = 1 to 20 seconds. This field sets how long after playing the prompts the Auto Attendant should wait for a valid key press. If exceeded, the caller is either transferred to the Fallback Extension set within the Incoming Call Route used for their call or else the caller is disconnected.
AA Number	This number is assigned by the system and cannot be changed. It is used in conjunction with short codes to access the auto attendant service or to record auto attendant greetings.

Table continues…

Name	Description
Direct Dial-By-Number	Default = Off. This setting affects the operation of any key presses in the auto attendant menu set to use the **Dial By Number** action. If selected, the key press for the action is included in any following digits dialed by the caller for system extension matching. For example, if 2 is set in the actions to **Dial by Number**, a caller can dial 201 for extension 201. If not selected, the key press for the action is not included in any following digits dialed by the caller for system extension matching. For example, if 2 is set in the actions to **Dial by Number**, a caller must dial 2 and then 201 for extension 201.
Dial by Name Match Order	Default = First Name/Last Name. Determines the name order used for the Embedded Voicemail Dial by Name function. The options are: • **First then Last** • **Last then First**
Enable Local Recording	Default = On. When off, use of short codes to record auto-attendant prompts is blocked. The short codes can still be used to playback the greetings.

Related links

Configuration dashboard on page 37
Configuring IP Office using the Dashboard on page 38
Configuration dashboard on page 37

Incoming Call Routes configuration

Use this page to configure Incoming Call Routes. A Working Hour Time Profile is created using the Days, Start time, and End Time provided on this page. You can then configure the destination of Incoming Call Routes for Working Hours and Out of Office Hours.

Name	Description
Working Hours Time Profile	The working hours as defined by the administrators. The Working Hours Time Profile is used to define Working Hours Destination.

Table continues…

Name	Description
Start Time	The time when the Working Hours Time Profile starts becoming applicable.
End Time	The time when the Working Hours Time Profile ends becoming applicable.
Year	The year in which the Working Hours Time Profile is applicable.
Incoming Line Group ID	The Incoming Line Group ID of the trunks to which Direct Inward Dialing (DID) is applied. The ID is unique in the configuration dashboard. The field comprises of SIP URIs and Analog lines for a selected Incoming Line Group ID. If the SIP trunk and Analog trunks have the same Incoming Line Group ID, system displays an error message. The Incoming Call Group ID cannot be deleted from the Configuration dashboard.
Trunk Identifier	The unique number to identify trunks.
Incoming Number	The Incoming phone number for incoming call routing.
Working Hours Destination	The destination Incoming Call Route for selected working hours.
Out of Office Hours Destination	The destination Incoming Call route for selected out of office hours.

Related links

Configuration dashboard on page 37
Configuring IP Office using the Dashboard on page 38
Configuration dashboard on page 37

Outgoing Call Routes configuration

Use the Outgoing Call Routing page to configure basic outgoing call routes that can be associated with the Users. By default all Users are associated with the Outgoing Route - Main. The following three Alternative Route Selection (ARS) are created by default:

- Unrestricted
- International
- Long Distance

The Outgoing Call Routing widget is enabled only if you have selected your **Locale** as **United States (US English)** or **Canada (Canadian French)** from the **Dashboard** > **System** page.

Name	Description
Directory Overrides Barring	Default = On. When enabled, barred numbers are not barred if the dialed number is in the External Directory.
Bar outgoing calls for Out of Office hours	Default = Off. When enabled, outgoing calls from the number are barred during Out of Office hours.
Select Line for Outgoing Calls	The Trunk line for outgoing calls. All the available SIP and Analog lines in the system are displayed in the drop-down list. You can select the Trunks for Outgoing Call Routes.
Outgoing Group ID	The Outgoing Line Group ID for Trunks.
Line Information	The associated Trunk line through which outgoing calls need to route.
Name	The User name. Click the User Name to assign an outgoing route for the user. Click the User to assign an Outgoing Route. You can edit inline and save the configuration.
Outgoing Route	The Outgoing Route to be assigned to a User. Select an Outgoing Route from the drop-down list and save the configuration.

Related links

Configuration dashboard on page 37
Configuring IP Office using the Dashboard on page 38
Configuration dashboard on page 37

Chapter 4: Solution

Navigation: **Solution**

Main content pane

The Solution main content pane lists all the servers in the Server Edition solution.

Server type	Description
Primary Server	A single Server Edition Primary server provides IP Office, Voicemail Pro, and Avaya one-X® Portal for IP Office.
Secondary Server	You can optionally add a Server Edition Secondary server to increase the capacity and provide resilience.
Expansion Server	IP Office Server Edition supports expansion systems which provide additional capacity, support analog or digital interfaces, and remote locations. A Server Edition Expansion System can be an IP500 V2 that is optimized for an hybrid of analogue/TDM and IP deployments or IP Office for Linux server that is optimized for IP only deployments.
one-X® Portal	You can optionally configure a separate application server dedicated to Avaya one-X® Portal to provide more one-X Portal user capacity above the maximum that a Server Edition Primary Server supports.
Application Server	The Application Server is an external, rack mounted server that provides scalability for larger IP Office installations and multi site deployments. The Application Server supports the Voicemail Pro and one-X Portal for IP Office applications.
Unified Communication Module (UCM)	The UCM is an embedded server on the IP500 V2 that allows Linux based IP Office applications to be run within the IP Office control unit rather than requiring separate PCs. The UCM supports the Voicemail Pro and one-X Portal for IP Office applications.
Contact Store	The standard call recording facilities provided with IP Office and Voicemail Pro can be extended further by using Contact Store.

Solution filters

Click Configure filter to create a custom filter.

Filter		Description
View All		Display all control units.
Type	Servers	Display all Primary and Secondary servers.
	Expansion Unit	Display all expansion units.

Table continues…

Filter		Description
Status	Online	Display all currently active control units.
	Offline	Display all offline control units.

Related links

Solution Objects on page 56
Solution Settings on page 57
Actions on page 66
Configure on page 74
Server Menu on page 77

Solution Objects

Navigation: **Solution** > **Solution Objects**

Click the **Global Objects** down arrow to display a list of configured global objects. Clicking a list item opens the configuration page for the object. The following global objects are listed.

- **Users**
- **Time Profiles**
- **Groups**
- **Locations**
- **Short Codes**
- **Directory**

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

- **Short Code** System short codes only.
- **Time Profile**
- **Account Code**
- **User Rights**
- **Location** Though consolidated, the **Emergency ARS** and **Fallback System** field settings of each location are configured separately at individual system level.
- **Incoming Call Route** For release 9.1 and higher, record consolidation is no longer applied to Incoming Call Routes.

In Web Manager, consolidated records are shown at the top the **Solutions** page, under **Solution Objects**. In Manager, operation of record consolidation is controlled by the **File** > **Preferences** > **Preferences** setting **Consolidate Solution to Primary Settings**. By default that setting is selected. The setting has the following effects.

If **Consolidate Network to Primary Settings** is selected:

- Entry and administration of consolidated records is performed only at the solution level except for the **Emergency ARS** and **Fallback System** field settings of location records.
- Those records are then automatically replicated in the configurations of all the systems in the solution but, except for locations, are still only visible and editable at the solution level.
- When the configurations are loaded or when this setting is changed to become selected, if any inconsistency between records are found, a **Consolidation Report** is displayed. This report allows selection of whether to update the system to match the primary or to update the primary to match.

If **Consolidate Network to Primary Settings** is not selected:

- Entry and administration of consolidated records can be performed at both the solution and individual system levels.
- Records entered and edited at the solution level are automatically replicated in the configurations of all the systems in the solution. Each record displays a label on the record indicating that it is a record that is shared across the solution.
- If a shared record is edited at the individual system level, that copy of the record is no longer shared with the other systems. It will not be updated by any changes to the solution level version of the same record.
- No consolidation checking for inconsistencies is done when the configurations are loaded.

Related links

Solution on page 55

Solution Settings

Navigation: **Solution** > **Solution Settings**

Related links

Solution on page 55
View Scheduled Jobs on page 57
Remote Server on page 58
Proxy on page 59
User Synchronization Using LDAP on page 60
Application Server on page 66

View Scheduled Jobs

Solution > **Solution Settings** > **View Scheduled Jobs**

Selecting **Schedule Jobs** from the **Solution Settings** list displays a table of existing scheduled jobs.

Scheduled tasks cannot be edited, other than to add or delete tasks. Click the delete icon to remove a schedule option.

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

Related links

Solution Settings on page 57

Remote Server

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

Selecting **Remote Server** from the **Solution Settings** list displays current remote server entries. Click the icons beside a record to edit or delete.

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

Related links

Solution Settings on page 57
Add Remote Server on page 58

Add Remote Server

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

Configuring a remote server may be required to

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

Additional configuration information

For additional information on backup and restore, see Backup and Restore on page 475.

Configuration settings

Field	Description
Storage Type	This field is only displayed on virtual servers deployed in a Google cloud environment. The options are: • **Google Storage**: Select this option you are using a Google Storage server inside the Google cloud. Note: Google storage can only be accessed by server's hosted in the cloud. It cannot be used as a backup destination by non —cloud—based servers in the same network. • **Custom Storage**: Select this option if you are not using a Google Storage server.
Server Name	A meaningful name for the remote server. Remote server names can be selected from other windows.
Protocol	Protocol supported by the remote server. The options are: **http**, **https**, **ftp**, **sftp**, **scp**. • When performing a backup to a Windows server with SCP, use OpenSSH. • For backup and restore, you can use HTTP, HTTPS, SFTP and SCP to connect to a remote IP Office Linux server. • HTTP and HTTPS can only be used to connect to an IP Office server. HTTP/ HTTPS backup to a non-IP Office server is not supported. **Note:** To create a dedicated IP Office Linux server for backup and restore, install an IP Office Application Server without enabling the Voicemail Pro and one-X Portal for IP Office applications on that server.
Remote Server	IP address or Domain name of remote server.
Port	Port of remote server.
Remote Path	Default path on the remote server.
User Name	If required, the user name for logging in to the remote server.

Related links

Remote Server on page 58

Proxy

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

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

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

Configuring proxy details may be required to

- download an ISO file from a remote server

- perform backup and restore actions on a remote server

Field	Description
Proxy Name	A meaningful name for the proxy. Proxy names can be selected from other windows.
Proxy Server	IP address or Domain name of proxy server.
Proxy Port	Port used for the proxy server.
User Name	If required, the user name for logging in to the proxy server.
Password	If required, the password for logging in to the proxy server.

Related links

Solution Settings on page 57

User Synchronization Using LDAP

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

Lightweight Directory Access Protocol (LDAP) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the internet or on a corporate intranet. IP Office supports LDAP version 2.

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

The information that can be managed through LDAP synchronization is:

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

- Mapping the **User Identification** and **Name** fields is mandatory for all operations. All the other fields are optional.

- Even if mapped, for each particular synchronization operation above, only those field labelled as ‘Yes’ are used.
- When creating a new user, if both the **Extension** and **User Provisioning Rule** have been mapped, the extension number setting in the UPR takes priority.
- An LDAP field can be mapped to several IP Office fields. For example, the same LDAP field can be mapped to the user **Name** and **Full Name** fields.
- The LDAP data is not validated during synchronization. When the IP Office configuration is opened in a manual configuration tool, those fields may be flagged as errors until manually corrected. To stop re-occurrence the LDAP data should be corrected and resynchronized.

Related links

Solution Settings on page 57
Connect to Directory Service on page 61
Synchronize User Fields on page 62
View Jobs on page 64
Manage User Provisioning Rules on page 65

Connect to Directory Service

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

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

Additional Configuration Information

For additional configuration information, see Managing Users with LDAP on page 579.

Configuration Settings

Field	Description
Host	Default = Blank. The host name or IP address of the LDAP server.
Port	Default = Blank. The listening port on the LDAP server. The standard ports used by the LDAP directory are 389 or 90389.
User Name	Default = Blank. The user name used to log in to the LDAP server.
Password	Default = Blank. The password for the user account used to log in to the LDAP server.
User Schema	Default = Blank. Specifies the type of resource in LDAP. For example, the type of user.

Table continues…

Field	Description
Search Filter	Default = Blank. Specifies which objects under the base are of interest. The search is applicable to the **project name** and **location** values for each employee. Example search values: • Search for all the names starting with “A”: **name=A*** • Get all the phone numbers in a domain, either telephone number or mobile: **(|(telephonenumber=*)(mobile=*))** • 1. Search for a user who is a member of cn=group1, cn=user, dc=acme,dc=com and with a telephone number: **(&(memberof=cn=group1,cn=users,dc=acme,dc=com)(telephonenumber=*))**
Base Distinguished Name	Default = Blank. Specifies the point in the LDAP tree to start searching. Specify the hierarchy in reverse order. For example: **OU=SBSUsers,OU=Users,OU=MyBusiness,DC=dnsroot,DC=ipoyvr,DC=ca**
Use SSL	Default = No. When set to Yes, a secure (SSL) connection must be used to connect to the LDAP server.
Test Connection	When clicked, Web Manager attempts to connect to the LDAP server with the specified credentials. You must provide the password each time you test the connection.
Save	If the **Test Connection** action is successful, **Save** is enabled. Click to save the configuration.

Related links

User Synchronization Using LDAP on page 60

Synchronize User Fields

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

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

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

Field	Description
User Identification	Mandatory. This field must be unique for each user to be imported into IP Office.
Name	Mandatory. The name of the user. User names must be unique across the system. If more than one user has the same name, only the first name must be unique.
Full Name	Optional. The full name of the user.

Table continues…

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

Field	Description
Operations in Synchronization	
New	Use defined settings to create new users. When a new user is created in LDAP, a new IP Office user is created the next time synchronization occurs.

Table continues…

Field	Description
Update	Use defined settings to update existing users. When a user is edited in LDAP, the IP Office user is edited the next time synchronization occurs.
Delete	Use defined settings to delete users. When a user is deleted in LDAP, the IP Office user is deleted the next time synchronization occurs.
Schedule Options	
Use Schedule	Default = Off
Start Date	Default = Blank. Click the calendar icon to select a start date.
Start Time	Click the arrow to select a start time.
Recurring Schedule	Default = No. Setting to Yes displays the configuration options.
Frequency	Default = Weekly. The options are: • **Daily** • **Weekly** • **Monthly**
Day of Week / Day of Month	Default = Blank. Depending on the **Frequency** setting, select a **Day of Week** or **Day of Month**.
Preview Results	Display a preview of the synchronization results based on the current settings.
Synchronize	Click to start the synchronization operation. **Important:** In order to perform the synchronization operation, you must set the current user for background configuration synchronization tasks. If this was not done when logging on to Web Manager, go to **Menu Bar Current User Icon** > **Preferences** and set **Set current user for configuration synchronization** to **Yes**.

Related links

User Synchronization Using LDAP on page 60

View Jobs

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

Field	Description
Job Name	A system generated name.

Table continues…

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

Related links

User Synchronization Using LDAP on page 60

Manage User Provisioning Rules

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

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

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

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

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

Field	Description
User Provisioning Rule Name	Default = Blank. Enter a descriptive name for the rule.
IP Office Name	Default = Blank. Select the IP Office system from the list.
Start Extension	Default = Blank. Specify the extension number from which to start. Extensions are created on IP Office in ascending order, skipping any existing used extension numbers. This field is mandatory if the **Extension Template** and/or **Extension Type** fields are used.

Table continues…

Field	Description
Select Extension Template	Default = Blank. Select an extension template from the list. You can define extension templates by selecting **Call Management** > **Extensions** > **Actions** > **Template Management**.
Extension Type	Default = Blank. The options are:**H323 Extenstion**, **IP DECT Extension**, **SIP DECT Extension** or **SIP Extension**
Select User Template	Default = Blank. Select a user template from the list. You can define user templates by selecting **Call Management** > **Users** > **Actions** > **Template Management**.

Related links

User Synchronization Using LDAP on page 60

Application Server

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

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

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

Related links

Solution Settings on page 57

Actions

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

Related links

Solution on page 55
Backup on page 67
Restore on page 70
Transfer ISO on page 71
Upgrade on page 72
Synchronize Service User and System Password on page 72
Download Configuration on page 73
Cloud Operations Management on page 73

Backup

Navigation: **Solution** > **Actions** > **Backup**

Solution > **Server menu** > **Backup**

Additional configuration information

For additional information on backup and restore, see Backup and Restore on page 475.

Configuration Settings

You can backup multiple servers with the same action. Select the check boxes in the server list for the servers you want to backup. When one or more of the server check boxes is checked, the **Backup** option in the **Actions** menu is enabled. To perform a backup on a single server, select **Backup** from the drop down list for the server.

To recover a failed server or a failed server upgrade the system backs up the configuration of the server, application and user data in a single file set locally or remotely. You can use this backup file to restore the server or a failed server upgrade. The system backs up the configuration of the application to a local drive, in a predefined directory. You can take a backup of the primary server on a local drive or a remote file server, which can optionally be the secondary server.

Security alert:

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

Note:

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

Field	Description
Backup Configuration	

Table continues…

Field	Description
Select IP Office Sets	Default = Blank. You can select **IP Office Configuration**. When selected for IP500 V2 Expansion systems, backs up • Configuration • Security Settings • DHCP Allocations • Call log When selected for Primary, Secondary, one-X Portal Server, and Linux Expansion systems, backs up • Linux Server Settings • Web Management Settings • Configuration • Security Settings • DHCP Allocations • Call log This backup set does not include any back data on the server itself.
Select one-X Portal Sets	Default = Blank. You can select **one-X Portal Configuration**. Backs up one-X Portal server settings.
Select Voicemail Pro Sets	Default = Blank. You can select from the following options. • **None** • **Voicemail Pro Configuration**: Backs up - Voicemail Pro server preferences - Call flows • **Messages & Recordings**: Backs up - Voice mailbox contents - Call recordings • **Voicemail Pro Full**: Backs up - Voicemail Pro server preferences - Call flows - Voice mailbox contents - Call recordings • **Selective Voicemails**

Table continues…

Field	Description
Select WebLM Sets	Default = Blank. You can select **WebLM Configuration**.
Select WebRTC Sets	Default = Blank. You can select **WebRTC Configuration**.
Select Media Manager Configuration	Default = Blank. You can select **Media Manager Configuration**. This backs up the configuration settings from the database.
Backup Label	
Remote Server	
Select Remote Server	A list of defined remote servers. You can select Add a Remote Server to define a server. Remote servers can also be defined at **Solution** > **Solution Settings** > **Remote Server**.
Proxy Settings	
Use Proxy	Default = Off
Select Proxy	
Schedule Options Use these settings to schedule a backup event. You can configure a regular backup routine using the **Recurring Schedule** options.	
Use Schedule	Default = Off
Start Date	Default = Blank. Click the calendar icon to select a start date.
Start Time	Click the arrow to select a start time.
Recurring Schedule	Default = No. Setting to Yes displays the configuration options.
Frequency	Default = Daily. The options are: • **Daily** • **Weekly** • **Monthly**
Day of Week / Day of Month	Default = Blank. Depending on the **Frequency** setting, select a **Day of Week** or **Day of Month**.

Related links

Actions on page 66

Restore

Navigation:

- **Solution** > **Actions** > **Restore**
- **Solution** > **Server Menu** > **Restore**

Additional configuration information

For additional information on backup and restore, see Backup and Restore on page 475.

Configuration Settings

You can restore multiple servers with the same action. Select the check boxes in the server list for the servers you want to restore. When one or more of the server check boxes is checked, the **Restore** option in the **Actions** menu is enabled. To perform a restore on a single server, select **Restore** from the drop down list for the server.

You can restore the primary server using the backup file on a local drive or a remote file server, which can optionally be the secondary server.

Security alert:

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

Note:

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

Note:

To restore a Voicemail Pro backup taken from an earlier Voicemail Pro software version, you must use Web Control to perform the restore. Do not use Web Manager.

To launch Web Control, open a browser window and enter `https://<IP_Office_ip_address>:7071`.

Do not use Web Control to restore backups taken from the current software version. Use Web Manager.

Field	Description
Restore Source	
Select Remote Server	A list of defined remote servers. You can select Add a Remote Server to define a server. Remote servers can also be defined at **Solution** > **Solution Settings** > **Remote Server**.

Table continues…

Field	Description
Restore Points	
Get Restore Points	The previously taken backup points of the selected servers that the administrator wants to restore operation from selected remote server.
Name	The name of the server that the administrator wants to restore.
Node Type	The type of server that the administrator wants to restore.
IP Address	The IP address of the server that the administrator wants to restore.
Version	The version of the server.
Set	The sets included in the backup that the administrator wants to restore (For Set information refer backup screen).
Time Stamp	The time stamp of the backup that the administrator wants to restore.

Related links

Actions on page 66

Transfer ISO

Solution > **Actions** > **Download ISO**

An ISO file of the IP Office software is required to perform an upgrade.

Authorization Error

If the Server Edition solution is configured for centralized authentication using LDAP (**Referred** mode) an authorization error may indicate connectivity issue with the LDAP server. You may need to switch the authentication mode from **Referred** to **Local**.

If you receive an authorization error while the transfer is in progress, the transfer will fail. You must log in and perform the transfer again.

For information on centralized authentication, see Managing Users with LDAP on page 579.

Field	Description
Available Version	Displays the release number and the build number in the format <release number>-<build number>
Transfer From	You can transfer an ISO file from the following locations: • **Remote Location** • **Primary Server Path** • **Client Machine** • **DVD Primary Server**
File path	Specify the path to the ISO file. Enabled when **Remote Location** or **Primary Server Path** is selected in the **Transfer From** field.

Table continues…

Field	Description
Select Remote Server	Enabled when **Remote Location** is selected in the **Transfer From** field. You have the option to add a remote server. Remote servers are listed at **Solution** > **Solution Settings** > **Remote Server**.
Use Proxy	Enabled when **Remote Location** is selected in the **Transfer From** field.
Select Proxy	Enabled when **Use proxy** is checked.
Select ISO	Enabled when **Client Machine** is selected in the **Transfer From** field.

Related links

Actions on page 66

Upgrade

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

You can upgrade multiple servers with the same action. Select the check boxes in the server list for the servers you want to upgrade. When one or more of the server check boxes is checked, the **Upgrade** option in the **Actions** menu is enabled. To perform a backup on a single server, select **Upgrade** from the drop down list for the server.

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

For information on performing an upgrade, see *Deploying IP Office Server Edition Solution*.

Field	Description
Upgrade from	Primary server is the only option. All systems are upgraded from the Primary Server.
Upgrade to version	The IP Office version you are upgrading to.
Restart IP Phones	The check box to select if you want to restart all the connected IP phones after the IP Office is upgraded.
Server Time	The current time on the server.
Use Schedule	You can schedule the upgrade. Select the **Schedule** check box to enable the **Select Schedule** field. Select a date and time from the corresponding drop-down menus to set a date and time for upgrade.

Related links

Actions on page 66

Synchronize Service User and System Password

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

Note:

This option is not available on IP500 V2 systems.

Synchronizing the service user and system password enables single sign on for all systems and applications across the solution. To enable single sign on, you must configure a service user with security web service rights and with the same credentials (user ID and password) on each system in the Server Edition solution. You then use this common user to manage all other service users.

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

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

Related links

Actions on page 66

Download Configuration

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

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

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

Related links

Actions on page 66

Cloud Operations Management

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

Name	Description
Enable Cloud Operations Management	Default = Off. The option to enable administration of the selected IP Office system through Cloud Operations Management. The Service Management Application (SMA) verifies whether access to Cloud Operations Management has been enabled before forwarding authentication requests from Cloud Operations Manager. If enabled, a Service User by the name *MCM Admin* is applied on all the connected IP Office systems. If disabled, Web Manager removes the entry about enabling COM but keeps the *MCM Admin* Service User in all the IP Office systems.

Related links

Actions on page 66

Configure

Navigation: **Solution** > **Configure**

Related links

Solution on page 55
Add System to Solution on page 74
Remove System from Solution on page 75
Convert to Select Licensed System on page 76
Resiliency Administration on page 76
Set All Nodes License Source on page 76
Link Expansions on page 77

Add System to Solution

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

When you add a system, an IP Office Lines connecting the new system are configured with default settings.

Important:

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

Perform the following steps to add a system to a IP Office Server Edition Solution.

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

   Add an offline or inaccessible system:

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

   Discover a system:

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

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

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

Related links

Configure on page 74

Remove System from Solution

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

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

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

Related links

Configure on page 74

Convert to Select Licensed System

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

Use this command to implement Select licensing in a IP Office Server Edition Solution. All systems in the solution must use the same licensing type.

Related links

Configure on page 74

Resiliency Administration

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

These settings set the **SCN Resiliency Options** on the IP Office Lines between systems to indicate which lines are being used to give/receive fallback options and what fallback options.

The options are:

- **Backup Primary Server IP Phones, Hunt Groups, Voicemail, and one-X Portal on the Secondary Server** When selected, the Secondary Server will support hunt group operation during any failure of the Primary Server. Also when selected, the Secondary Server will support the continued operation of Avaya IP phones normally registered to the Primary Server.
- **Backup Secondary Server IP Phones on Primary Server** When selected, the Primary Server will support the continued operation of Avaya IP phones normally registered to the Secondary Server.
- **Backup Expansion Systems** All Expansion systems are listed in the table.
  - For each expansion system, you can select to **Backup Phones** and **Backup Hunt Groups** by clicking the check boxes.
  - In the **Resilient To** field, select the IP Office system that will act as the backup.

Related links

Configure on page 74

Set All Nodes License Source

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

All systems in the Server Edition solution must use the same license source. The license source is defined by the configuration setting **System Settings** > **Licenses** > **Server Menu** > **Manage Licenses** > **License Source**. Use this setting to set all nodes to use the same license source.

Related links

Configure on page 74

Link Expansions

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

You can link Server Edition Expansion systems with an IP Office Line in order to enable:

- Direct dialing between Expansion systems
- Resiliency capability

For more information on resiliency, see Server Edition Resiliency on page 653.

When you link expansion systems using the Link Expansions tool, an IP Office Line connecting the two systems is configured with default settings. You must select the security level for the line.

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

Related links

Configure on page 74

Server Menu

Navigation: **Server Menu**

Note:

This option is not available on IP500 V2 systems.

The **Solution** page lists all the servers in a Server Edition network. To the left of each server listed, there is

- The **Server Menu**
- A chevron that allows you to display or hide the server inventory. The server inventory provides a summary of the objects provisioned on the server.

Related links

Solution on page 55
Dashboard on page 78
Platform on page 79
On-boarding on page 88
Launch SSA on page 89
Service Commands on page 90
Initial Configuration on page 91
Download Configuration on page 94
View Upgrade Report on page 95

Dashboard

Navigation: **Server Menu** > **Dashboard**

Note:

This option is not available on IP500 V2 systems.

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

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

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

Related links

Server Menu on page 77

Platform

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

Note:

This option is not available on IP500 V2 systems.

Related links

Server Menu on page 77
System on page 79
Logs on page 80
Updates on page 81
Settings on page 82
AppCenter on page 88

System

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

The **System** page provides a status overview of the server. The main content pain contains two sections, **Services** and **System**.

Services

A list of the services being supported by the server and provides a status summary. Use the Start All and Stop All buttons to start or stop all services on the server. The following status elements are displayed.

Field	Description
Start automatically check box	When enabled, the service is configured to start automatically.
Service name and software version	The service name, software release number and build number.
Up Time	The system running time since the last server start.
Mem/CPU Usage	Displays the current memory and CUP usage. Clicking the current usage text opens a summary graph.
Stop/Start	Click to stop or start the service. You can also use the **Start All** and **Stop All** buttons.
Notifications	A summary of the most recent log messages generated by the services running on the control unit. Detailed information is available on the Logs page.

System

Provides a general overview of the sever status and controls to shutdown or reboot the server. Note that it may take up to 10 minutes for CPU usage data to appear after a server reboot.

Control	Description
Shutdown	Selecting Shutdown stops all the application services and then shuts down the server. Use this process when it is necessary to switch off the server for any period. Once the shut down is complete, power to the server can be switched off. To restart the server, switch the power back on.
Reboot	Selecting Reboot stops all the application services and then stops and restarts the server and services.

The left side of the display contains graphs for CPU Usage History, Memory Usage, Disk Usage. The right side of the display contains the following status information.

Field	Description
OS/Kernel	The overall version of the Linux operating system installed on the server and the version of the operating system kernel.
Up Time	The system running time since the last server start.
Server Time	The current time on the server.
Average CPU Load	The average CPU load (percentage use) for the preceding minute, 5 minute and 15 minute periods.
Material Code	The material code for the server. This code is used as part of the system registration with the Avaya Global Registration Tool (GRT).
Model Info	The model information for the server.
System Manufacturer Serial No	The manufacturer's serial number for the server.
Speed	The processor speed.
Cores	The number of processor cores.
Hard Disk Size	The hard disk size.
RAM	The amount of RAM memory.
Disk RAID Levels	The RAID type, if any, being used.
Disk Array Types	The type of disk array being used for RAID.
Quota available for backup data	Displays the amount of space reserved for local backups if **Enable HTTP file store for backup/restore** is enabled.
Virtualized	Indicates if the server is running as a virtualized session.
Last Successful Logon	The date and time of the last successful logon, including the current logon.
Unsuccessful Logon Attempts	A count of unsuccessful logon attempts.

Related links

Platform on page 79

Logs

Navigation: **Server Menu** > **Platform View** > **Logs**

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

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

Related links

Platform on page 79

Updates

Navigation: **Server Menu** > **Platform View** > **Updates**

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

The main content pain contains two sections, System and Services.

Warning:

Before using any upgrade, refer to the IP Office Technical Bulletin for the IP Office release to confirm that Avaya supports the upgrade path. Some releases include changes that require additional steps. In all cases, always backup all application data before upgrading.

System

The System section displays operating system details and available updates.

Control	Description
Check Now	Click to recheck the version of update files available in the file repository. Normally, this occurs automatically when the Updates page is loaded.
Review updates	Click to display a list of the available update files. You can select the updates you want to install.
Update All	Click to install all available updates.

Services

The Services section displays details of the current version of each application installed and the latest version available. The **Change Version**, **Update**, **Update All**, and **Install** buttons are only enabled when appropriate update files are available in the applications software repository.

Control	Description
Check Now	Click to recheck the version of update files available in the file repository. Normally, this occurs automatically when the Updates page is loaded.
Clear Local Cache	Click to remove older update installation files and other material that may accumulate on the server over time.

Table continues…

Control	Description
Update All	When selected, applications that support upgrading without being uninstalled are updated to the latest versions available in the application file repository.
Change Version	Click to show the update files available for the related application in the server's file repository. The current version is selected. Select another version and click Apply to upgrade or downgrade to the selected version.
Update	Click to update the application to the latest version available in the application file repository.
Install/Uninstall	The button toggles depending on if there are application files available in the repository. Click to install or uninstall the selected application.

Related links

Platform on page 79

Settings

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

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

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

Related links

Platform on page 79
Settings — General on page 82
Settings — System on page 85

Settings — General

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

The **General** page displays server settings, such as the locations of software update repositories.

Field / Control	Description
Software Repositories The sever can use either remote or local software repositories to store software update files. Separate repositories are configured for operating system updates, IP Office application installation files and Windows client files. The files uploaded or present in the file repositories are used on the Updates and Apps Center pages.	
URL	If the Local option is not selected, this field is used to set the URL of a remote HTTP file repository. Note that each repository must be different, the same URL must not be used for multiple repositories.
Local	This checkbox is used to set whether the file repository used is local or remote (a folder on a HTTP web server specified in the Repository field).

Table continues…

Field / Control	Description
File / Browse / Add	If the Local option is selected, the File field and adjacent buttons can be used to browse to a specific update file. When the file is located and selected, click Add to upload the file to the file store on the server.
Syslog The Syslog section controls the receiving and forwarding of Syslog records. These options are not shown for a Server Edition Linux Expansion systems.	
Log files age (days)	Set the number of days each type of record is retained on the server before being automatically deleted. Separate settings are available for each log type.
Apply general settings to all file types	If selected, the setting for General log files is applied to all file types.
Max log size (MB)	Set the maximum total size of each type of records retained on the server before the oldest records of that type are automatically deleted. Separate settings are available for each log type.
Apply general settings to all file types	If selected, the setting for General log files is applied to all file types.
Receiver Settings	These settings control if and how the server can receive Syslog records. • **Enable**: If selected, the server is able to receive Syslog records using the port configured below. • **TCP Port**: Sets the port number used for receiving Syslog records if the Protocol is set to TCP. • **UDP Port**: Sets the port number used for receiving Syslog records if the Protocol is set to UDP.
Forward Destination 1	These settings control whether the server forwards copies of Syslog records it receives to another server. If enabled, the server will forward copies of the Syslog records it receives. • **IP Address**: Sets the address of the destination server. • **Port**: Set the destination port for the forwarded records. • **Protocol**: Set the protocol, UDP or TCP, for the forwarding.
Forward Destination 2	These settings control wether the server forwards copies of the Syslog records it receives to a second server. The settings are the same as for the first forwarding destination.
Select Log Sources	These options allow selection of which server reporting to include in the Syslog reports. The available options are: • Authentication and authorization privileges • Information stored by the Linux audit daemon (auditd) • NNTP(News)/UUCP(Usenet) protocols • Apache web server access_log and error_log
Certificates	

Table continues…

Field / Control	Description
Certified Authority Settings	The options are: • Create CA • Import CA
Generate/Download	
Certificate Settings	The options are: • Renew automatically • Create certificate for a different machine
Generate/Apply	
Web Control **Inactivity Timeout**	Select the period of inactivity after which the web session is automatically logged out. Changing this value will require you to login again. The options are 5 minutes, 10 minutes, 30 minutes and 1 hour.
Voicemail Settings **Debug Level**	This setting can be used to set the debug logging level used by the Voicemail Pro application if running. For the one-X Portal for IP Office application, the logging level is set through the applications own web administration menus. Log files are retrievable through the Logs | Download menu. The options are None, Critical, Error, Warning, Information and Verbose. The default level is Critical.
EASG Settings	
Status	Default = Disabled. The field to enable access to the EASG users. The options are: • Enabled • Disabled
Port	Default = 2222 The port used to run the service.
Service Listening	The interface on which the service is running. The options are: • **Any Tunnel** • **Any**
EASG Users	The EASG users who can log on to the system. The options are: • **Craft** • **init** • **inads** • **rasaccess** • **sroot**
EASG User Enabled	The option to enable EASG users.
EASG Technician Certificates	The drop-down menu lists the EASG Technician certificates.

Table continues…

Field / Control	Description
Upload Technician Certificate	The option to upload technician certificate so that the technician can log on to the console.
Password	The password to be used for logging in.
Change Product ID	This is required only for Linux machines and is used in the authentication algorithm.
Watchdog **Log files age (days)**	Sets the number of days that log file records are retained. This does not affect log file archives. Not applied to one-X Portal for IP Office which performs its own log file size limitation.
Set Login Banner	Default = Blank. The login menu can include custom text. For example, to indicate the server's role in a network. This may be useful in a network with multiple servers. Use this field to set the text that should be displayed on the login menu. After changing the text click **Save**.
one-X Portal Settings **Use Local IP**	The location of the one-X Portal for IP Office server, normally running on the Primary Server, is required by other applications in a Server Edition network. Select **Use Local IP** if the Primary Server is hosting the one-X Portal for IP Office application.

Related links

Settings on page 82

Settings — System

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

On the **System** page, view and manage the server settings for the server.

Field / Control	Description
Network	
Network Interface	Allows selection of network interfaces is currently being configured by the web form. Within the IP Office configuration, Eth0 matches LAN1, Eth1 matches LAN2.
Host Name	Sets the host name that the system should use. This setting requires the local network to support a DNS server. Do not use localhost. **Warning:** For a virtualized server, shown by the Virtualized value on the Home menu, this field is part of the System Identification (SID) used for licensing. Changing this value also changes the System Identification and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new System Identification.
Use DHCP	If selected, the IP address, subnet mask and default gateway information is obtained by the server making DHCP requests. The related fields are greyed out and cannot be set manually, instead they show the values obtained in response to the DHCP request.

Table continues…

Field / Control	Description
IP Address	Displays the IP address set for the server. If DHCP is not being used, the field can be edited to change the setting.
Subnet Mask	Displays the subnet mask applied to the IP address. If DHCP is not being used, the field can be edited to change the setting.
Default Gateway	Displays the default gateway settings for routing. If DHCP is not being used, the field can be edited to change the setting.
System DNS	Enter the address of the primary DNS server. This option is greyed out if the address of the DNS server is set to be obtained from the DHCP server.
Automatically obtain DNS from provider	This setting is only used if Use DHCP is also selected. If selected, the server attempts to obtain DNS server details from the DHCP server.
Avaya Office LAN Settings	
Avaya Office LAN1	These settings are used for the LAN1 interface of the server. LAN1 is also referred to as LAN.
Enable traffic control	Select whether the web control menus should be used to adjust the IP Office LAN settings.
Network Interface	Use the drop-down to select which port on the server should be used for LAN1.
Avaya Office LAN2	These settings are used for the LAN2 interface of the server. LAN2 is also referred to as WAN.
Date and Time These settings are used to set or obtain a UTC date and time value for use by the system and services.	
Date	Shows the current date being used by the server. If Enable Network Time Protocol is selected, this is the date obtained from the NTP server and cannot be manually changed. For virtual servers this field is not used. If not using NTP, the virtual server takes its date from the virtual server host platform.
Time	Shows the current UTC time being used by the server. If Enable Network Time Protocol is selected, this is the time obtained from the NTP server and cannot be manually changed. The current time being used by the server is shown on the Home menu. For virtual servers this field is not used. If not using NTP, the virtual server takes its time from the virtual server host platform.
Timezone	In some instances the time displayed or used by a function needs to be the local time rather than UTC time. The Timezone field is used to determine the appropriate offset that should be applied to the UTC time above. Note that changing the timezone can cause a Session expired message to appear in the browser. **Warning:** For a virtualized server, shown by the Virtualized value on the Home menu, this field is part of the System Identification (SID) used for licensing. Changing this value also changes the System Identification and so invalidates any current licenses. If that happens, new licenses need to be obtained using the new System Identification.

Table continues…

Field / Control	Description
Enable Network Time Protocol	If this option is selected, the system will attempt to obtain the current UTC time from the NTP servers listed in the NTP Servers list below. It will then use that time and make regular NTP requests to update the date and time. The following options are only used if Enable Network Time Protocol is selected.
NTP Servers	This field is used to enter the IP address of an NTP server or servers which should be used when Enable Network Time Protocol is selected. Enter each address as a separate line. The network administrator or ISP may have an NTP server for this purpose. A list of publicly accessible NTP servers is available at http://support.ntp.org/bin/view/Servers/WebHome, however it is your responsibility to make sure you are aware of the usage policy for any servers you choose. Choosing several unrelated NTP servers is recommended in case one of the servers you are using becomes unreachable or its clock is unreliable. The operating system uses the responses it receives from the servers to determine which are reliable. The IP Office system can also use NTP to obtain its system time.
Authentication **Enable referred authentication**	
HTTP Server **Enable HTTP file store for backup/restore**	
Change Root Password	
New Password	Enter the new password for the server's root account. Enter again to confirm.
Change Local Linux Account Password	
Account Name	The user name for the local Linux account.
New Password	Enter the new password for the server's root account. Enter again to confirm.
System Identification These settings are shown are for information only.	
System ID (SID)	This is the unique system reference that is used to validate licenses issued for this particular system. For a physical server this is a unique value based on the server hardware. For a virtual server this value is based on several factors including the LAN1 and LAN2 IP addresses, the host name and the timezone. If any of those are changed, the System ID changes and any existing licenses become invalid.
Licensing Mode	Indicates the licensing method being used by the system. Internal indicates that the system uses the unique system ID. Currently Internal is the only supported option.
Firewall Settings	
Status	
Active	
Enable Filtering	
Enable TCP ports	
Enable UDP ports	

Table continues…

Field / Control	Description
Additional Hard Drive Settings	

Related links

Settings on page 82

AppCenter

Navigation: **Server Menu** > **Platform View** > **AppCenter**

The **AppCenter** page is used to download files for use on the local PC. The file repository location is configured through the **Settings** > **General** page.

The files included in the installation may vary. Typical files are listed below. Note that some packages require the addition of licenses to the system and configuration changes. Refer to the specific installation manuals for those applications.

Application	Description
VmPro...ClientOnly.exe	The installation package for the Voicemail Pro client application used to administer the Voicemail Pro server application.
VmPro...Mapi.exe	The installation package for the MAPI proxy. This can be installed on a Windows PC in the same network as the Windows Exchange server. It allows the Linux based Voicemail Pro server to access UMS services. Refer to the Voicemail Pro installation manual.
Admin...	the installation package for the Manager application. Note that this is an installer for Manager, System Monitor and System Status Application tools only. It is not the full IP Office Administration and User package used with other IP Office systems.
DLink...	The installation package for the IP Office DevLink 3rd-party TAPI interface.
Flare...	The installation package for the IP Office Flare application.
TAPI...	The installation package for the IP Office 1st -party TAPI interface.
Softconsole...	The installation package for the IP Office SoftConsole application. This is an application used by receptionist and operator type users to answer and distribute incoming calls.
...Softphone...	A SIP softphone application for use by individual users. Separate installation packages are provided for Windows and Mac PCs.

Related links

Platform on page 79

On-boarding

Navigation: **Solution** > **Server Menu** > **On-boarding**

Additional configuration information

- For a procedure on configuring IP Office for Avaya support through an SSL VPN, see On-boarding on page 514.
- For full details on how to configure and administer SSL VPN services, refer to *Deploying Avaya IP Office™ Platform SSL VPN Services*.

Configuration settings

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

Warning:

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

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

Related links

Server Menu on page 77

Launch SSA

Navigation: **Server Menu** > **Platform View** > **Launch SSA**

The System Status Application is a diagnostic tool for system managers and administrators and is used to monitor and check the status of systems. Select **Launch SSA** from the menu for a server to check the status of that server. For more information, see *IP Office Using System Status*.

Note:

This option is not available on IP500 V2 systems.

Note:

This command is only supported with Internet Explorer.

Related links

Server Menu on page 77

Service Commands

Navigation: **Server Menu** > **Service Commands**

Related links

Server Menu on page 77
Restart IP Office Service on page 90
Erase Configuration on page 90
Erase Security Settings on page 90

Restart IP Office Service

Navigation: **Server Menu** > **Service Commands** > **Restart IP Office Service**

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

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

Related links

Service Commands on page 90

Erase Configuration

Navigation: **Server Menu** > **Service Commands** > **Erase Configuration**

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

Related links

Service Commands on page 90

Erase Security Settings

Navigation: **Server Menu** > **Service Commands** > **Erase Security Settings**

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

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

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

Warning:

Service Disruption.

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

Related links

Service Commands on page 90

Initial Configuration

Navigation: **Server Menu**

Note:

The Initial Configuration utility changes the security settings. Therefore, the user running the utility must have security read/write rights.

Standard Mode Initial Configuration

The Initial Configuration menu is displayed for all new or fully defaulted IP500 V2 systems. It allows the required operating mode for the system to be selected.

.

For a system that you want to run in Essential Edition, Preferred Edition or Advanced Edition modes, select **IP Office Standard Mode**.

For an IP500 V2 system to run in Standard Mode, its configuration must include an **Essential Edition** license. A Standard Mode system without this license will not allow any telephony functions.

For a system that is being installed as an expansion server for a Server Edition solution, select **Server Edition Expansion**.

Server Edition Initial Configuration

On a Standard Mode system, use the Initial Confguration option to convert the existing system configuration into a Server Edition system configuration. It will effectively default the configuration and reload it in Manager in Server Edition mode. Once **Server Edition Expansion** is selected as the **System Type**, the **Initial Configuration** menu is displayed. If **Server Edition Expansion** is selected in that menu, following selection of the various menu options, the system is rebooted as a Expansion System (V2) for a Server Edition network.

For systems being configured for operation in a Server Edition solution, the Initial Configuration menu is used to set or confirm a range of settings. The field shown and accessible in the form depend on the selected **System Type**.

Once the menu is completed and **Save** is clicked, the values entered are written into the system configuration and the system is restarted. The menu is also displayed when creating an offline

configuration for a Server Editionsystem. The configuration of an existing non-Server Edition system can be converted to a Server Edition configuration, invoking this menu, using the **File | Advanced | Initial Configuration** menu option.

System Type Indicate the type of sever role the system will perform.

Retain Configuration Data This option is shown for IP500 V2 units being converted to become Expansion System (V2)s in a Server Edition solution.

If left unselected, the default, the existing configuration of the system is defaulted as per a standard Server Edition expansion system.

If selected, the existing configuration is retained. However, some elements of that configuration may be invalid or ignored in a Server Edition solution. It is the installers responsibility to ensure that the final configuration is valid for use in the solution. For more information on IP500 V2 conversion, see *Deploying Avaya IP Office™ Platform Server Edition*.

Option	Description
Hosted Deployment	The option to select when deploying IP Office in a hosted environment. Selecting this option sets HTTP directory to HTTPS. The default is unchecked.
System Name	A name to identify this system. This is typically used to identify the configuration by the location or customer's company name. Some features such as Gatekeeper require the system to have a name. This field is case sensitive and within any network of systems must be unique. Do not use <, >, |, \0, :, *, ?, . or /.
Locale	This setting sets default telephony and language settings based on the selection. It also sets various external line settings and so must be set correctly to ensure correct operation of the system. See *Avaya IP Office™ Platform Locale Settings*. For individual users the system settings can be overridden through their own locale setting (**User | User | Locale**).
Services Device ID	Set a Device ID for the system. This ID is displayed on the Solution View and System Inventory pages and on the System | System tab in the configuration. The value can be changed using the **Device ID** field on the System | System Events | Configuration tab. If an SSL VPN is configured, , Avaya recommends that the Device ID match an SSL VPN service Account Name. Each SSL VPN service account name has an associated SSL VPN tunnel IP address. Having the displayed Device ID match an SSL VPN service account name helps identify a particular SSL VPN tunnel IP address to use for remotely managing IP Office.
LAN Interface	This IP Address, IP Mask, Gateway and DHCP Mode settings can be set for the systems two LANs, LAN1 and LAN2. These radio buttons are used to switch between displaying the LAN1 details or the LAN2 details.
IP Address	LAN1 Default = 192.168.42.1. LAN2 Default = 192.168.43.1. This is the IP address of the Control Unit on LAN1. If the control unit is also acting as a DHCP server on the LAN, this address is the starting address for the DHCP address range.
IP Mask	Default = 255.255.255.0. This is the IP subnet mask used with the IP address.
Gateway	The address of the default gateway for routing traffic not in the same subnet address range of the **IP Address**/**IP Mask** set above. A default IP Route for this address is added to the systems configuration.

Table continues…

Option	Description
DHCP Mode:	Default = Server. This controls the control unit's DHCP mode for the LAN. When doing DHCP: • LAN devices are allocated addresses from the bottom of the available address range upwards. • Dial In users are allocated addresses from the top of the available range downwards. • If the control unit is acting as a DHCP server on LAN1 and LAN2, Dial in users are allocated their address from the LAN1 pool of addresses first. • **Server** When this option is selected, the system will act as a DHCP Server on this LAN, allocating address to other devices on the network and to PPP Dial in users. • **Disabled** When this option is selected, the system will not use DHCP. It will not act as a DHCP server and it will not request an IP address from a DHCP server on this LAN. • **Dial In** When this option is selected, the system will allocate DHCP addresses to PPP Dial In users only. On systems using DHCP pools, only addresses from a pool on the same subnet as the system's own LAN address will be used. • **Client** When this option is selected, the system will request its IP Address and IP Mask from a DHCP server on the LAN.
Server Edition Primary Server	The IP address of the Primary Server. This address is used to add an IP line to the Primary Server to the configuration.
Server Edition Secondary Server	The IP address of the Secondary Server. This address is used to add an IP line to the Secondary Server to the configuration.
DNS Server	This is the IP address of a DNS Server. If this field is left blank, the system uses its own address as the DNS server for DHCP client and forwards DNS requests to the service provider when **Request DNS** is selected in the service being used (Service | IP).

Enterprise Branch Initial Configuration

The Initial Installation utility provides a default configuration and security settings that minimize initial installation activities and maximize security. The system must be configured with the default settings before the system can be administered by System Manager. This utility is used for new installations and after an upgrade to enable System Manager administration of the IP Office.

1. Select **File > Advanced > Launch Initial Installation Utility**.
2. In the **System Name** field, enter the appropriate system name.
3. For the **WAN Interface**, select LAN1 or LAN2. If you select LAN1, the DHCP Mode is disabled.
4. In the **IP Address** field, enter the appropriate IP address.
5. In the **IP Mask** field, enter the appropriate IP mask.
6. In the **Gateway** field, enter the appropriate gateway. Manager will create an IP route using this gateway with the selected WAN as the destination.
7. In the **DHCP Mode** section, if you selected LAN1, select the appropriate DHCP option. If you selected LAN2, DHCP Mode is disabled.

8. Select the **Under Centralized Management?** check box if you want the IP Office system to be managed by System Manager.
9. If you selected the **Under Centralized Management?** check box, a number of additional fields are shown, configure these additional fields as appropriate:

- **SMGR Address** - the IP address of the server running System Manager
- **SNMP Community**
- **SNMP Device ID**
- **Trap Community**
- **SCEP Domain Certificate Name**
- **Certificate Enrollment (SCEP) Password**

Select **Save**.

When you run the Initial Installation Utility, the Initial Installation utility also configures the following:

- System Status Interface (SSA) service security level – Unsecure only
- Configuration service security level –Secure, Medium
- Security Administration service security level – Secure, Medium
- OAMP Web Services service security level – Secure, Low (if locally administered)
- OAMP Web Services service security level – Secure, High (if administered by System Manager)
- Admin Client Certificate checks:-- High (if administered by System Manager)
- SCEP client active (if administered by System Manager)
- SCEP server IP address from SMGR IP address (if administered by System Manager)
- Legacy Program Code – Active (if locally administered)

If the system is administered by System Manager, the following is automatically configured:

- SNMP enabled
- SNMP trap destination 1 from System Manager IP address
- All SNMP traps active
- WebLM client active
- WebLM service address from System Manager IP address
- Remove all default extension users, leaving “NoUser” and “RemoteManager”

Related links

Server Menu on page 77

Download Configuration

Navigation: **Server Menu** > **Download Configuration**

Related links

Server Menu on page 77

View Upgrade Report

Navigation: **Server Menu** > **View Upgrade Report**

Related links

Server Menu on page 77

Chapter 5: Call Management

Related links

Users on page 96
Extension on page 150
Groups on page 166
Auto Attendant on page 188

Users

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

Additional configuration information

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

For additional configuration information, see Configure User Settings on page 573.

Main content pane

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

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

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

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

User Filters

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

Related links

Call Management on page 96
User Actions on page 97
Add Users on page 98

User Actions

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

Related links

Users on page 96
Import Users on page 97
Export users on page 97
User Template Management on page 97
Create From Template on page 98

Import Users

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

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

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

Related links

User Actions on page 97

Export users

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

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

Related links

User Actions on page 97

User Template Management

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

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

Related links

User Actions on page 97

Create From Template

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

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

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

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

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

Related links

User Actions on page 97
Provision Users on page 98

Provision Users

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

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

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

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

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

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

Related links

Create From Template on page 98

Add Users

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

Related links

Users on page 96
Users on page 99
Voicemail on page 106
Button Programming on page 111
Telephony on page 112
Short Codes on page 122
Forwarding on page 123
Mobility on page 126
Group Membership on page 133
Voice Recording on page 133
Do Not Disturb on page 134
Announcements on page 135
Personal Directory on page 137
SIP on page 139
Menu Programming on page 140
Dial In on page 142
Source Numbers on page 142
Web Self Administration on page 149

Users

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

Additional configuration information

- For a summary of user management, including a description of centralized users, see User Management Overview on page 573.
- The **Unique Identity** setting is used to configure Gmail Integration. For additional information, see Configuring Gmail Integration on page 581.

Users are the people who use the system or are Dial In users for data access. A system User may or may not have an Extension Number that physical exists - this is useful if users do not require a physical extension but wish to use system features, for example voicemail, forwarding, etc.

NoUser is used to apply settings to extensions which have no associated user. **Remote Manager** is used as the default settings for dial in connections.

Configuration Settings

These settings can be edited online. Changes to these settings do not require a reboot of the system. You can also perform inline editing of the fields on this page. Click the User to enable inline editing and click **Save** or **Cancel** to save or discard the changes respectively.

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

Field	Description
Name	Range = Up to 15 characters. This is the user's account name used for RAS Dial In, Caller Display and voicemail mailbox. As the display on Caller Display telephones is normally only 16 digits long it is useful to keep the name short. Only alphanumeric characters and space are supported in this field. This field is case sensitive and must be unique. Names should not start with a space. Do not use punctuation characters such as #, ?, /, ^, > and ,. Voicemail uses the name to match a user to their mailbox. Changing a user's name will route their voicemail calls to a new mailbox. Note however that Voicemail Pro is not case sensitive and will treat names such as "Steve Smith", "steve smith" and "STEVE SMITH" as being the same. Do not provision a user with the Name "admin". The user name "admin" is a reserved value on the one-X Portal Instant Message (IM) and Presence server. An IP Office "admin" user will not have IM and presence services. For Outbound Contact Express deployments, when an agent logs in to an extension, the user name associated with the extension is changed to the agent ID.
Password	Default = Blank. Range = Up to 31 alphanumeric characters. This password is used by user applications such as SoftConsole and TAPI. It is also used for user's with Dial In access. Note that this is not the user's voicemail mailbox password (see **Call Management** > **Users** > **Add/Edit Users** > **Voicemail** > **Voicemail Code**) or their phone log in code (see **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Supervisor Settings** > **Login Code**). Password complexity rules can be set through the General security settings. If complexity is not met, an error is displayed. The configuration can still be saved, except if system locale is set to France2.
Unique Identity	Default = Blank. A Google for Work account email address for the user. The address must be unique for each user. The account is used for: • Avaya Communicator for Web client login • Gmail voicemail to email messages To use Gmail for voicemail to email, set **Call Management** > **Users** > **Add/Edit Users** > **Voicemail** > **Enable Gmail API** to **On**.
Conference PIN / Confirm Conference PIN	Default = Blank. Range = Up to 15 numeric characters. Use this field to configure PIN access for meet me conferences. An **L** in this field indicates that the unscheduled meet-me conference feature is disabled for this user.

Table continues…

Field	Description
Account Status	Default = Enabled. Use this setting to **Enable** or **Disable** a user account. You can also require a password reset by selecting Force New Password. A user can only set a new password through the one-X Portal user interface. This option should not be used if one-X Portal is not available. The **Account Status** can also be **Locked - Password Error** or **Locked - Temporary**. The user account enters these states automatically based on the password settings configured in the Security Settings General tab. If a user exceeds the **Password Reject Limit**, then the **Password Reject Action** is implemented. If the **Password Reject Action** is **Log and Disable Account**, then the account status is changed to **Locked - Password Error**. If the **Password Reject Action** is **Log and Temporary Disable**, then the account status is changed to **Locked - Temporary**.
Full Name	Default = Blank Use this field to enter the user's full name. The recommended format is <first name><space><last name> in order for this value to be used correctly by voicemail dial by name features. When set, the **Full Name** is used in place of the **Name** for display by phones and user applications. Names should not start with a space. Do not use punctuation characters such as @, #, ?, /, ^, > and ,.
Extension	Range = 2 to 15 digits. In general all extensions should have the same number of digits. This setting can be left blank for users used just for dial in data connections. • Users for Delta Server, CBC and CCC should only use up to 4 digit extension numbers. • Users associated with IP phones or who may log in as such devices should not be given extension numbers greater than 7 digits. • Centralized users' extension numbers can be up to 13 digits in length. Although IP Office supports extension numbers up to 15 digits, the 13-digit length is determined by the maximum extension number length allowed for provisioning Centralized users in Communication Manager.
Email Address	Default = Blank Use this field to enter the user's email address.

Table continues…

Field	Description
Directory Common Name	Default = Blank. The Directory Common Name (CN) attribute. This setting can be used when configuring the Authentication Module for centralized authentication using LDAP. The Directory CN attribute is used for authentication. If the LDAP CN string is too complex to be used as a user name, enter an LDAP CN value here. The Directory CN must be exact copy of LDAP CN. The Directory CN can be any text string and must not exceed 63 characters. The Directory CN is not mandatory. If the LDAP CN is used for authentication as a user name, this field can be left blank.
Locale	Default = Blank (Use system locale) Configures the language used for voicemail prompts played to the user, assuming the language is available on the voicemail server. See *Avaya IP Office™ Platform Locale Settings*. On a digital extension it also controls the display language used for messages from the system. Note however that some phones have their own menu options for the selected language for the phone menus.
Priority:	Default = 5. Range = 1 (Lowest) to 5 (Highest) This setting is used by ARS.
System Phone Rights	Default = None. Users set as a system phone user are able to access additional functions. The settings are: • **None**: The user cannot access any system phone options. • **Level 1**: The user can access all system phone options supported on the type of phone they are using except system management and memory card commands. • **Level 2**: The user can access all system phone options supported on the type of phone they are using including system management and memory card commands. Due to the nature of the additional commands a login code should be set for the user to restrict access.

Table continues…

Field	Description
Profile	Default = Basic User. A user's profile controls whether they can be configured for a number of features. The table below lists the different user profiles and the features accessible by each profile. Setting a user to a particular profile enables those features by default, however they can be manually disabled if necessary. The number of users that can be configured for each profile is controlled by the user licenses present in the configuration. A **Non-licensed User** is allowed dial in access and paging and can be used as a Music on Hold or Analog paging port. Except for a Basic User, a **Preferred Edition** system license is a pre-requisite for any user profile licenses. In a multi-site network, the **Preferred Edition** license of the central system is automatically shared with other systems in the network, enabling user profile licenses on those other systems. However, each system supporting a Voicemail Pro server still requires its own **Preferred Edition** license for Voicemail Pro operation.

Feature		Standard Mode					Server Edition		
	Non-licensed User [1]	Basic User	Office Worker	Tele-worker	Mobile Worker	Power User	Basic User	Office Worker	Power User
one-X Portal Services	–	–	Yes	Yes	–	Yes	–	Yes	Yes
Telecommuter options	–	–	–	Yes	–	Yes	–	–	Yes
UMS Web Services	–	–	Yes	Yes	–	Yes	–	Yes	Yes
TTS for Email Reading	–	–	–	–	Yes	Yes	–	–	Yes
Remote Worker [2]	–	–	–	Yes	–	Yes	Yes	Yes	Yes
Avaya Communicator [3]	–	–	Yes	Yes	–	Yes	Yes	Yes	Yes
WebRTC	–	–	Yes	–	–	Yes	–	Yes	Yes

User Profile Notes:

1. Non-licensed users can be created on both Standard Mode and Server Edition systems.
2. The system supports users using remote H.323 or SIP extensions. On non-Server Edition systems, up to 4 users are supported as remote extensions without needing to be

configured and licensed for a user profile. Additional remote users are supported if licensed and configured for either a **Teleworker** or **Power User** user profile. On Server Edition systems, the remote worker is supported for all user profiles.

3. Supported for advanced Avaya Communicator for IP Office usage if one-X Portal and Voicemail Pro applications are also installed. If otherwise, only basic Avaya Communicator for IP Office usage is supported.

Note:

To upgrade an Office Worker or Mobile Worker to a Power User when no additional Office Worker or Mobile Worker licenses are available, you must first set the user **Profile** to **Basic User**. Once the user **Profile** has been set to **Basic User**, the **Power User** option is available in the drop down menu.

Field	Description
Receptionist	Default = Off. This settings allows the user to use the SoftConsole application. This requires the configuration to contain **Receptionist** licenses. Up to 4 users can be licensed, 10 for Server Edition systems. The use of SoftConsole is not supported for user's who then hot-desk to other systems in the multi-site network. A license is only required when a configured user runs SoftConsole.
Enable Softphone	Default = Off. If selected, the user is able to use the IP Office Softphone application.
Enable one-X Portal Services	Default = Off. If selected, the user is able to use the one-X Portal application to access their phone settings and to control phone calls
Enable one-X TeleCommuter:	Default = Off. If selected, the user is able to use the telecommuter mode features of the one-X Portal application.
Enable Remote Worker	Default = Off. Indicates whether the user is allowed to use an H.323 or SIP remote extension. Supported for up to 4 Basic users plus any users licensed and configured as **Teleworker** and or **Power User** user profiles. On Server Edition systems, all user types can be Remote Workers. If the user's **Extension Number** matches the **Base Extension** setting of an IP extension, the **H.323 Remote Extn Enable** setting of that extension is automatically changed to match the user's **Enable Remote Worker** setting and vice versa. The **Enable Remote Worker** option does not need to be enabled for users with SIP phones if an Avaya Session Border Controller for Enterprise (ASBCE) is deployed in the network to allow remote workers to register their SIP phone from a remote location.

Table continues…

Field	Description
Enable Desktop/ Tablet Voip client	Default = Off. This option allows users to use Avaya Communicator for IP Office or Avaya Equinox™ for IP Office as their current telephone device on Windows or macOS operating systems. It can be enabled for users whose **Profile** is set to **Officeworker**, **Power User**, or **Teleworker**. On non-Server Editionsystems, Avaya Communicator can be enabled for **Basic User** or **Mobile Worker** using Avaya Softphone licenses.
Enable Mobile VoIP Client	Default = Off. This option allows the users to use Avaya Communicator for IP Office or Avaya Equinox™ for IP Office as their current telephone device on Android and iOS operating systems. It can be enabled for users whose Profile is set to **Power User**.
Send Mobility Email	Default = Off When on, users that are assigned a **Profile** of **Mobile Worker** or **Power User** automatically receive a welcome email with the following information: • A brief introduction of one-X Mobile Preferred for IP Office. • Instructions and links for installing and configuring the one-X Mobile Preferred client. For more information on installing the one-X Mobile Preferred client, see *Administering Avaya one-X® Mobile for IP Office™ Platform* .
Exclude From Directory	Default = Off When on, the user does not appear in the directory list shown by the user applications and on phones with a directory function. For users logging on as agents in an Outbound Contact Express deployment, **Exclude From Directory** must be **Off**.
Web Collaboration	Default = Off. When on, allows the user to use the Web Collaboration application. A Web Collaboration license is required. For IP500 V2, the user license must be Office Worker User, Teleworker User, or Power User. For Server Edition, the user license must be Office Worker User, or Power User. Web Collaboration requires one-X Portal on Linux and is not supported on Windows or on the Unified Communications Module (UCM). The one-X Portal server name must be DNS resolvable.
Device Type	This field shows the type of phone at which the user is current logged in. If the user is logged out but is associated with a **Base Extension**, the device type for that extension port is shown. If the user has been logged out and is not associated with a **Base Extension**, the device type is listed as **Device Type Unknown**.
User Rights	
User Rights View	This field affects Manager only. It allows you to switch between displaying the user settings as affected by their associated **Working Hours User Rights** or **Out of Hours User Rights**.

Table continues…

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

Related links

Add Users on page 98
Configuring IP Office using the Dashboard on page 38
Configuration dashboard on page 37

Voicemail

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

Additional configuration information

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

For additional information, see Configuring Gmail Integration on page 581.

Configuration settings

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

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

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

Table continues…

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

Table continues…

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

Table continues…

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

Table continues…

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

Related links

Add Users on page 98

Button Programming

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

Additional configuration information

For additional information on programming button actions, see Button Programming Overview on page 789.

For additional information on programming button actions, see the chapter “Button Programming Overview” in *Administering Avaya IP Office™ Platform with Web Manager*.

Configuration settings

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

T3 Phones T3 phone buttons have default functions. These are not shown in the configuration file but can be overridden by settings added to the configuration file. Buttons left blank or set to call appearance will use the phone's default function for that button.

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

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

Related links

Add Users on page 98

Telephony

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

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

Related links

Add Users on page 98
Telephony Call Settings on page 112
Supervisor Settings on page 115
Multiline Options on page 118
Telephony Call Log on page 120
Telephony TUI on page 121

Telephony Call Settings

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

Additional configuration information

For additional information on ring tones, see Ring Tones on page 535.

Configuration settings

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

Field	Description
Outside Call Sequence	Default = Default Ring (Use system setting) Applies only to analog phones. Sets the ring pattern used for external calls to the user. The distinctive ring patterns used for other phones are fixed. Note that changing the pattern for users associated with fax and modem device extensions may cause those devices to not recognize and answer calls.
Inside Call Sequence	Default = Default Ring (Use system setting) Applies only to analog phones. Sets the ring pattern used for internal calls to the user. The distinctive ring patterns used for other phones are fixed.
Ring Back Sequence	Default = Default Ring (Use system setting) Applies only to analog phones. Sets the ring pattern used for ringback calls to the user. The distinctive ring patterns used for other phones are fixed.
No Answer Time	Default = Blank (Use system setting). Range = 6 to 99999 seconds. Sets how long a call rings the user before following forwarded on no answer if set or going to voicemail. Leave blank to use the system default setting.
Wrap-up Time (secs)	Default = 2 seconds, Range 0 to 99999 seconds. Specifies the amount of time after ending one call during which the user is treated as still being busy. During this time: • Other phones or applications monitoring the user's status will indicate the user as still being busy (on a call). • Hunt group calls will not be presented to the user. • If the user is using a single line set, direct calls also receive busy treatment. If the user is using a mutli-line set (multiple call appearances), direct calls to them will ring as normal. • It is recommended that this option is not set to less than the default of 2 seconds. 0 is used to allow immediate ringing.
Transfer Return Time (secs)	Default = Blank (Off), Range 1 to 99999 seconds. Sets the delay after which any call transferred by the user, which remains unanswered, should return to the user. A return call will continue ringing and does not follow any forwards or go to voicemail. Transfer return will occur if the user has an available call appearance button. Transfer return is not applied if the transfer is to a hunt group that has queuing enabled.

Table continues…

Field	Description
Call Cost Mark-Up	Default = 100. This setting is used for ISDN advice of charge (AOC). The markup is applied to the cost calculations based on the number of units and the line base cost per charging unit. The field is in units of 1/100th, for example an entry of 100 is a markup factor of 1. This value is included in the system SMDR output.
Advertize Callee State To Internal Callers	Default = System Default (Off). The options are: • **System Default (Off)**. The system setting is **System Settings** > **System** > **Telephony** > **Advertize Callee State To Internal Callers**. • **On** • **Off** When enabled, for phones on the same IP Office network (internal phones), additional status information is communicated to the calling party. Not supported for SIP endpoints. • When calling another internal phone and the called phone is set to Do Not Disturb or on another call, the calling phone displays “Do Not Disturb” or “On Another Call” rather than “Number Busy”. • On 95xx and 96xx phones, if a line appearance is programmed on a button on phone A and that line is in use on phone B, then phone A displays the name of the current user of the line along with the line number. • If a line appearance on a phone is in use elsewhere in the system and another extension unsuccessfully attempts to seize that line, the phone displays “In Use:<name>” where <name> is the name of the user currently using the line.
Call Waiting On	Default = Off For users on phones without appearance buttons, if the user is on a call and a second call arrives for them, an audio tone can be given in the speech path to indicate a waiting call (the call waiting tone varies according to locale). The waiting caller hears ringing rather than receiving busy. There can only be one waiting call, any further calls receive normal busy treatment. If the call waiting is not answered within the no answer time, it follows forward on no answer or goes to voicemail as appropriate. User call waiting is not used for users on phones with multiple call appearance buttons.
Answer Call Waiting on Hold	Default = On Applies to analog and IP DECT extension users only. If the user has a call waiting and places their current call on hold, the waiting call is automatically connected.

Table continues…

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

Related links

Telephony on page 112

Supervisor Settings

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

Additional configuration information

- For additional information on the **Force Authorization Code** setting, see Configuring Authorization Codes on page 567.

- For additional information on the **Inhibit Off-Switch Forward/Transfers** setting see, Off-Switch Transfer Restrictions on page 643.

Configuration settings

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

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

Field	Description
Login Code	Default = Blank. Range = Up to 31 digits. The code that has to be entered, as part of a log in sequence, to allow a user to make use of an extension as if it was their own phone. This entry must be at least 4 digits for DS port users. Login codes of up to 15 digits are supported with Extn Login buttons. Login codes of up to 31 digits are supported with Extn Login short codes. Centralized users use the **Login Code** for SIP registration on Session Manager. • For IP phone users, the login code should be limited to 13 digits. The user's login code is used by IP phones during registration with the system. • This log in code can be used for hot desking as well as logging back onto your phone after it has been used by a hot desking user. Hot desking is not supported for centralized users. • Users can only log out if they have a **Login Code** set. Users can log out without having a **Login Code** set if they are currently logged in at an extension whose Base Extension Number (**Call Management** > **Extensions** > **Edit Extension** > **Common**) no longer matches their own Extension (**Call Management** > **Users** > **Add/Edit Users** > **User**). • Supports the short code feature Change Login Code. • If the user has a login code set, it is used by the Outgoing Call Bar Off short code feature. • If the user has a login code set, access to a range of programmable button features will require entry of the login code. For example access Self Admin and **System Phone** features.
Login Idle Period (secs)	Default = Blank (Off). Range = 0 (Off) to 99999. If the telephone is not used for this period; the user currently logged in is automatically logged out. This option should be used only in conjunction with Force Login (see below).
Monitor Group	Default = <None> Sets the hunt group whose members the user can monitor if silent monitoring is setup. See the Call Listen short code.
Privacy Override Group	Default = <None> The drop-down menu lists the local and network advertised hunt groups. If selected, calls to this user cannot be seen or picked up by other users unless they are a member of the selected group.

Table continues…

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

Table continues…

Field	Description
Outgoing Call Bar	Default = Off When enabled, this setting stops a user from making any external calls except those that use dial emergency features. On many Avaya display phones, this causes a **B** to be displayed. The following features can be used with outgoing call bar: Outgoing Call Bar On, Outgoing Call Bar Off and Change Login Code.
Inhibit Off-Switch Forward/Transfers	Default = Off. When enabled, this setting stops the user from transferring or forwarding calls externally. This does not stop another user transferring the restricted users calls off-switch on their behalf. Note that a number of other controls may inhibit the transfer operation.
Can Intrude	Default = Off Check this option if the user can join or interrupt other user's calls using call intrusion methods other than conferencing.
Cannot be Intruded	Default = On If checked, this user's calls cannot be interrupted or acquired by other internal users using call intrusion. For users with **Cannot Be Intruded** off, private call can be used to indicate whether a call can be intrude or not.
Can Trace Calls	Default = Off. This settings controls whether the user is able to make used of ISDN MCID controls.
Can Control After Call Work	Default = Off. If enabled, the agent can extend the currently active After Call Work time indefinitely.
After Call Work Time (Sec)	Default = The value in this field is populated from the **Default After Call Work Time** field located at **System | Contact Center**. The time after a call when an agent is busy and unable to deal with hunt group calls. Change the value if you want to specify ACW time for this user to be different from the system default.
Can Accept Collect Calls	Default = Off [Brazil Only] Determines whether the user is able to receive and accept collect calls.
Deny Auto Intercom Calls	Default = Off. When enabled, any automatic intercom calls to the user's extension are automatically turned into normal calls.

Related links

Telephony on page 112

Multiline Options

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

Additional configuration information

- For additional configuration information, see Appearance Button Operation on page 943.

- For the **Reserve Last CA** setting, 1400, 1600, 9500 and 9600 Series telephone users can put a call on hold pending transfer if they already have held calls even if they have no free call appearance button available. For additional information, see Context Sensitive Transfer on page 644.

Configuration settings

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

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

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Individual Coverage Time (secs)</td><td>Default = 10 seconds, Range 1 to 99999 seconds.
This function sets how long the phone will ring at your extension before also alerting at any call coverage users. This time setting should not be equal to or greater than the No Answer Time applicable for the user.</td></tr>
<tr><td>Ring Delay</td><td>Default = Blank (Use system setting). Range = 0 (use system setting) to 98 seconds.
This setting is used when any of the user's programmed appearance buttons is set to Delayed ringing. Calls received on that button will initially only alert visually. Audible alerting will only occur after the ring delay has expired.</td></tr>
<tr><td>Coverage Ring</td><td>Default = Ring.
This field selects the type of ringing that should be used for calls alerting on any the user's call coverage and bridged appearance buttons. Ring selects normal ringing. Abbreviated Ring selects a single non-repeated ring. No Ring disables audible ringing. Note that each button's own ring settings (Immediate, Delayed Ring or No Ring) are still applied.
The ring used for a call alerting on a call coverage or bridged appearance button will vary according to whether the user is currently connected to a call or not.
• If not currently on a call, the Coverage Ring setting is used.
• If currently on a call, the quieter of the Coverage Ring and Attention Ring settings is used.
<table>
<tr><th>Attention Ring Setting</th><th colspan="3">Coverage Ring Setting</th></tr>
<tr><td></td><td>Ring</td><td>Abbreviated</td><td>Off</td></tr>
<tr><td>Ring</td><td>Ring</td><td>Abbreviated</td><td>Off</td></tr>
<tr><td>Abbreviated</td><td>Abbreviated</td><td>Abbreviated</td><td>Off</td></tr>
</table>
</td></tr>
<tr><td>Attention Ring</td><td>Default = Abbreviated Ring. This field selects the type of ringing that should be used for calls alerting on appearance buttons when the user already has a connected call on one of their appearance buttons. Ring selects normal ringing. Abbreviated Ring selects a single ring. Note that each button's own ring settings (Immediate, Delayed Ring or No Ring) are still applied.</td></tr>
</table>

Table continues…

Field	Description
Ringing Line Preference	Default = On. For users with multiple appearance buttons. When the user is free and has several calls alerting, ringing line preference assigns currently selected button status to the appearance button of the longest waiting call. Ringing line preference overrides idle line preference.
Idle Line Preference	Default = On. For users with multiple appearance buttons. When the user is free and has no alerting calls, idle line preference assigns the currently selected button status to the first available appearance button.
Delayed Ring Preference	Default = Off. This setting is used in conjunction with appearance buttons set to delayed or no ring. It sets whether ringing line preference should use or ignore the delayed ring settings applied to the user's appearance buttons. When on, ringing line preference is only applied to alerting buttons on which the ring delay has expired. When off, ringing line preference can be applied to an alerting button even if it has delayed ring applied.
Answer Pre-Select	Default = Off. Normally when a user has multiple alerting calls, only the details and functions for the call on currently selected button are shown. Pressing any of the alerting buttons will answer the call on that button, going off-hook will answer the currently selected button. Enabling **Answer Pre-Select** allows the user to press any alerting button to make it the current selected button and displaying its call details without answering that call until the user either presses that button again or goes off-hook. Note that when both **Answer Pre-Select** and **Ringing Line Preference** are enabled, once current selected status is assigned to a button through ringing line preference it is not automatically moved to any other button.
Reserve Last CA	Default = Off. Used for users with multiple call appearance buttons. When selected, this option stops the user's last call appearance button from being used to receive incoming calls. This ensures that the user always has a call appearance button available to make an outgoing call and to initiate actions such as transfers and conferences. 1400, 1600, 9500 and 9600 Series telephone users can put a call on hold pending transfer if they already have held calls even if they have no free call appearance button available.

Related links

Telephony on page 112

Telephony Call Log

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

The system can store a centralized call log for users. Each users' centralized call log can contain up to 30 call records for user calls. When this limit is reached, each new call records replaces the oldest previous record.

On Avaya phones with a fixed **Call Log** or **History** button (1400, 1600, 9500 and 9600 Series), that button can be used to display the user's centralized call log. The centralized call log is also

used for M-Series and T-Series phone. The user can use the call log to make calls or to store as a personal speed dial. They can also edit the call log to remove records. The same call log is also used if the user logs into one-X Portal.

The centralized call log moves with the user if they log on and off from different phones. This includes if they hot desk within a network.

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

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

Related links

Telephony on page 112

Telephony TUI

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

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

Field	Description
Features Menu Controls	
User Setting	Default = Same as System When set to **Custom**, the **Features Menu** list is enabled.

Table continues…

Field	Description
Features Menu	Default = On When set to off, TUI feature menus are not available. When set to on, you can select to turn individual feature menus off or on. The following feature menus are listed: • Basic Call Functions (Transfer to Mobile, Pickup, Park) • Advanced Call Functions (Do Not Disturb, DNS Exceptions, Account Code, Withhold Number, and Internal Auto Answer) • Forwarding • Hot Desk Functions • Passcode Change • Phone Lock • Self Administration • Voicemail Controls

Related links

Telephony on page 112

Short Codes

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

Additional configuration information

For additional configuration information on short codes, see Short Code Overview on page 693.

Configuration settings

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

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

Warning:

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

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

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

***FWD:**

Short codes of this form are inserted by the system. They are used in conjunction with the **User | Forwarding** settings to remember previously used forwarding numbers. They can be accessed on that tab by using the drop-down selector on the forwarding fields.

***DCP:**

Short codes of this form are often inserted by the system. They are used by some phone types to contain settings relating to functions such as ring volume and auto answer. Deleting such short codes will cause related phone settings to return to their defaults.

***DCP/Dial/8xxxxxxx, 0, 1, 1, 0/0:**

For system's with TCM phone ports, when a phone is first connected to the port, the button programming of the associated user is overwritten with the default button programming appropriate for the phone model. Adding the above short code prevents that behavior if not required, for example if a pre-built configuration including user button programming is added to the system before the connection of phones.

Related links

Add Users on page 98

Forwarding

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

Additional configuration information

For additional configuration information, see the section “DND, Follow Me, and Forwarding” in the chapter **Configure user settings** in *Administering Avaya IP Office™ Platform with Web Manager*.

For additional configuration information, see DND, Follow Me, and Forwarding on page 598.

Configuration settings

Use this page to check and adjust a user's call forwarding and follow me settings.

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

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

To bar a user from forwarding calls to an external number, select the setting **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Supervisor Settings** > **Inhibit Off-Switch Forward/Transfers**.

To bar all users from forwarding calls to external numbers, select the setting **System Settings** > **System** > **Telephony** > **Inhibit Off-Switch Forward/Transfers**.

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

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

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

Field	Description
Block Forwarding	Default = Off. When enabled, call forwarding is blocked for this user. The following actions are blocked: Follow me, Forward unconditional, Forward on busy, Forward on no answer and Hot Desking The following actions are not blocked: **Do not disturb**, Voicemail and Twinning
Follow Me Number	Default = Blank. Range = Internal extension number. Redirects the user's calls to the internal extension number entered. If the redirected call receives busy or is not answered, it follows the user's forwarding and or voicemail settings as if it had been presented to their normal extension. When a user has follow me in use, their normal extension will give alternate dialtone when off hook. Using **Follow Me** overrides **Forward Unconditional**. Calls targeting longest waiting type hunt groups ignore Follow Me. Calls triggered by actions at the user's original extension, for example voicemail ringback, ignore Follow Me. Park, hold and transfer return calls will go to the extension at which the user initiated the park, hold or transfer action.
Forward Unconditional	Default = Off This option, when checked and a **Forward Number** also set, forwards all external calls immediately. Additional options allow this forwarding to also be applied to internal calls and to hunt group calls if required. When a user has forward unconditional in use, their normal extension will give alternate dialtone when off hook. If the destination is an internal user on the same system, they are able to transfer calls back to the user, overriding the Forward Unconditional. After being forwarded for the user's no answer time, if still unanswered, the system can apply additional options. It does this if the user has forward on no answer set for the call type or if the user has voicemail enabled. • If the user has forward on no answer set for the call type, the call is recalled and then forwarded to the forward on no answer destination. • If the user has voicemail enabled, the call is redirected to voicemail. • If the user has both options set, the call is recalled and then forwarded to the forward on no answer destination for their no answer time and then if still unanswered, redirected to voicemail. • If the user has neither option set, the call remains redirected by the forward unconditional settings. Note that for calls redirected via external trunks, detecting if the call is still unanswered requires call progress indication. For example, analog lines do not provide call progress signalling and therefore calls forwarded via an analog lines are treated as answered and not recalled.

Table continues…

Field	Description
To Voicemail	Default = Off. If selected and forward unconditional is enabled, calls are forwarded to the user's voicemail mailbox. The **Forward Number** and **Forward Hunt Group Calls** settings are not used. This option is not available if the system's **Voicemail Type** is set to **None**. 1400, 1600, 9500 and 9600 Series phone users can select this setting through the phone menu. Note that if the user disables forward unconditional the **To Voicemail** setting is cleared.
Forward Number	Default = Blank. Range = Internal or External number. Up to 33 characters. This option sets the destination number to which calls are forwarded when **Forward Unconditional** is checked. The number can be an internal or external number. This option is also used for **Forward on Busy** and **Forward on No Answer** if no separate **Forward Number** is set for those features. If a user forwards a call to a hunt group of which they are a member, the group call is not presented to them but is presented to other members of the hunt group.
Forward Hunt Group Calls	Default = Off Hunt group calls (internal and external) are not normally presented to a user who has forward unconditional active. Instead they are presented to the next available member of the hunt group. This option, when checked, sets that hunt group calls (internal and external) are also forwarded when forward unconditional is active. The group's **Ring Type** must be **Sequential** or **Rotary**, not **Collective** or **Longest Waiting**. The call is forwarded for the period defined by the hunt group's **No Answer Time** after which it returns to the hunt group if unanswered. Note also that hunt group calls cannot be forwarded to another hunt group.
Forward Internal Calls	Default = On. This option, when checked, sets that internal calls should be also be forwarded immediately when forward unconditional is active.
Forward On Busy	Default = Off When checked and a forward number is set, external calls are forwarded when the user's extension is busy. The number used is either the **Forward Number** set for **Forward Unconditional** or if set, the separate **Forward Number** set under **Forward On Busy**. Having **Forward Unconditional** active overrides **Forward on Busy**. If the user has **Busy on Held** selected, if forward on busy is active it is applied when the user is free to receive calls but already has a call on hold. If the user's phone has multiple call appearance buttons, the system will not treat them as busy until all the call appearance buttons are in use unless the last appearance button has been reserved for outgoing calls only.
Forward On No Answer	Default = Off When checked and a forward number is set, calls are forwarded when the user does not answer within their set No Answer Time (User | Telephony | Call Settings).

Table continues…

Field	Description
Forward Number	Default = Blank. Range = Internal or External number. Up to 33 characters. If set, this number is used as the destination for **Forward On Busy** and **Forward On No Answer** when on. If not set, the **Forward Number** set for **Forward Unconditional** is used. If a user forwards a call to a hunt group of which they are a member, the group call is not presented to them but is presented to other members of the hunt group.
Forward Internal Calls	Default = On. When checked, this option sets that internal calls should be also be forwarded when forward on no answer or forward on busy is active.

Related links

Add Users on page 98

Mobility

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

Additional configuration information

For additional configuration information regarding the **Mobile Call Control** setting, see Mobile Call Control. on page 631

Configuration settings

These settings relate to twinning features where a user has a main or primary extension but also regularly answer calls at a secondary or twinned phone. These features are intended for a single user. They are not aimed at two users answering calls presented to a single primary extension.

Twinning allows a user's calls to be presented to both their current extension and to another number. The system supports two modes of twinning:

	Internal	Mobile
Twinning Destination	Internal extensions only	External numbers only.
Supported in	All locales.	All locales.
License Required	The primary phone user must be a licensed user.	Yes

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

Field	Description
Internal Twinning Select this option to enable internal twinning for a user. **Internal Twinning** cannot be selected for a user if they already have **Mobility Features** selected. Internal twinning is not supported across an SCN or SE network. Internal twinning is not supported during resilience.	

Table continues…

Field	Description
Twinned Handset	Default = Blank. For internal twinning, the drop-down list can be used to select an available user as the twinned calls destination. The secondary phone: • must be on the same system • must not be a simultaneous mode phone. For example, Avaya Communicator (for Windows, iPad, or Web), or WebRTC web client. If the list is grayed out, the user is a twinning destination and the primary to which they are twinned is displayed. All **Call Management** > **Users** > **Add/Edit Users** > **Mobility** fields are grayed out for unlicensed users.
Maximum Number of Calls	Default = 1. If set to one, when either the primary or secondary phone are in use, any additional incoming call receives busy treatment. If set to two, when either phone is in use, it receives call waiting indication for any second call. Any further calls above two receive busy treatment.
Twin Bridge Appearances	Default = Off. By default only calls alerting on the primary phone's call appearance buttons also alert at the secondary. When this option is enabled, calls alerting on a bridged appearance button at the primary can also alert at the secondary.
Twin Coverage Appearances	Default = Off. By default only calls alerting on the primary phone's call appearance buttons also alert at the secondary. When this option is enabled, calls alerting on a coverage appearance button at the primary can also alert at the secondary.
Twin Line Appearances:	Default = Off. By default only calls alerting on the primary phone's call appearance buttons also alert at the secondary. When this option is enabled, calls alerting on a line appearance button at the primary can also alert at the secondary.
Mobility Features If enabled this option allows any of the mobility features to be enabled for the user.	
Mobile Twinning	If selected, the user is enable for mobile twinning. The user can control this option through a Twinning programmable button on their a phone. For user's setup for one-X Mobile Client, changes to their Mobile Twinning status made through the system configuration or using a **Twinning** button are not reflected in the status of the **Extension to Cellular** icon on their mobile client. However, changes to the **Extension to Cellular** status made from the mobile client are reflected by the **Mobile Twinning** field in the system configuration. Therefore, for one-X Mobile Client users, it is recommended that they control their Mobile Twinning status through the one-X Mobile Client rather than through a **Twinning** button.

Table continues…

Field	Description
Fallback Twinning	Default = Disabled When Fallback Twinning is enabled and the user's primary extensions are unreachable, IP Office redirects the calls to the Twinned Mobile Number even if Mobile Twinning is disabled. The Mobile Dial Delay time set up by the user is not considered during Fallback Twinning.
Twinned Mobile Number	Default = Blank. This field sets the external destination number for mobile twinned calls. It is subject to normal short code processing and should include any external dialing prefix if necessary. For users of Mobile Call Control, the number in this field is used to match the users setting to the incoming CLI.
Twinning Time Profile	Default = <None> (Any time) This field allows selection of a time profile during which mobile twinning will be used.
Mobile Dial Delay	Default = 2 seconds This setting controls how long calls should ring at the user's primary extension before also being routed to ring at the twinning destination number. This setting may be used at the user's choice, however it may also be a necessary control. For example, if the twinning number is a mobile device that has been switched off, the mobile service provider may immediately answer the call with their own voicemail service. This would create a scenario where the user's primary extension does not ring or ring only briefly.
Mobile Answer Guard	Default = 0 (Off). Range = 0 to 99 seconds. This control can be used in situations where calls sent to the twinned destination are automatically answered by a voicemail service or automatic message if the twinned device is not available. If a twinned call is answered before the **Mobile Answer Guard** expires, the system will drop the call to the twin.
Hunt group calls eligible for mobile twinning	Default = Off This setting controls whether hunt group calls ringing the user's primary extension should also be presented to the mobile twinning number.
Forwarded calls eligible for mobile twinning	Default = Off This setting controls whether calls forwarded to the user's primary extension should also be presented to the mobile twinning number.

Table continues…

Field	Description
Twin When Logged Out	Default = Off. If enabled, if the user logs off their primary extension, calls to that extension will still alert at their twinned device rather than going immediately to voicemail or busy. • When logged out but twinned, **Mobile Dial Delay** is not applied. • Hunt group calls (all types) will be twinned if **Hunt group calls eligible for mobile twinning** is enabled. When this is the case the user's idle time is reset for each externally twinned call answered. Note that calls twinned over analog and analog emulation trunks are automatically treated as answered. • When the user's **Mobile Time Profile**, if configured, is not active they will not get twinning calls. Calls will be treated the same as the user was logged out user with no twinning. • Callback calls initiated by the user will mature to the **Twinned Mobile Number**. It will also be possible to initiate Automatic Callback to the user with external twinning and their busy/free state will be tracked for all calls via the system. • Any Bridged Appearance set to the user will not alert. Coverage appearance buttons for the user will continue to operate. • The BLF/user button status shown for a logged out user with **Logged Off Mobile Twinning** is as follows: - If there are any calls alerting or in progress through the system to the twin the user status is shown as alerting or in-use as appropriate. This includes the user showing as busy/in-use if they have such a call on hold and they have Busy on Held enabled. - If the user enables DND through Mobile Call Control or one-X Mobile client their status will show as DND/busy. - Calls from the system dialed direct to the users twinned destination rather than directed by twinning from their primary extension will not change the user's status.
one-X Mobile Client	Default = Off. one-X Mobile Client is a software application that can be installed on Windows Mobile and Symbian mobile cell phones. It allows the user to access a number of system features.
Mobile Call Control	Default = Off. This feature allows a user receiving a call on their twinned device to access system dial tone and then perform dialing action including making calls and activating short codes. See Mobile Call Control on page 631.
Mobile Callback	Default = Off. Mobile callback allows the user to call the system and then hang up. The system will then make a call to the user's CLI and when answered, provide them with dial tone from the system to make calls. SeeMobile Callback on page 635 .

Field	Description
Internal Twinning Select this option to enable internal twinning for a user. **Internal Twinning** cannot be selected for a user if they already have **Mobility Features** selected. Internal twinning is not supported across an SCN or SE network. Internal twinning is not supported during resilience.	
Twinned Handset	Default = Blank. For internal twinning, the drop-down list can be used to select an available user as the twinned calls destination. The secondary phone: • must be on the same system • must not be a simultaneous mode phone. For example, Avaya Communicator (for Windows, iPad, or Web), or WebRTC web client. If the list is grayed out, the user is a twinning destination and the primary to which they are twinned is displayed. All **Call Management** > **Users** > **Add/Edit Users** > **Mobility** fields are grayed out for unlicensed users.
Maximum Number of Calls	Default = 1. If set to one, when either the primary or secondary phone are in use, any additional incoming call receives busy treatment. If set to two, when either phone is in use, it receives call waiting indication for any second call. Any further calls above two receive busy treatment.
Twin Bridge Appearances	Default = Off. By default only calls alerting on the primary phone's call appearance buttons also alert at the secondary. When this option is enabled, calls alerting on a bridged appearance button at the primary can also alert at the secondary.
Twin Coverage Appearances	Default = Off. By default only calls alerting on the primary phone's call appearance buttons also alert at the secondary. When this option is enabled, calls alerting on a coverage appearance button at the primary can also alert at the secondary.
Twin Line Appearances:	Default = Off. By default only calls alerting on the primary phone's call appearance buttons also alert at the secondary. When this option is enabled, calls alerting on a line appearance button at the primary can also alert at the secondary.
Mobility Features If enabled this option allows any of the mobility features to be enabled for the user.	

Table continues…

Field	Description
Mobile Twinning	If selected, the user is enable for mobile twinning. The user can control this option through a Twinning programmable button on their a phone. For user's setup for one-X Mobile Client, changes to their Mobile Twinning status made through the system configuration or using a **Twinning** button are not reflected in the status of the **Extension to Cellular** icon on their mobile client. However, changes to the **Extension to Cellular** status made from the mobile client are reflected by the **Mobile Twinning** field in the system configuration. Therefore, for one-X Mobile Client users, it is recommended that they control their Mobile Twinning status through the one-X Mobile Client rather than through a **Twinning** button.
Fallback Twinning	Default = Disabled When Fallback Twinning is enabled and the user's primary extensions are unreachable, IP Office redirects the calls to the Twinned Mobile Number even if Mobile Twinning is disabled. The Mobile Dial Delay time set up by the user is not considered during Fallback Twinning.
Twinned Mobile Number	Default = Blank. This field sets the external destination number for mobile twinned calls. It is subject to normal short code processing and should include any external dialing prefix if necessary. For users of Mobile Call Control, the number in this field is used to match the users setting to the incoming CLI.
Twinning Time Profile	Default = <None> (Any time) This field allows selection of a time profile during which mobile twinning will be used.
Mobile Dial Delay	Default = 2 seconds This setting controls how long calls should ring at the user's primary extension before also being routed to ring at the twinning destination number. This setting may be used at the user's choice, however it may also be a necessary control. For example, if the twinning number is a mobile device that has been switched off, the mobile service provider may immediately answer the call with their own voicemail service. This would create a scenario where the user's primary extension does not ring or ring only briefly.
Mobile Answer Guard	Default = 0 (Off). Range = 0 to 99 seconds. This control can be used in situations where calls sent to the twinned destination are automatically answered by a voicemail service or automatic message if the twinned device is not available. If a twinned call is answered before the **Mobile Answer Guard** expires, the system will drop the call to the twin.
Hunt group calls eligible for mobile twinning	Default = Off This setting controls whether hunt group calls ringing the user's primary extension should also be presented to the mobile twinning number.
Forwarded calls eligible for mobile twinning	Default = Off This setting controls whether calls forwarded to the user's primary extension should also be presented to the mobile twinning number.

Table continues…

Field	Description
Twin When Logged Out	Default = Off. If enabled, if the user logs off their primary extension, calls to that extension will still alert at their twinned device rather than going immediately to voicemail or busy. • When logged out but twinned, **Mobile Dial Delay** is not applied. • Hunt group calls (all types) will be twinned if **Hunt group calls eligible for mobile twinning** is enabled. When this is the case the user's idle time is reset for each externally twinned call answered. Note that calls twinned over analog and analog emulation trunks are automatically treated as answered. • When the user's **Mobile Time Profile**, if configured, is not active they will not get twinning calls. Calls will be treated the same as the user was logged out user with no twinning. • Callback calls initiated by the user will mature to the **Twinned Mobile Number**. It will also be possible to initiate Automatic Callback to the user with external twinning and their busy/free state will be tracked for all calls via the system. • Any Bridged Appearance set to the user will not alert. Coverage appearance buttons for the user will continue to operate. • The BLF/user button status shown for a logged out user with **Logged Off Mobile Twinning** is as follows: - If there are any calls alerting or in progress through the system to the twin the user status is shown as alerting or in-use as appropriate. This includes the user showing as busy/in-use if they have such a call on hold and they have Busy on Held enabled. - If the user enables DND through Mobile Call Control or one-X Mobile client their status will show as DND/busy. - Calls from the system dialed direct to the users twinned destination rather than directed by twinning from their primary extension will not change the user's status.
one-X Mobile Client	Default = Off. one-X Mobile Client is a software application that can be installed on Windows Mobile and Symbian mobile cell phones. It allows the user to access a number of system features.
Mobile Call Control	Default = Off. This feature allows a user receiving a call on their twinned device to access system dial tone and then perform dialing action including making calls and activating short codes. See Mobile Call Control on page 631.
Mobile Callback	Default = Off. Mobile callback allows the user to call the system and then hang up. The system will then make a call to the user's CLI and when answered, provide them with dial tone from the system to make calls. SeeMobile Callback on page 635 .

Related links

Add Users on page 98

Group Membership

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Group Membership**

This tab displays the groups of which the user has been made a member.

Related links

Add Users on page 98

Voice Recording

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

Used to activate the automatic recording of user's external calls. The recording of internal calls is also supported.

Call recording requires Voicemail Pro to be installed and running. Call recording also requires available conference resources similar to a 3-way conference.

Note the following:

- Calls to and from IP devices, including those using Direct media, can be recorded.
- Calls parked or held pause recording until the unparked or taken off hold (does not apply to SIP terminals).
- Recording is stopped if:
  - User recording stops if the call is transferred to another user.
  - User account code recording stops if the call is transferred to another user.
  - Hunt group recording stops if the call is transferred to another user who is not a member of the hunt group.
  - Incoming call route recording continues for the duration of the call on the system.

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

Field	Description
Auto Recording	
Inbound	Default = None. Select whether automatic recording of incoming calls is enabled. The field to the right sets whether just external, just internal, or both external and internal calls are included. The options are: • **None**: Do not automatically record calls. • **On**: Record the call if possible. If not possible to record, allow the call to continue. • **Mandatory**: Record the call if possible. If not possible to record, block the call and return busy tone. • **Percentages of calls**: Record a selected percentages of the calls.

Table continues…

Field	Description
Outbound	Default = None. Select whether automatic recording of out going calls is enabled. The field to the right sets whether just external, just internal, or both external and internal calls are included. The options are: • **None**: Do not automatically record calls. • **On**: Record the call if possible. If not possible to record, allow the call to continue. • **Mandatory**: Record the call if possible. If not possible to record, block the call and return busy tone. • **Percentages of calls**: Record a selected percentages of the calls.
Destination	Default = None. Sets the destination for automatically triggered recordings. The options are: • **Voice Recording Library**: This options set the destination for the recording to be a VRL folder on the voicemail server. The ContactStore application polls that folder and collects waiting recordings which it then places in its own archive. Recording is still done by Voicemail Pro. • **Voice Recording Library Authenticated**: This option is similar to Voice Recording Library above but instructs the voicemail server to create an authenticated recording. If the file contents are changed, the file is invalidated though it can still be played. This option is not currently supported with Linux based systems.
Time Profile	Default = None. (Any time). Used to select a time profile during which automatic call recording of incoming calls is applied. If no profile is selected, automatic recording of incoming calls is active at all times.
Manual Recording	
Destination	Default = None. Sets the destination for automatically triggered recordings. The options are: • **Voice Recording Library**: This options set the destination for the recording to be a VRL folder on the voicemail server. The ContactStore application polls that folder and collects waiting recordings which it then places in its own archive. Recording is still done by Voicemail Pro. • **Voice Recording Library Authenticated**: This option is similar to Voice Recording Library above but instructs the voicemail server to create an authenticated recording. If the file contents are changed, the file is invalidated though it can still be played.

Related links

Add Users on page 98

Do Not Disturb

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Do Not Disturb**

Additional configuration information

For additional configuration information, see DND, Follow Me, and Forwarding on page 598.

See Do Not Disturb in the Telephone Features section for full details of Do Not Disturb operation.

Do not disturb prevents the user from receiving hunt group and page calls. Direct callers hear busy tone or are diverted to voicemail if available. It overrides any call forwarding, follow me and call coverage settings. A set of exception numbers can be added to list numbers from which the user still wants to be able to receive calls when they have do not disturb in use.

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

Field	Description
Do Not Disturb	Default = Off When checked the user's extension is considered busy, except for calls coming from sources listed in their Do Not Disturb Exception List. When a user has do not disturb in use, their normal extension will give alternate dialtone when off hook. Users with DND on are indicated as 'busy' on any BLF indicators set to that user.
Do Not Disturb Exception List	Default = Blank This is the list of telephone numbers that are still allowed through when Do Not Disturb is set. For example this could be an assistant or an expected phone call. Internal extension numbers or external telephone numbers can be entered. If you wish to add a range of numbers, you can either enter each number separately or make use of the wildcards "N" and "X" in the number. For example, to allow all numbers from 7325551000 to 7325551099, the DND Exception number can be entered as either 73255510XX or 73255510N. Note that this list is only applied to direct calls to the user. Calls to a hunt group of which the user is a member do not use the Do Not Disturb Exceptions list.

Related links

Add Users on page 98

Announcements

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

Announcements are played to callers waiting to be answered. This includes callers being presented to hunt group members, ie. ringing, and callers queued for presentation.

- The system supports announcements using Voicemail Pro or Embedded Voicemail.
- If no voicemail channel is available for an announcement, the announcement is not played.
- In conjunction with Voicemail Pro, the system allows a number of voicemail channels to be reserved for announcements. See **System Settings** > **System** > **Voicemail**.
- With Voicemail Pro, the announcement can be replaced by the action specified in a Queued (1st announcement) or Still Queued (2nd announcement) start point call flow. Refer to the Voicemail Pro Installation and Maintenance documentation for details.

- Calls can be answered during the announcement. If it is a mandatory requirement that announcements should be heard before a call is answered, then a Voicemail Pro call flow should be used before the call is presented.

  Note:

  Call Billing and Logging

  A call becomes connected when the first announcement is played to it. That connected state is signaled to the call provider who may start billing at that point. The call will also be recorded as answered within the SMDR output once the first announcement is played.

- If a call is rerouted, for example forwarded, the announcement plan of the original user is still applied until the call is answered. The exception is calls rerouted to a hunt group at which point the hunt group announcement settings are applied.
- For announcements to be used effectively, either the user's no answer time must be extended beyond the default 15 seconds or Voicemail On should be deselected.

Recording Announcements

Voicemail Pro:

There is no mechanism within the telephony user interfaces (TUI) to record user announcements. To provide custom announcements, user queued and still queued start points must be configured with Voicemail Pro with the required prompts played by a generic action.

Embedded Voicemail:

Embedded Voicemail does not include any default announcement or method for recording an announcement. The Record Message short code feature is provided to allow the recording of announcements. The telephone number field of short codes using this feature requires the extension number followed by either ".1" for announcement 1 or ".2" for announcement 2. For example, for extension number 300, the short codes ***91N# | Record Message | N".1"** and ***92N# | Record Message | N".2"** could be used to allow recording of the announcements by dialing ***91300#** and ***92300#**.

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

Field	Description
Announcements On	Default = Off. This setting enables or disables announcements.
Wait before 1st announcement:	Default = 10 seconds. Range = 0 to 255 seconds. This setting sets the time delay from the calls presentation, after which the first announcement should be played to the caller.
Flag call as answered	Default = Off. This setting is used by the CCC and CBC applications. By default they do not regarded a call as answered until it has been answered by a person or by a Voicemail Pro action with **Flag call as answered** selected. This setting allows calls to be marked as answered once the caller has heard the first announcement.

Table continues…

Field	Description
Post announcement tone	Default = Music on hold. Following the first announcement, you can select whether the caller should hear Music on Hold, **Ringing** or **Silence** until answered or played another announcement.
2nd Announcement	Default = On. If selected, a second announcement can be played to the caller if they have still not been answered.
Wait before 2nd announcement	Default = 20 seconds. Range = 0 to 255 seconds. This setting sets the wait between the 1st and the 2nd announcement.
Repeat last announcement	Default = On. If selected, the last announcement played to the caller is repeated until they are answered or hang-up.
Wait before repeat	Default = 20 seconds. Range = 0 to 255 seconds. If **Repeat last announcement** is selected, this setting sets is applied between each repeat of the last announcement.

Related links

Add Users on page 98

Personal Directory

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Personal Directory**

Each user is able to have up to 250 personal directory records (100 pre-Release 10.0), up to the overall system limit.

These records are used as follows:

- When using ETR, J129, M-Series, T-Series, 1400, 1600, 9500 or 9600 Series phones, the user is able to view and call their personal directory numbers.
- When using a J129, 1400, 1600, 9500 or 9600 Series phone, the user is also able to edit and add personal directory records.
- If the user hot desks to a 1400, 1600, 9500 or 9600 Series phone on another system in a multi-site network, they can still access their personal directory.

Users are able to view and edit their personal directory through their phone. Directory records are used for dialing and caller name matching.

Dialing

Directory Dialing:

Directory numbers are displayed by user applications such as SoftConsole. Directory numbers are viewable through the Dir function on many Avaya phones (**Contacts** or **History**). They allow the user to select the number to dial by name. The directory will also contain the names and numbers of users and hunt groups on the system.

The **Dir** function groups directory records shown to the phone user into the following categories. Depending on the phone, the user may be able to select the category currently displayed. In some

scenarios, the categories displayed may be limited to those supported for the function being performed by the user:

- **External** Directory records from the system configuration. This includes HTTP and LDAP imported records.
- **Groups** Groups on the system. If the system is in a multi-site network, it will also include groups on other systems in the network. For pre-Release 5 systems, this feature requires the systems to have **Advanced Small Community Networking** licenses.
- **Users** or **Index** Users on the system. If the system is in a multi-site network it will also include users on other systems in the network. For pre-Release 5 systems, this feature requires the systems to have **Advanced Small Community Networking** licenses.
- **Personal** Available on 1400, 1600, 9500 and 9600 Series phones. These are the user's personal directory records stored within the system configuration.

Speed Dialing:

On M-Series and T-Series phones, a Speed Dial button or dialing **Feature 0** can be used to access personal directory records with an index number.

- **Personal**: Dial **Feature 0** followed by ***** and the 2-digit index number in the range 01 to 99.
- **System**: Dial **Feature 0** followed by 3-digit index number in the range 001 to 999.
- The Speed Dial short code feature can also be used to access a directory speed dial using its index number from any type of phone.

Caller Name Matching

Directory records are also used to associate a name with the dialled number on outgoing calls or the received CLI on incoming calls. When name matching is being done, a match in the user's personal directory overrides any match in the system directory. Note that some user applications also have their own user directory.

SoftConsole applications have their own user directories which are also used by the applications name matching. Matches in the application directory may lead to the application displaying a different name from that shown on the phone.

Name matching is not performed when a name is supplied with the incoming call, for example QSIG trunks. On SIP trunks the use of the name matching or the name supplied by the trunk can be selected using the setting **System Settings** > **System** > **Telephony** > **Default Name Priority**. This setting can also be adjusted on individual SIP lines to override the system setting.

Directory name matching is not supported for DECT handsets. For information on directory integration, see *IP DECT R4 Installation Manual*.

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

Field	Description
Index	Range = 00 to 99 or None. This value is used with personal speed dials set and dialed from M and T-Series phones. The value can be changed but each value can only be applied to one directory record at any time. Setting the value to **None** makes the speed dial inaccessible from M and T-Series phones, however it may still be accessible from the directory functions of other phones and applications. The Speed Dial short code feature can be used to create short codes to dial the number stored with a specific index value. Release 10.0 allows users to have up to 250 personal directory entries. However, only 100 of those can be assigned index numbers.
Name	Range = Up to 31 characters. Enter the text to be used to identify the number.
Number	Range = Up to 31 digits plus * and #. Enter the number, without spaces, to be dialed. Wildcards are not supported in user personal directory records. Note that if the system has been configured to use an external dialing prefix, that prefix should be added to directory numbers.

Related links

Add Users on page 98

SIP

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

This tab is available when either of the following has been added to the configuration:

- an **IP Office Line**
- a SIP trunk with a SIP URI record containing a field that has been set to **Use Internal Data**.

Various fields within the URI settings used by SIP trunks can be set to **Use Internal Data**. When that is the case, the values from this tab are used inserted into the URI when the user makes or receives a SIP call. Within a multi-site network, that includes calls which break out using a SIP trunk on another system within the network.

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

Field	Description
SIP Name	Default = Blank on Voicemail tab/Extension number on other tabs. The value from this field is used when the From field of the SIP URI being used for a SIP call is set to **Use Internal Data**.
SIP Display Name (Alias)	Default = Blank on Voicemail tab/Name on other tabs. The value from this field is used when the Display Name field of the SIP URI being used for a SIP call is set to **Use Internal Data**.

Table continues…

Field	Description
Contact	Default = Blank on Voicemail tab/Extension number on other tabs. The value from this field is used when the Contact field of the SIP URI being used for a SIP call is set to **Use Internal Data**.
Anonymous	Default = On on Voicemail tab/Off on other tabs. If the From field in the SIP URI is set to **Use Internal Data**, selecting this option inserts **Anonymous** into that field rather than the SIP Name set above.

Related links

Add Users on page 98

Menu Programming

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

This tab is used to set and lock the user's programmable button set.

When **Apply User Rights value** is selected, the tab operates in the same manner as the User | Menu Programming tab.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Related links

Add Users on page 98
Menu Programming — T3 Telephony on page 140
Menu Programming — Hunt Group on page 141
Menu Programming — 4400/6400 on page 141

Menu Programming — T3 Telephony

Navigation: **Call Management** > **Users** > **Edit** > **Advanced** > **Menu Programming** > **T3 Telephony**

These settings are applied to the user when they are using a T3 phone.

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

Configuration Settings

Third Party Forwarding Avaya T3 phone users can be given menu options to change the forwarding settings of other users. In addition to the following controls, this functionality is protected by the forwarding user's log in code.

- **Allow Third Party Forwarding**: Default = Off Sets whether this user can change the forwarding settings of other users.
- **Protect from Third Party Forwarding**: Default = Off Sets whether this user's forwarding settings can be changed by other users.

Advice of Charge

Display Charges: Default = On. This setting is used to control whether the user sees ISDN AOC information when using a T3 phone.

Allow Self Administer: Default = Off. If selected, this option allows the user to self-administer button programming.

Related links

Menu Programming on page 140

Menu Programming — Hunt Group

Navigation: **Call Management** > **Users** > **Edit** > **Advanced** > **Menu Programming** > **Hunt Group**

Avaya T3, 1400, 1600, 9500 and 9600 Series phone users can control various settings for selected hunt groups. These settings are also used for one-X Portal for IP Office.

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

Configuration Settings

Can Change Membership: Default = Off This list shows the hunt groups of which the user is a member. Up to 10 of these groups can be checked; those group and the users current membership status are then displayed on the phone. The user can change their membership status through the phone's menus.

T3 Series Phones: The selected hunt groups and the user's current membership status are displayed on the T3 phones status display. That display can be used to change the status.

Can Change Service Status: Default = Off This list shows all the hunt groups on the system. Up to 10 of these groups can be checked.

T3 Series Phones:

The user is then able to view and change the service status of the checked groups through their T3 phones menus (**Menu | Group State**).

In addition to changing the status of the individual hunt groups displayed via **Menu | Group State**, the menu also displays option to change the status of all the groups; **All in service**, **All night service** and **All out service**.

Can Change Night Service Group: Default = Off. If selected, the user can change the fallback group used when the hunt group is in Night Service mode.

Can Change Out of Service Group: Default = Off. If selected, the user can change the fallback group used when the hunt group is in Out of Service mode.

Related links

Menu Programming on page 140

Menu Programming — 4400/6400

Navigation: **Call Management** > **Users** > **Edit** > **Advanced** > **Menu Programming** > **4400/6400**

4412, 4424, 4612, 4624, 6408, 6416 and 6424 phones have a **Menu** key, sometimes marked with an  icon. When **Menu** is pressed, a number of default functions are displayed. The < and >

keys can be used to scroll through the functions while the keys below the display can be used to select the required function.

The default functions can be overwritten by selections made within this tab.

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

Configuration Settings

Menu No. The menu position which the function is being set.

Label This is a text label for display on the phone. If no label is entered, the default label for the selected action is used. Labels can also be changed through the menu on some phones, refer to the appropriate telephone user guide.

Action Defines the action taken by the menu button.

Action Data This is a parameter used by the selected action. The options here will vary according to the selected button action.

Related links

Menu Programming on page 140

Dial In

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Dial In**

Use this dialogue box to enable dial in access for a remote user. An Incoming Call Route and RAS service must also be configured.

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

Field	Description
Dial In On	Default = Off When enabled, dial in access into the system is available via this user.
Dial In Time Profile	Default = <None> Select the Time Profile applicable to this User account. A **Time Profile** can be used to set time restrictions on dial in access via this User account. Dial In is allowed during the times set in the Time Profile form. If left blank, then there are no restrictions.
Dial In Firewall Profile	Default = <None> Select the Firewall Profile to restrict access to the system via this User account. If blank, there are no Dial In restrictions.

Related links

Add Users on page 98

Source Numbers

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Source Numbers**

This page is used to enter values that have special usages. These are entered using the **Add**, **Edit** and **Remove** buttons.

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

User Source Numbers

The following types of records can be added to a user's source numbers:

Value	Description
AT<string>	Strings beginning with AT can be used with a user called **DTEDefault** to configure the default settings of the control unit's DTE port.
BST_MESSAGE_FOR_YOU	If set, then the BST phone user sees the top line **Message for you** or **Messages for you**, indicating that voicemail messages are present. This source number can be used as a NoUser source number to enable the feature for all users.
BST_NO_MESSAGE_FOR_YOU	If the source number above has been used as a NoUser source number to enable the feature for all BST users, this individual user source number can be used to disable the feature for selected users. If set, the user does not see a message indication when the NoUser setting **BST_MESSAGE_FOR_YOU** is set. The user's phone presents the idle date/time in the normal fashion.
Enable_OTT	Enable one touch transfer operation for the user.
H<Group_Name>	Allows the user to receive message waiting indication of new group messages. Enter H followed by the group name, for example **HMain**. The group is added to the user's Visual Voice menu. On suitable display extensions, the hunt group name and number of new messages is displayed. Refer to the appropriate telephone user guide. If the user is not a member of the group, a voicemail code must be set for the group's mailbox. See the setting **Call Management** > **Group** > **Add/Edit Group** > **Voicemail** > **Voicemail Code** .
P<Telephone Number>	This record sets the destination for callback (outbound alert) calls from voicemail. Enter Pfollowed by the telephone number including any necessary external dialing prefix, for example P917325559876. This facility is only available when using Voicemail Pro through which a default Callback or a user specific Callback start point has been configured. Refer to the Voicemail Pro documentation. This feature is separate from voicemail ringback and Voicemail Pro outcalling.
R<Caller's ICLID>	To allow Dial In/RAS call access only from a specified number prefix the number with a "R", for example **R7325551234**.

Table continues…

Value	Description
U<User_Name or Extension#>	Allows the user to receive message waiting indication of new messages. Enter U followed by the user name or extension number, for example **U201**. The specified user is added to the user's Visual Voice menu. On suitable display extensions, the user name and number of new messages is displayed. Refer to the appropriate telephone user guide. If the user is not a trusted source and a Voicemail Code exists, the user must enter the Voicemail Code corresponding to the monitored mailbox.
V<Caller's ICLID>	Strings prefixed with a **V** indicate numbers from which access to the users mailbox is allowed without requiring entry of the mailbox's voicemail code. This is referred to as "trusted source". For Voicemail Pro running in Intuity mode, trusted source is used for calls from programmable buttons set to Voicemail Collect and Visual Voice. Other controls are prompted for the mailbox number and then password.

NoUser Source Numbers

The following source numbers can also be used on the **Source Numbers** tab of the NoUser user. These affect all users on the system.

Note:

Changes to these source numbers require a system reboot to become effective.

Value	Description
ATM4U_PCS7_RINGDETECT	For some cellular or mobile interfaces connected to a IP500 ATM4U card, the card may not detect the ring signal. For PCS4 and higher card this NoUser source number can be used activate alternate ring detection. Refer to IP Office Technical Tip 204.
ALLOW_5410_UPGRADES	Previously the only control over the upgrading of 5410 phones was controlled by the use of the turn_on.bat and turn_off.bat batch files installed with the Manager application. Now in addition, this option must be present for 5410 phones to update their firmware. Refer to the IP Office Installation manual for full details.
B_DISABLE_SIP_IPADDR	Disables the blacklisting of SIP device registration based on the device IP address. Refer to the IP Office Security Guidelines document for more details.
BST_MESSAGE_FOR_YOU	If set, all BST phones display the top line **Message for you** or **Messages for you**, indicating that voicemail messages are present.
DECT_REVERSE_RING	By default, when this parameter is not set, calls on DECT phones associated with a CTI application will ring as a Priority call. When this parameter is set, DECT phones ring as a normal, external or internal, call.
DISTINCT_HOLD_RINGBACK	Used to display a specific message about the call type for calls returning after timing out from being parked or held. If set, such calls display **Return Call - Held** or **Return Call – Parked** rather than connected party name or line name.
Enable_OTT	Enable one touch transfer for all users.

Table continues…

Value	Description
FORCE_HANDSFREE_TRANSFER	If set, when using the handsfree announced transfer process, both the transfer enquiry and transfer completion calls are auto-answered. Without this setting only the transfer enquiry call is auto-answered.
HIDE_CALL_STATE	Used to hide the call status information, for example Dial, Conn, etc, on DS phones. Used in conjunction with the LONGER_NAMES option. Not supported for 1600 and 9600 Series phones.
LONGER_NAMES	Used to increase the length of names sent for display on older DS phones, i.e. 2400, 4400 and 5400 Series.
MEDIA_NAT_DM_INTERNAL=X	Used in conjunction with the setting **System Settings** > **System** > **VoIP** > **Allow Direct Media Within NAT Location** When **Allow Direct Media Within NAT Location** is set to on, The default behavior is to allow direct media between all types of devices (H323 and SIP remote workers and IP Office Lines behind a NAT). In the case of routers that have H323 or SIP ALG, it can be desirable to allow direct media only between certain categories of devices. In this case, set this NoUser user source number where X is a hex number defined as a combination of the following flags: • 0x01 (includes H323 phones) • 0x02 (includes SIP phones) • 0x04 (includes IP Office Lines) For example, if the router has SIP ALG that can't be disabled, you might want to disable direct media for SIP devices. To configure, set **MEDIA_NAT_DM_INTERNAL=5** to include only H323 phones and IP Office Lines.
NI2_CALLED_PARTY_PLAN=X	X = UNKNOWN or ISDN Forces the NI2 Called Party Numbering plan for ETSI PRI trunks.
NI2_CALLED_PARTY_TYPE=X	X = UNKNOWN, INTERNATIONAL, NATIONAL or SUBSCRIBER Forces the NI2 Called Party Numbering type for ETSI PRI trunks.
NI2_CALLING_PARTY_PLAN=X	X = UNKNOWN or ISDN Forces the NI2 Calling Party Numbering plan for ETSI PRI trunks.
NI2_CALLING_PARTY_PLAN=X	X = UNKNOWN, INTERNATIONAL, NATIONAL or SUBSCRIBER Forces the NI2 Calling Party Numbering type for ETSI PRI trunks.
NO_DIALLED_REF_EXTERNAL	On outgoing external calls made using short codes to dial the full number, only the short code dialed is displayed on the dialing user's phone and any directory matching is based on that number dialled. On systems with this source number added to the configuration, after dialing a short code the full number dialled by that short code is shown and directory matching is based on that full number.
onex_l1=X	Sets the IP address of the one-X server that can be accessed by clients registered on the LAN1 interface.
onex_l2=X	Sets the IP address of the one-X server that can be accessed by clients registered on the LAN2 interface.

Table continues…

Value	Description
onex_port_l1=X	Sets the port of the one-X server that can be accessed by clients registered on the LAN1 interface.
onex_port_l2=X	Sets the port of the one-X server that can be accessed by clients registered on the LAN2 interface.
onex_port_r1=X	Sets the port of the one-X server that can be accessed by remote clients registered on the LAN1 interface.
onex_port_r2=X	Sets the port of the one-X server that can be accessed by remote clients registered on the LAN2 interface.
onex_r1=X	Sets the IP address of the one-X server that can be accessed by remote clients registered on the LAN1 interface.
onex_r2=X	Sets the IP address of the one-X server that can be accessed by remote clients registered on the LAN2 interface.
PRESERVED_CONN_DURATION=X	X = time in minutes. Range = 1 to 120. When the setting **System Settings** > **System** > **Telephony** > **Media Connection Preservation** is enabled, preserved calls have a maximum duration of 120 minutes. After that time, they are hung up. Use this setting to change the maximum duration value.
PRESERVED_NO_MEDIA_DURATION=X	X = time in minutes. Range = 1 to 120. When the setting **System Settings** > **System** > **Telephony** > **Media Connection Preservation** is enabled, preserved calls have a maximum duration of 120 minutes. If monitoring RTP or RTCP and no speech is detected, calls are hung up after 10 minutes. Use this setting to change the default value of 10 minutes.
ProgressEndsOverlapSend	See **Line | VoIP**.
REPEATING_BEEP_ON_LISTEN	By default, if you set Beep on Listen and invoke Call Listen you'll hear an entry tone (3 beeps). When this parameter is set, you hear a beep every 10 seconds when you invoke Call Listen.
RTCP_COLLECTOR_IP=X	X = IP address of the IP Office system as configured in the Prognosis server.
RW_SBC_REG=<SBC-B1-public-SIP-IPaddr>	Used for Remote Worker Session Boarder Controller Enterprise (SBCE) configuration on 11xx, 12xx, and E129 phones. The IP address is used as a S1/S2 for 11xx and 12xx and for outbound-proxy-server for E129 sets.
RW_SBC_PROV=<SBC-B1-private-HTTP/S-IPaddr>	Used for Remote Worker Session Boarder Controller Enterprise (SBCE) configuration on 11xx, 12xx, and E129 phones. The IP address is used to determine whether a 11xx, 12xx, or E129 set is registered as an IP Office SBCE Remote Worker.
RW_SBC_TLS=<SBC-public-TLS-port>	Used for Remote Worker Session Boarder Controller Enterprise (SBCE) configuration on 11xx, 12xx, and E129 phones. The port is used as a S1/S2 TLS port for 11xx and 12xx phones and as outbound-proxy-server TLS port for E129 phones.

Table continues…

Value	Description
RW_SBC_TCP=<SBC-public-TCP-port>	Used for Remote Worker Session Boarder Controller Enterprise (SBCE) configuration on 11xx, 12xx, and E129 phones. The port is used as a S1/S2 TCP port for 11xx and 12xx phones and as outbound-proxy-server TCP port for E129 phones.
RW_SBC_UDP=<SBC-public-UDP-port>	Used for Remote Worker Session Boarder Controller Enterprise (SBCE) configuration on 11xx, 12xx, and E129 phones. The port is used as a S1/S2 UDP port for 11xx and 12xx phones and as outbound-proxy-server UDP port for E129 phones.
SET_46xx_PROCPSWD=X	X= New password When set, the new password is indicated to phones through the auto-generated settings file.
SET_96xx_SIG=X	When set, inserts the line “SET SIG X into the auto-generated settings files.
SET_HEADSYS_1	If set, alters the operation of the headset button on 96x1 phones via the auto-generated settings file. Normally the headset goes off-hook when the far end disconnects. When this option is set, the headset remains on-hook when the far end disconnects.
SIP_E129_PREFER_UDP	When set, the auto-generated E129 configuration file is altered to set the transport method as UDP regardless of whether TCP or TLS are selected on the LAN1/LAN2 VoIP configuration settings.
SIP_ENABLE_HOT_DESK	For IP Office Release 10.1, by default the use of hot-desking on J129 and H175 phones is blocked. This source numbers overrides that behavior.
SIP_EXTN_CALL_Q_TIMEOUT=X	X = Number of minutes (0 (no limit) to 255). Sets the unanswered call duration after which unanswered SIP calls are automatically disconnected. If not set, the normal default is 5 minutes.
SIP_OPTIONS_PERIOD=X	X = time in minutes. The system sends SIP options messages periodically to determine if the SIP connection is active. The rate at which the messages are sent is determined by the combination of the **Binding Refresh Time** (in seconds) set on the Network Topology tab and the **SIP_OPTIONS_PERIOD** parameter (in minutes). The frequency of sent messages is determined as follows: If no **SIP_OPTIONS_PERIOD** parameter is defined and the **Binding Refresh Time** is **0**, then the default value of 300 seconds is used. To establish a period less than 300 seconds, do not define a **SIP_OPTIONS_PERIOD** parameter and set the **Binding Refresh Time** to a value less than 300 seconds. The OPTIONS message period will be equal to the **Binding Refresh Time**. To establish a period greater than 300 seconds, a **SIP_OPTIONS_PERIOD** parameter must be defined. The **Binding Refresh Time** must be set to a value greater than 300 seconds. The OPTIONS message period will be the smaller of the **Binding Refresh Time** and the **SIP_OPTIONS_PERIOD**.
SOFTPHONE_RTP_MAX=X	X = Maximum port in the range 1024 to 65534. The maximum usable port indicated to the IP Office Video Softphone when **SOFTPHONE_RTP_RANGE_ENABLE** and **SOFTPHONE_RTP_MIN** are set.

Table continues…

Value	Description
SOFTPHONE_RTP_MIN=X	X = Minimum port in the range 1024 to 65534. The minimum usable port indicated to the IP Office Video Softphone when **SOFTPHONE_RTP_RANGE_ENABLE** and **SOFTPHONE_RTP_MAX** are set.
SOFTPHONE_RTP_RANGE_ENABLE	When set, the usable ports indicated to the IP Office Video Softphone are set via the **SOFTPHONE_RTP_MIN** and **SOFTPHONE_RTP_MAX** values.
SUPPRESS_ALARM=1	When set, suppresses the NoCallerID alarm otherwise shown in SysMonitor, SNMP traps, email notifications, SysLog or System Status.
TUI:NAME_SEARCH_MODE=1	The default directory search matching behavior is to simultaneously match against first and last name characters. This source number sets the system to match from the start of the name only.
VM_TRUNCATE_TIME=X	X= time in seconds. Range = 0 to 7. On analog trunks, call disconnection can occur though busy tone detection. When such calls go to voicemail to be recorded or leave a message, when the call ends the system indicates to the voicemail server how much to remove from the end of the recording in order to remove the busy tone segment. This amount varies by system locale, the defaults being listed below. For some systems it may be necessary to override the default if analog call recordings are being clipped or include busy tone. That can be done by adding a **VM_TRUNCATE_TIME=** setting with the required value in the range 0 to 7 seconds. • **New Zealand, Australia, China, Saudi Arabia and Custom**: 5 seconds. • **Korea**: 3 seconds. • **Italy, Mexico, Chile, Colombia and Brazil**: 2 seconds. • **Argentina, United States, Canada and Turkey**: 0 seconds. • **All other locales**: 7 seconds.
VMAIL_WAIT_DURATION=X	The number of milliseconds to wait before cutting through the audio to Voicemail. Some delay is required to allow for codec negotiation.
VMPRO_OOB_DTMF_OFF	When set, disabled the sending of out-of-band digits to the Voicemail Pro voicemail server.
xmpp_port_l1=X	X = The port of the XMPP server that can be accessed by clients registered on the LAN1 interface.
xmpp_port_l2=X	X = The port of the XMPP server that can be accessed by clients registered on the LAN2 interface.
xmpp_port_r1=X	X = The port of the XMPP server that can be accessed by remote clients registered on the LAN1 interface.
xmpp_port_r2=X	X = The port of the XMPP server that can be accessed by remote clients registered on the LAN2 interface.

Related links

Add Users on page 98

Web Self Administration

Navigation: **Call Management** > **Users** > **Add/Edit Users** > **Self Administration**

Use this page to enable self administration for users.

For a description of the configuration fields available to the user, open the help from the Self Administration user interface or see the document *Avaya IP Office™ Platform Web Self Administration*.

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

Name	Description
Self Adminstration	Default = Off. When enabled, users can log in to the Web Self Administration interface. In a web browser, enter the IP address of the system in the format `http://<ip_address>` and select **IP Office Self Administration**. Configuration settings are grouped under the following categories. • **User** • **Voicemail** • **DND** • **Forwarding** • **Mobility** • **Personal Directory** • **Button Programming** • **Download Applications** For each option, except **Download Applications**, the following can be selected: • **Visible**: If selected, the user can view the matching settings in the Self Administration user interface. • **Write**: If selected, the users can change the matching settings in the Self Administration interface. **Download Applications** can be set to **Visble**.

Table continues…

Name	Description
Media Manager Replay Self-Administration	Default = Off. When enabled, users can replay recordings on the Web Self Administration user interface. Configuration settings: • **Enable Media Manager Replay**: The field to enable replay feature for a user. • **Replay All Recordings**: The field to enable replay of all recordings for a user. • **Replay Own Recordings**: The field to enable replay of own recordings for a user. • **Replay Recordings For Group**: The field to enable replay the recordings of the selected groups for a user. Select the groups from the listed groups. • **Replay Recordings For Others**: The field to enable replay of the recordings for other users. List the users in the text box. • **Download Recordings**: The field to enable downloading of recordings for users.

Related links

Add Users on page 98

Extension

Navigation: **Call Management** > **Extensions**

Main content pane

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

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

Click **Actions** for extension template management.

Click **Add/Edit Extension** to select an extension type to add. When you click **Add/Edit Extension**, you are prompted to specify the system where the extension will be added.

Extension Filters

Filter	Description
Show All	List all provisioned extensions on all systems.
Systems	List all provisioned extensions on specific systems.
Extension Type	List a specific provisioned extension type on all systems.

Related links

Call Management on page 96
Extension Actions on page 151

Add Extension on page 152

Extension Actions

Navigation: **Call Management** > **Extensions** > **Actions**

Related links

Extension on page 150
Extension Template Management on page 151
Create From Template on page 151

Extension Template Management

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

Select the **Template Management** action to open the Extension Templates page. Click **Add** to define an extension template.

Related links

Extension Actions on page 151

Create From Template

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

Use this page to add extensions using a template. You can define extension templates by selecting **Call Management** > **Extensions** > **Actions** > **Template Management**.

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

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

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

Related links

Extension Actions on page 151
Provision Extensions on page 151

Provision Extensions

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

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

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

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

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

Related links

Create From Template on page 151

Add Extension

Navigation: **Call Management** > **Extensions** > **Add/Edit Extension**

Extension Type	Description
H323 **SIP**	IP extensions are either added manually or by the automatic detection of the phone being connected. IP extensions can also be added manually to support a third-party IP phone device.
IP DECT **SIP DECT**	An extension port manually added to match extensions within an Avaya IP DECT system connected to the system via an IP DECT line.

Related links

Extension on page 150
Extension Common Fields on page 152
H323 Extension VoIP on page 155
SIP Extension VOIP on page 159
T38 Fax on page 163
IP DECT Extension on page 165

Extension Common Fields

Navigation: **Call Management** > **Extensions** > **Edit Extension** > **Common**

Additional configuration information

The Caller Display Type setting controls the presentation of caller display information. For additional configuration information, see Caller Display on page 529.

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 518.

Configuration Settings

These settings can be edited online except **Base Extension** and **Caller Display Type**. Changes to those settings require a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Extension ID	The physical ID of the extension port. Except for IP extensions, this settings is allocated by the system and is not configurable.
Base Extension	Range = 2 to 15 digits. This is the directory number of the extension's default associated user if one is required. The field does not have to match a user, in which case user's need to login to use the extension. The field can be left blank for digital and analogue extensions, creating and extension where users are forced to login but the extension has no default associated user. This option is not supported for IP and CTI extensions. Following a restart, the system will attempt to log in the user with the same extension number (if they are not already logged in elsewhere in the multi-site network). This does not occur if that user is set to **Force Login**. If another user logs onto an extension, when they log out, the extension returns to its default associated user unless they have logged in elsewhere or are set to **Force Login**.
Phone Password	Default = Blank. Range = Up to 31 digits. H.323 Extensions only. Does not apply to DECT phones. The password that must be entered as part of phone registration. This password is used to secure registration of H.323 phones when there is no matching user to authenticate against. Required if Media Security is enabled.
Caller Display Type	Default = On. Controls the presentation of caller display information for analog extensions. For digital and IP extensions, this value is fixed as **On**. The table below lists the supported options, all others are currently not used and default to matching **UK**.

Type	Description
Off	Disables caller display.
On	Enables caller display using the caller display type appropriate to the System Locale, see *Avaya IP Office™ Platform Locale Settings*. If a different setting is required it can be selected from the list of supported options. For an analog extension connected to a fax server or other device that requires the pass through of DTMF tones, select DTMFF.
UK	FSK before the first ring conforming to BT SIN 227. Name and number.
UK20	As per UK but with a maximum length of 20 characters. Name and number.

Table continues…

Field	Description	
	DTMFA	Caller ID in the DTMF pattern A<caller ID>C. Number only.
	DTMFB	Caller ID in DTMF after call connection. Number only.
	DTMFC	Caller ID in the DTMF pattern A<caller ID>#. Number only.
	DTMFF	Sends the called number in DTMF after call connection. Number only. Used for fax servers. When calls are delivered via a hunt group it is recommended that hunt group queuing is not used. If hunt group queuing is being used, set the Queue Type to Assign Call on Agent Alert.
	DTMFD	Caller ID in the DTMF pattern D<caller ID>C. Number only.
	FSKA	Variant of UK used for BT Relate 1100 phones. Name and number.
	FSKB	ETSI specification with 0.25 second leading ring. Name and number.
	FSKC	ETSI specification with 1.2 second leading ring. Name and number.
	FSKD	Conforms to Belcore specification. Name and number.
Reset Volume after Calls	Default = Off. Resets the phone's handset volume after each call. This option is supported on Avaya 1400, 1600, 2400, 4400, 4600, 5400, 5600, 6400, 9500 and 9600 Series phones.	
Device Type	This field indicates, the last known type of phone connected to the extension port. • Analogue extension ports always report as **Analog Handset** since the presence or absence of actual analog phone cannot be detected. • Digital extension ports report the type of digital phone connected or **Unknown digital handset** if no phone is detected. • H.323 extensions report the type of IP phone registered or **Unknown H.323 handset** if no phone is currently registered as that extension. • SIP extensions report the type of SIP phone registered or **Unknown SIP device** if no SIP device is currently registered as that extension. Applications such as Avaya Communicator and one-X Mobile Preferred that do not use extension records also display Device type as **Unknown SIP device**. For some types of phone, the phone can only report its general type to the system but not the specific model. When that is the case, the field acts as a drop-drown to allow selection of a specific model. The value selected here is also reported in other applications such as the System Status Application, SNMP, etc.	
	Default Type	**Possible Phone Models**
	T7100	M7100, M7100N, T7100, Audio Conferencing Unit.
	T7208	M7208, M7208N, T7208.
	M7310	M7310, M7310N, T7406, T7406E.
	M7310BLF	M7310BLF, T7316.
	M7324	M7324, M7324N.

Table continues…

Field	Description
Location	Specify a location to associate the extension with a physical location. Associating an extension with a location allows emergency call routing using settings specific to that location. The drop down list contains all locations that have been defined in the Location page. The display of location based time is only supported on 1100, 1200, 1600 and 9600 Series (96x0 and 96x1) phones and D100, E129 and B179 telephones.
Fallback as Remote Worker	Default = Auto. Determines what fallback address is used for Remote Worker phone resiliency. The options are: • **Auto**: Use the fallback address configured on the IP Office Line providing the service. • **No**: Use the alternate gateway private address. • **Yes**: Use the alternate gateway public address.
Module	This field indicates the external expansion module on which the port is located. **BP** indicates an analog phone extension port on the base or control unit. **BD** indicates a digital station (DS) port on the control unit. For an IP500 V2 control unit, **BD** and **BP** is also followed by the slot number. VoIP extensions report as **0**.
Port	This field indicates the port number on the **Module** indicated above. VoIP extensions report as **0**.
Disable Speakerphone	Default = Off (Speakerphone enabled). When selected, disables the fixed **SPEAKER** button if present on the phone using this extension port. Only supported on Avaya DS, TCM and H.323 IP phones. An audible beep is sounded when a disabled **SPEAKER** button is pressed. Incoming calls such as pages and intercom calls are still connected but the speech path is not audible until the user goes off-hook using the handset or headset. Similarly calls made or answered using other buttons on the phone are not audible unless the user goes off-hook using the handset or headset. Currently connected calls are not affected by changes to this setting.

Related links

Add Extension on page 152

H323 Extension VoIP

Navigation: **Call Management** > **Extensions** > **Edit Extension** > **H323 VoIP**

These settings are shown for a H.323 IP extension.

These settings can only be edited offline. Changes to these settings require a reboot of the system.

Field	Description
IP Address	Default = 0.0.0.0 The IP address of the phone. The default setting accepts connection from any address. For phones using DHCP, the field is not updated to show the IP address being used by the phone. The **IP Address** field can be used to restrict the the source IP address that can used by a Remote H.323 Extension. However, it should not used in the case where there is more than one remote extension behind the domestic router.
MAC Address	Default = 0000000000000 (Grayed out) This field is grayed out and not used.
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. The supported codecs (in default preference order) are: **G.711 A-Law**, **G.711 U-Law**, **G.722**, **G.729** and **G.723.1**. The default order for G.711 codecs will vary to match the system's default companding setting. **G.723.1** and **G.729b** are not supported on Linux based systems. The codecs available to be used are set through the **System Codec** list (System | System Codec). The options are: • **System Default**: This is the default setting. When selected, the codec list below show matches the codecs set in the system wide **Default Selection** list (System | Codecs). • **Custom**: This option allows specific configuration of the codec preferences to be different from the system **Default Selection** list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.
TDM | IP Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the system TDM interface to the IP connection. This field is not shown on Linux based platforms.
IP | TDM Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the IP connection to the system TDM interface. This field is not shown on Linux based platforms.
Supplementary Services	Default = H450. Selects the supplementary service signaling method for use with non-Avaya IP devices. Options are **None**, **QSIG** and **H450**. For H450, hold and transfer are supported. Note that the selected method must be supported by the remote end.

Table continues…

Field	Description
Media Security	Default = Same as System. These settings control whether SRTP is used for this extension and the settings used for the SRTP. The options are: • **Same as System**: Matches the system setting at **System Settings** > **System** > **VoIP Security**. • **Disabled**: Media security is not required. All media sessions (audio, video, and data) will be enforced to use RTP only. • **Preferred**: Media security is preferred. Attempt to use secure media first and if unsuccessful, fall back to non-secure media. • **Enforced**: Media security is required. All media sessions (audio, video, and data) will be enforced to use SRTP only. **Warning:** Selecting **Enforced** on a line or extension that does not support media security will result in media setup failures.
Advanced Media Security Options	Not displayed if **Media Security** is set to **Disabled**. The options are: • **Same as System**: Use the same settings as the system setting configured on **System Settings** > **System** > **VoIP Security**. • **Encryptions**: Default = RTP This setting allows selection of which parts of a media session should be protected using encryption. The default is to encrypt just the RTP stream (the speech). • **Authentication**: Default = RTP and RTCP This setting allows selection of which parts of the media session should be protected using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Currently not adjustable. • **Crypto Suites**: Default = SRTP_AES_CM_128_SHA1_80. There is also the option to select SRTP_AES_CM_128_SHA1_32.
VoIP Silence Suppression	Default = Off When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.
Enable FastStart for non-Avaya IP Phones	Default = Off A fast connection procedure. Reduces the number of messages that need to be exchanged before an audio channel is created.

Table continues…

Field	Description
Out of Band DTMF	Default = On When on, DTMF is sent as a separate signal ("Out of Band") rather than as part of the encoded voice stream ("In Band"). The "Out of Band" signaling is inserted back into the audio by the remote end. This is recommended for low bit-rate compression modes such as G.729 and G.723 where DTMF in the voice stream can become distorted. For Avaya 1600, 4600, 5600 and 9600 Series phones, the system will enforce the appropriate setting for the phone type.
Requires DTMF	Default = Off. This field is displayed when **System Settings** > **System** > **VoIP** > **Ignore DTMF Mismatch for Phones** is set to **On**. It can be used to allow direct media connections between devices despite the devices having differing DTMF setting. When **Requires DTMF** is set to **Off**, during the checks for direct media, the system ignores the DTMF checks if the call is between two VoIP phones. The two phones can be located on different systems in a Server Edition or SCN deployment. Set to **On** if the extension needs to receive DTMF signals. SIP endpoints using simultaneous login, which do not have physical extensions in the configuration, are treated by the system as not requiring DTMF. **Note:** • Direct media may still not be possible if other settings, such as codecs, NAT settings, or security settings, are mismatched. • When the system setting is set to **On**, the extension setting is ignored for contact center applications. Contact center application SIP extensions are always treated as requiring DTMF.
Local Tones	Default = Off When selected, the H.323 phones generate their own tones.
Allow Direct Media Path	Default = On This settings controls whether IP calls must be routed via the system or can be routed alternatively if possible within the network structure. • If enabled, IP calls can take routes other than through the system, removing the need for system resources such as voice compression channels. Both ends of the calls must support Direct Media and have compatible VoIP settings such as matching codec, etc. If otherwise, the call will remain routed via the system. Enabling this option may cause some vendors problems with changing the media path mid call. Disabling the extension's **Requires DTMF** setting above allows it to attempt direct media even if the other phone has differing DTMF settings. • If disabled, the call is routed via the system. In that case, RTP relay support may still allow calls between devices using the same audio codec to not require a voice compression channel.

Table continues…

Field	Description
Reserve License	Default = None. Each Avaya IP phones requires an Avaya IP Endpoint license. Each non-Avaya IP phones requires an 3rd Party IP Endpoint license. Normally these licenses are issued in the order that devices register. This option allows this extension to be pre-licensed before the device has registered. This helps prevent a previously licensed phone becoming unlicensed following a system restart if unlicensed devices are also present. The options are: • **Reserve Avaya IP Endpoint License** • **Reserve 3rd Party IP Endpoint License** • **Both** • **None** Note that when WebLM licensing is enabled, this field is automatically set to **Reserve Avaya IP Endpoint License.** The **None** option is not available.

Related links

Add Extension on page 152

SIP Extension VOIP

Navigation: **Call Management** > **Extensions** > **Edit Extension** > **SIP VoIP**

These settings are shown for SIP IP extensions.

These settings can only be edited offline. Changes to these settings require a reboot of the system.

Field	Description
IP Address	Default = 0.0.0.0 The IP address of the phone. The default setting accepts connection from any address. If an address is entered, registration is only accepted from a device with that address.

Table continues…

Field	Description
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. The available codecs in default preference order are: **G.711 A-Law**, **G.711 ULAW**, **G.729** and **G.723.1**. Note that the default order for G.711 codecs will vary to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition it is supported on Primary Server, Secondary Serverand Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo. The codecs available to be used are set through the **System Codec** list (**System | System Codec**). The options are: • **System Default**: This is the default setting. When selected, the codec list below show matches the codecs set in the system wide **Default Selection** list (**System | Codecs**). • **Custom**: This option allows specific configuration of the codec preferences to be different from the system **Default Selection** list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.
Fax Transport Support:	Default = Off. This option is only available if **Re-Invite Supported** is selected. When enabled, the system performs fax tone detection on calls routed via the line and, if fax tone is detected, renegotiates the call codec as configured below. The SIP line provider must support the selected fax method and Re-Invite. The system must have available VCM resources using an IP500 VCM, IP500 VCM V2 or IP500 Combo base card. For systems in a network, fax relay is supported for fax calls between the systems. The options are: • **None** Select this option if fax is not supported by the line provider. • **G.711** G.711 is used for the sending and receiving of faxes. • **T38** T38 is used for the sending and receiving of faxes. • **T38 Fallback** When you enable this option, T38 is used for sending and receiving faxes on a SIP line. If the called destination does not support T38, the system will send a re-invite to change the transport method to G.711.
TDM | IP Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the system TDM interface to the IP connection. This field is not shown on Linux based platforms.
IP | TDM Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the IP connection to the system TDM interface. This field is not shown on Linux based platforms.

Table continues…

Field	Description
DTMF Support	Default = RFC2833. This setting is used to select the method by which DTMF key presses are signalled to the remote end. The supported options are **In Band**, **RFC2833** or **Info**.
3rd Party Auto Answer	Default = None. This setting applies to 3rd party standard SIP extensions. The options are: • **RFC 5373**: Add an RFC 5373 auto answer header to the INVITE. • **answer-after**: Add answer-after header. • **device auto answers**: IP Office relies on the phone to auto answer calls.
Media Security	Default = Same as System. These settings control whether SRTP is used for this extension and the settings used for the SRTP. The options are: • **Same as System**: Matches the system setting at **System Settings** > **System** > **VoIP Security**. • **Disabled**: Media security is not required. All media sessions (audio, video, and data) will be enforced to use RTP only. • **Preferred**: Media security is preferred. Attempt to use secure media first and if unsuccessful, fall back to non-secure media. • **Enforced**: Media security is required. All media sessions (audio, video, and data) will be enforced to use SRTP only. **Warning:** Selecting **Enforced** on a line or extension that does not support media security will result in media setup failures.
Advanced Media Security Options	Not displayed if **Media Security** is set to **Disabled**. The options are: • **Same as System**: Use the same settings as the system setting configured on **System Settings** > **System** > **VoIP Security**. • **Encryptions**: Default = RTP This setting allows selection of which parts of a media session should be protected using encryption. The default is to encrypt just the RTP stream (the speech). • **Authentication**: Default = RTP and RTCP This setting allows selection of which parts of the media session should be protected using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Currently not adjustable. • **Crypto Suites**: Default = SRTP_AES_CM_128_SHA1_80. There is also the option to select SRTP_AES_CM_128_SHA1_32.

Table continues…

Field	Description
VoIP Silence Suppression	Default = Off When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends
Requires DTMF	Default = Off. This field is displayed when **System Settings** > **System** > **VoIP** > **Ignore DTMF Mismatch for Phones** is set to **On**. It can be used to allow direct media connections between devices despite the devices having differing DTMF setting. When **Requires DTMF** is set to **Off**, during the checks for direct media, the system ignores the DTMF checks if the call is between two VoIP phones. The two phones can be located on different systems in a Server Edition or SCN deployment. Set to **On** if the extension needs to receive DTMF signals. SIP endpoints using simultaneous login, which do not have physical extensions in the configuration, are treated by the system as not requiring DTMF. **Note:** • Direct media may still not be possible if other settings, such as codecs, NAT settings, or security settings, are mismatched. • When the system setting is set to **On**, the extension setting is ignored for contact center applications. Contact center application SIP extensions are always treated as requiring DTMF.
Local Hold Music	Default = Off. When enabled, the extension plays local music when on HOLD. If **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Advanced** > **Local Hold Music** is enabled, the extension **Local Hold Music** must be disabled to play far end music to the extension.
Allow Direct Media Path	Default = On This settings controls whether IP calls must be routed via the system or can be routed alternatively if possible within the network structure. • If enabled, IP calls can take routes other than through the system, removing the need for system resources such as voice compression channels. Both ends of the calls must support Direct Media and have compatible VoIP settings such as matching codec, etc. If otherwise, the call will remain routed via the system. Enabling this option may cause some vendors problems with changing the media path mid call. Disabling the extension's **Requires DTMF** setting above allows it to attempt direct media even if the other phone has differing DTMF settings. • If disabled, the call is routed via the system. In that case, RTP relay support may still allow calls between devices using the same audio codec to not require a voice compression channel.

Table continues…

Field	Description
RE-Invite Supported	Default = On. When enabled, **Re-Invite** can be used during a session to change the characteristics of the session. For example, when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk. Requires the ITSP to also support **Re-Invite**. This setting must be enabled for video support.
Codec Lockdown	Default = Off. Supports RFC 3264 Section 10.2 when **RE-Invite Supported** is enabled. In response to a SIP offer with a list of codecs supported, some SIP user agents supply a SDP answer that also lists multiple codecs. This means that the user agent may switch to any of those codecs during the session without further negotiation. The system does not support multiple concurrent codecs for a session, so loss of speech path will occur if the codec is changed during the session. If codec lockdown is enabled, when the system receives an SDP answer with more than one codec from the list of offered codecs, it sends an extra re-INVITE using just a single codec from the list and resubmits a new SDP offer with just the single chosen codec.
Reserve License	Default = None. Each Avaya IP phones requires an Avaya IP Endpoint license. Each non-Avaya IP phones requires an 3rd Party IP Endpoint license. Normally these licenses are issued in the order that devices register. This option allows this extension to be pre-licensed before the device has registered. This helps prevent a previously licensed phone becoming unlicensed following a system restart if unlicensed devices are also present. The options are: • **Reserve Avaya IP Endpoint License** • **Reserve 3rd Party IP Endpoint License** • **Both** • **None** Note the following: • When WebLM licensing is enabled, this field is automatically set to **Reserve Avaya IP Endpoint License.** The **Both** and **None** options are not available. • When the **Profile** of the corresponding user is set to **Centralized User**, this field is automatically set to **Centralized Endpoint License** and cannot be changed.

Related links

Add Extension on page 152

T38 Fax

Navigation: **Call Management** > **Extensions** > **Edit Extension** > **SIP T38 Fax**

The settings are available only on IP500 V2 since it can terminate T38 fax. On the **VoIP** settings for the line type, **Fax Transport Support** must be set to **T38** or **T38 Fallback**.

These settings are mergeable.

Field	Description
Use Default Values	Default = On. If selected, all the fields are set to their default values and greyed out.
T38 Fax Version	Default = 3. During fax relay, the two gateways will negotiate to use the highest version which they both support. The options are: • **0** • **1** • **2** • **3**
Transport	Default = UDPTL (fixed). Only **UDPTL** is supported. **TCP** and **RTP** transport are not supported. For **UDPTL**, redundancy error correction is supported. Forward Error Correction (FEC) is not supported.
Redundancy Redundancy sends additional fax packets in order to increase the reliability. However increased redundancy increases the bandwidth required for the fax transport.	
Low Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for low speed V.21 T.30 fax transmissions.
High Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for V.17, V.27 and V.28 fax transmissions.
TCF Method	Default = Trans TCF. TCF = Training Check Frame.
Max Bit Rate (bps)	Default = 14400. Lower rates can be selected if the current rate is not supported by the fax equipment or is found to not be reliable.
EFlag Start Timer (msecs)	Default = 2600.
EFlag Stop Timer (msecs)	Default = 2300.
Tx Network Timeout (secs)	Default = 150.
Scan Line Fix-up	Default = On.
TFOP Enhancement	Default = On.
Disable T30 ECM	Default = Off. When selected, disabled the T.30 Error Correction Mode used for fax transmission.

Table continues…

Field	Description
Disable EFlags For First DIS	Default = Off.
Disable T30 MR Compression	Default = Off.
NSF Override	Default = Off. If selected, the NSF (Non-Standard Facility) information sent by the T38 device can be overridden using the values in the fields below. **Country Code**: Default = 0. **Vendor Code**: Default = 0.

Related links

Add Extension on page 152

IP DECT Extension

Navigation: **Call Management** > **Extensions** > **Edit Extension** > **IP DECT**

IP DECT extensions are created manually after an IP DECT line has been added to the configuration or added automatically as DECT handsets subscribe to the DECT system.

These settings can be edited online with the exception of the **Reserve License** setting. The **Reserve License** setting must be edited offline and requires a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
DECT Line ID	Use the drop-down list to select the IP DECT line from the system to the Avaya IP DECT system.
Message Waiting Lamp Indication Type	Default = On Allows selection of the message waiting indication to use with the IP DECT extension. The options are: • None • On
Reserve License	Default = None. Avaya IP phones require an Avaya IP Endpoint license in order to register with the system. Normally licenses are issued in the order that devices register. This option allows this extension to be pre-licensed before the device has registered. The options are • Reserve Avaya IP Endpoint License • None Note that when WebLM licensing is enabled, this field is automatically set to **Reserve Avaya IP Endpoint License** and cannot be changed.

The additional fields below depend on whether the IP DECT line has **Enable Provisioning** selected.

Field	Description
Enable Provisioning Not Selected	
Handset Type	Default = Unknown Correct selection of the handset type allows application of appropriate settings for the handset display and buttons. Selectable handset types are **3720**, **3725**, **3740**, **3749** or **Unknown**.
Enable Provisioning Selected	
IPEI	Default = 0 This field, if set to a value other than 0, sets the IPEI number of the handset that is able to subscribe to the DECT R4 system using this extension number. The IPEI for each DECT handset is unique.
Use Handset Configuration	Default = Off. If **Use Handset Configuration**. is selected, the handset user is able to set the phone language and date/time format. If not selected, those settings will be driven by the system or user locale settings in the system configuration.

Related links

Add Extension on page 152

Groups

Navigation: **Call Management** > **Group**

Additional configuration information

This section provides the Group field descriptions.

For additional configuration information, see Group Operation on page 618.

Main content pane

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

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

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

Group Filters

Filter	Description
Show All	List all provisioned groups on all systems.
Systems	List the groups provisioned on a specific system.
Ring Modes	List groups provisioned with specific ring modes on all systems.
Profiles	
Queuing	List groups with queuing enabled.

Related links

Call Management on page 96
Add Groups on page 167

Add Groups

Navigation: **Call Management** > **Group** > **Add/Edit Group**

Related links

Groups on page 166
Group settings on page 167
Queuing on page 171
Overflow on page 174
Fallback on page 176
Voicemail on page 179
Voice Recording on page 184
Announcements on page 185
SIP on page 188

Group settings

Navigation: **Call Management** > **Group** > **Add/Edit Group** > **Group**

Additional configuration information

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 518.

Configuration settings

The Group settings are used to define the name, extension number and basic operation of the group. It is also used to select the group members.

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

Field	Description
Name	Range = Up to 15 characters The name to identify this group. This field is case sensitive and must be unique. Names should not start with a space. Do not use punctuation characters such as #, ?, /, ^, > and ,. Voicemail uses the name to match a group and its mailbox. Changing a group's name will route its voicemail calls to a new mailbox. Note however that Voicemail Pro will treat names such as "Sales", "sales" and "SALES" as being the same.
Profile	Default = Standard Hunt Group Defines the group type. The options are: • **Standard Hunt Group**: The default group type and the standard method for creating IP Office user groups. • **XMPP Group**: Extensible Messaging and Presence Protocol (XMPP) is a communications protocol for presence status and Instant Messaging (IM). Select XMPP to enable presence information and instant messaging within a defined group of XMPP enabled one-X clients. Two users can see each other's presence and exchange instant messages only if they are members of the same XMPP group. A user can be a member of zero or more groups. **Important:** Before adding a user to an XMPP group, the user must be added to the configuration and the configuration saved. If the user is added to the group before the directory is synchronized, the user will not be visible in one-X Portal. • **Centralized Group**: Select Centralized Group for extensions that are normally handled by the core feature server (Avaya Aura Communication Manager) and are handled by the IP Office only when in survival mode due to loss of connection to the Avaya Aura® Session Manager. Calls arriving to a centralized hunt group number when the Avaya Aura Session Manager line is in-service are sent by the IP Office> to Avaya Aura Session Manager and are then processed by the core feature server according to the core feature server hunt group configuration. Calls arriving to a centralized hunt group number when the Avaya Aura Session Manager line is out-of-service are processed by the IP Office and targeted to the hunt group members as configured on the IP Office. To provide consistent operation when the Avaya Aura Session Manager line is in-service or out-of-service, the following is recommended: - The IP Office hunt group should be configured consistently with the hunt group administration at the core feature server that serves the survivable branch endpoints in normal mode. - Members included in the IP Office hunt group should be only those members that are in the local branch, even if the core feature server hunt group includes additional members from other branches (that is, centralized users).

Table continues…

Field	Description
Extension	Range = 1 to 15 digits. This sets the directory number for calls to the hunt group. • Groups for CBC and CCC should only use up to 4 digit extension numbers. • Extension numbers in the range 8897 to 9999 are reserved for use by the IP Office Delta Server.
Exclude From Directory	Default = Off When on, the user does not appear in the directory list shown by the user applications and on phones with a directory function.
Ring Mode	Default = Sequential Sets how the system determines which hunt group member to ring first and the next hunt group member to ring if unanswered. This is used in conjunction with the **User List** which list the order of group membership. The options are: • **Collective** All available phones in the **User List** phones ring simultaneously. Although DECT handsets can be programmed as members of groups and receive calls in the same manner as any other extension within that group, you must not configure DECT handsets into collective groups. • **Collective Call Waiting** This is a **Collective** hunt group as above but with hunt group call waiting also enabled (previous versions of Manager used a separate **Call Waiting On** control to select this option for a **Collective** group). When an additional call to the hunt group call is waiting to be answered, users in the group who are already on a call will receive call waiting indication. On phones with call appearance buttons, the call waiting indication takes the form of an alert on the next available call appearance button. On other phones, call waiting indication is given by a tone in the speech path (the tone is locale specific). The user's own **Call Waiting On** setting is overridden when they are using a phone with call appearances. Otherwise the user's **Call Waiting On** setting is used in conjunction with the hunt group setting. • **Sequential** Each extension is rung in order, one after the other, starting from the first extension in the list each time. • **Rotary** Each extension is rung in order, one after the other. However, the last extension used is remembered. The next call received rings the next extension in the list. • **Longest Waiting** The extension that has been unused for the longest period rings first, then the extension that has been idle second longest rings, etc. For extensions with equal idle time, 'sequential' mode is used. Where hunt group calls are being presented to a twinned extension, the longest waiting status of the user can be reset by calls answered at either their master or twinned extension.

Table continues…

Field	Description
No Answer Time (secs)	Default = System Default. Range = System Default or 6 to 99999 seconds. The number of seconds an extension rings before the call is passed to another extension in the list. This applies to all telephones in this group and also any Overflow Groups it uses. For collective hunt groups, the idea of moving to the next member when the **No Answer Time** expires does not apply, instead calls will continue ringing unless overflow or voicemail is applied.
Hold Music Source	Default = No Change. The system can support multiple music on hold sources; the **System Source** (either an internal file or the external source port or tones) plus a number of additional internal sources (3 on IP500 V2 systems, 31 on Linux systems), see System | Telephony | Tones & Music. Before reaching a hunt group, the source used is set by the system wide setting or by the Incoming Call Route that routed the call. If the system has several hold music sources available, this field allows selection of the source to associate with calls presented to this hunt group or to leave it unchanged. The new source selection will then apply even if the call is forwarded or transferred out of the hunt group unless changed again by another hunt group. If the call is routed to another system in a multi-site network, the matching source on that system is used if available. Calls overflowing from a hunt group will use the hold music source setting of the original hunt group and ignore the setting of the overflow group. Calls going to night service or out of service fallback group use the hold music source setting of the original hunt group and then, if different, the setting of the fallback group. The setting of further fallback groups from the first are ignored.
Ring Tone Override	Default = Blank If ring tones have been configured in the **System | Telephony | Ring Tones** tab, they are available in this list. Setting a ring tone override applies a unique ring tone for the hunt group. Ring tone override features are only supported on 1400 Series, 9500 Series and J100 Series (except J129) phones.
Agent's Status on No-Answer Applies To	Default = None (No status change). For call center agents, that is hunt group members with a log in code and set to forced log in, the system can change the agent's status if they do not answer a hunt group call presented to them before being automatically presented to the next available agent. • This setting defines what type of hunt group calls should trigger use of the agent's **Status on No Answer** setting. The options are **None**, **Any Call** and **External Inbound Calls Only**. • The new status is set by the agent's Status on No Answer (User | Telephony | Supervisor Settings) setting. • This action is only applied if the call is unanswered at the agent for the hunt group's **No Answer Time** or longer. It does not apply if the call is presented and, before the **No Answer Time** expires, is answered elsewhere or the caller disconnects. • This option is not used for calls ringing the agent because the agent is in another group's overflow group.

Table continues…

Field	Description
User List	This is an ordered list of the users who are members of the hunt group. For **Sequential** and **Rotary** groups it also sets the order in which group members are used for call presentation. • Repeated numbers can be used, for example 201, 202, 201, 203, etc. Each extension will ring for the number of seconds defined by the **No Answer Time** before moving to the next extension in the list, dependent on the Hunt Type chosen. • The check box next to each member indicates the status of their membership. Group calls are not presented to members who have their membership currently disabled. However, those users are still able to perform group functions such as group call pickup. • The order of the users can be changed by dragging the existing records to the required position. • To add records select **Edit**. A new menu is displayed that shows available users on the left and current group members of the right. The lists can be sorted and filtered. • Users on remote systems in a multi-site network can also be included. Groups containing remote members are automatically advertised within the network. • Before adding a user to an XMPP group, the user must be added to the configuration and the configuration saved. If the user is added to the group before the directory is synchronized, the user will not be visible in one-X Portal.

Related links

Add Groups on page 167
Configuring IP Office using the Dashboard on page 38
Configuration dashboard on page 37

Queuing

Navigation: **Call Management** > **Group** > **Add/Edit Group** > **Queuing**

Any calls waiting to be answered at a hunt group are regarded as being queued. The **Normalise Queue Length** control allows selection of whether features that are triggered by the queue length should include or exclude ringing calls. Once one call is queued, any further calls are also queued. When an available hunt group member becomes idle, the first call in the queue is presented. Calls are added to the queue until the hunt group's Queue Limit, if set, is reached.

- When the queue limit is reached, any further calls are redirected to the hunt group's voicemail if available.
- If voicemail is not available excess calls receive busy tone. An exception to this are analog trunk and T1 CAS trunk calls which will remain queued regardless of the queue limit if no alternate destination is available.
- If an existing queued call is displaced by a higher priority call, the displaced call will remain queued even if it now exceeds the queue limit.

Hunt group announcements are separate from queuing. Announcements can be used even if queuing is turned off and are applied to ringing and queued calls. See Hunt Group | Announcements.

There are several methods of displaying a hunt group queue.

- **Group Button**: On phones, with programmable buttons, the **Group** function can be assigned to monitor a specified group. The button indicates when there are calls ringing within the group and also when there are calls queued. The button can be used to answer the longest waiting call.
- **SoftConsole**: The SoftConsole applications can display queue monitors for up to 7 selected hunt groups. This requires the hunt group to have queuing enabled. These queues can be used by the SoftConsole user to answer calls.

When a hunt group member becomes available, the first call in the queue is presented to that member. If several members become available, the first call in the queue is simultaneously presented to all the free members.

Overflow Calls Calls that overflow are counted in the queue of the original hunt group from which they overflow and not that of the hunt group to which they overflow. This affects the **Queue Limit** and **Calls in Queue Threshold**.

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

Field	Description
Queuing On	Default = On
Queue Length	Default = No Limit. Range = No Limit, 1 to 99 calls. This setting can be used to limit the number of calls that can be queued. Calls exceeding this limit are passed to voicemail if available or otherwise receive busy tone. This value is affected by Normalize Queue Length setting. • If voicemail is not available excess calls receive busy tone. An exception to this is analog trunk and T1 CAS trunk calls which will remain queued regardless of the queue limit if no alternate destination is available. This is due to the limited call status signalling supported by those trunks which would otherwise create scenarios where the caller has received ringing from the local line provider and then suddenly gets busy from the system, creating the impression that the call was answered and then hung up. • If priority is being used with incoming call routes, high priority calls are place ahead of lower priority calls. If this would exceed the queue limit the limit is temporarily increased by 1. • If an existing queued call is displaced by a higher priority call, the displaced call will remain queued even if it now exceeds the queue limit.

Table continues…

Field	Description
Normalize Queue Length	Default = On. Calls both waiting to ring and ringing are regarded as being queued. This therefore affects the use of the **Queue Limit** and **Calls in Queue Alarm** thresholds. If **Normalize Queue Length** is enabled, the number of hunt group members logged in and not on DND is added to those thresholds. For example, a customer has two products that it is selling through a call center with 10 available agents; one product with a $10 margin and one with a $100 margin. Separate hunt groups with the same 10 members are created for each product. • The $100 product has a Queue Limit of 5 and Normalize Queue Length is on. The maximum number of $100 calls that can be waiting to be answered will be 15 (10 ringing/connected + 5 waiting to ring). • The $10 product has a Queue Limit of 5 and Normalize Queue Length is off. The maximum number of $10 calls that can be waiting to be answered is 5 (5 ringing/connected).
Queue Type	Default = Assign Call On Agent Answer. When queuing is being used, the call that the agent receives when they answer can be assigned in one of two ways: • **Assign Call On Agent Answer** In this mode the call answered by the hunt group member will always be the longest waiting call of the highest priority. The same call will be shown on all ringing phones in the group. At the moment of answering that may not necessarily be the same call as was shown by the call details at the start of ringing. • **Assign Call on Agent Alert** In this mode, once a call has been presented to a hunt group member, that is the call they will answer if they go off hook. This mode should be used when calls are being presented to applications which use the call details such as a fax server, CTI or TAPI.
Calls In Queue Alarm	The system can be set to send an alert to a analog specified extension when the number of calls queued for the hunt group reaches the specified threshold.
Calls In Queue Threshold	Default = Off. Range = 1 to 99. Alerting is triggered when the number of queued calls reaches this threshold. Alerting will stop only when the number of queued calls drops back below this threshold. This value is affected by **Normalize Queue Length** setting above.
Analog Extension to Notify	Default = <None>. This should be set to the extension number of a user associated with an analog extension. The intention is that this analog extension port should be connected to a loud ringer or other alerting device and so is not used for making or receiving calls. The list will only shown analog extensions that are not members of any hunt group or the queuing alarm target for any other hunt group queue. The alert does not follow user settings such as forwarding, follow me, DND, call coverage, etc or receive ICLID information.

Group Queue Controls

Group Queue Settings	
Manager	Hunt group queuing is enabled using the Queuing On option on the **Hunt Group | Queuing** tab.
Controls	The following short code features/button programming actions can be used:
SoftConsole	SoftConsole can display up to 7 hunt group queues (an eight queue is reserved for recall calls). They are configured by clicking and selecting the Queue Mode tab. For each queue alarm threshold can be set based on number of queued calls and longest queued call time. Actions can then be selected for when a queue exceeds its alarm threshold; **Automatically Restore SoftConsole**, **Ask me whether to restore SoftConsole** or **Ignore the Alarm**. Within the displayed queues, the number of queued calls is indicated and the time of the longest queued call is shown. Exceeding an alarm threshold is indicated by the queue icons changing from white to red. The longest waiting call in a queue can be answered by clicking on the adjacent button.

Related links

Add Groups on page 167

Overflow

Navigation: **Call Management** > **Group** > **Add/Edit Group** > **Overflow**

Overflow can be used to expand the list of group members who can be used to answer a call. This is done by defining an overflow group or groups. The call is still targeted to the original group and subject to that group's settings, but is now presented to available members in the overflow groups in addition to its own available members.

Overflow calls still use the settings of the original target group. The only settings of the overflow group that is used is it's **Ring Mode**. For example:

- Calls that overflow use the announcement settings of the group from which they are overflowing.
- Calls that overflow use the **Voicemail Answer Time** of the original group from which are are overflowing.
- Calls that are overflowing are included in the overflowing group's **Queue Length** and **Calls In Queue Threshold**. They are not included in those values for the hunt group to which they overflow.
- The queuing and overflow settings of the overflow groups are not used, ie. calls cannot cascade through a series of multiple overflows.

A call will overflow in the following scenarios:

- If **Queuing** is off and all members of the hunt group are busy, a call presented to the group will overflow immediately, irrespective of the **Overflow Time**.
- If **Queuing** is on and all members of the hunt group are busy, a call presented to the group will queue for up to the **Overflow Time** before overflowing.

- If **Queuing** is on but there are no members logged in or enabled, calls can be set to overflow immediately by setting the **Overflow Immediate** setting to **No Active Members**. Otherwise calls will queue until the **Overflow Time** expires.
- If no **Overflow Time** is set, a call will overflow when it has rung each available hunt group member without being answered.
- Once one call is in overflow mode, any additional calls will also overflow if the **Overflow Mode** is set to **Group** (the default).

An overflow call is presented to available group members as follows:

- Once a call overflows, it is presented to the first available member of the first overflow group listed. The **Ring Mode** of the overflow group is used to determine its first available member. However the **No Answer Time** of the original targeted group is used to determine how long the call is presented.
- When the **No Answer Time** expires, the call is presented to the next available member in the overflow group. If all available members in the overflow group have been tried, the first member in the next listed overflow group is tried.
- When the call has been presented to all available members in the overflow groups, it is presented back to the first available member in the original target group.
- While the call is being presented to members in an overflow group, the announcement and voicemail settings of the original targeted group are still applied.

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

Field	Description
Overflow Time	Default = Blank. Range = Off or 1 to 3600 seconds. For a group using queuing, the **Overflow Time** sets how long a call queues before being presented to available agents in the group's **Overflow Group List**. Note that if the call is currently ringing an agent when the timer expires, it will complete ringing for the group's **No Answer Time** before overflowing.
Overflow Mode	Default = Group. This option allows selection of whether the overflow of queued calls is determined on an individual call by call basis or is applied to all calls once any one call overflows. The options are: • **Group**: In this mode, once one call overflows all additional queued calls also overflow. • **Call**: In this mode, each individual call will follow the group's overflow settings before it overflows.

Table continues…

Field	Description
Immediate Overflow:	Default = Off. For groups which are using queueing, this setting can be used to control whether calls should overflow immediately when there are no available or active agents. The options are: • **Off**: Do not overflow immediately. Use the **Overflow Time** setting as normal. • **No Active Agents**: Overflow immediately if there are no available or active agents as defined above, regardless of the **Overflow Time** setting. - An active agent is an agent who is either busy on a call or in after call work. An available agent is one who is logged in and enabled in the hunt group but is otherwise idle. - A hunt group is automatically treated as having no available or active agents if: - The group's extension list is empty. - The group's extension list contains no enabled users. - The group's extension list contains no extensions that resolve to a logged in agent (or mobile twin in the case of a user logged out mobile twinning).
Overflow Group List	This list is used to set the group or groups that are used for overflow. Each group is used in turn, in order from the top of the list. The call is presented to each overflow group member once, using the **Ring Mode** of the overflow group. If the call remains unanswered, the next overflow group in the list is used. If the call remains unanswered at the end of the list of overflow groups, it is presented to available members of the original targeted group again and then to those in its overflow list in a repeating loop. A group can be included in the overflow list more than once if required and the same agent can be in multiple groups.

Related links

Add Groups on page 167

Fallback

Navigation: **Call Management** > **Group** > **Add/Edit Group** > **Fallback**

Fallback settings can be used to make a hunt group unavailable and to set where the hunt group's calls should be redirected at such times. Hunt groups can be manually placed In Service, Out of Service or in Night Service. Additionally using a time profile, a group can be automatically placed in Night Service when outside the Time Profile settings.

Fallback redirects a hunt group's calls when the hunt group is not available, for example outside normal working hours. It can be triggered either manually or using an associated time profile.

Group Service States:

A hunt group can be in one of three states; **In Service**, **Out of Service** or **Night Service**. When **In Service**, calls are presented as normal. In any other state, calls are redirected as below.

Call Redirection:

The following options are possible when a hunt group is either **Out of Service** or in **Night Service**.

- **Destination**: When in **Out of Service**, if an **Out of Service Destination** has been set, calls are redirected to that destination. When in **Night Service**, if a **Night Service Destination** has been set, calls are redirected to that destination.
- **Voicemail**: If no fallback destination has been set but voicemail is enabled for the group, calls are redirected to voicemail.
- **Busy Tone**: If no fallback destination has been set and voicemail is not available, busy tone is returned to calls.

Manually Controlling the Service State:

Manager and or short codes can be used to change the service state of a hunt group. The short code actions can also be assigned to programmable buttons on phones.

- The  icon is used for a hunt group manually set to **Night Service** mode.
- The  icon is used for a hunt group manually set to **Out of Service** mode.

Setting and clearing hunt group night service can be done using either manual controls or using a system time profile. The use of both methods to control the night service status of a particular hunt group is not supported. You can manually override a time profile.

Time Profile:

A **Day Service Time Profile** can be associated with the hunt group. A time profile if required, is set through **System Settings** > **Time Profiles** > **Add/Edit Time Profile**.

When outside the time profile, the hunt group is automatically placed into night service. When inside the time profile, the hunt group uses manually selected mode.

- When outside the time profile and therefore in night service, manual night service controls cannot be used to override the night service. However the hunt group can be put into out of service.
- When a hunt group is in Night Service due to a time profile, this is not indicated within Manager.
- Time profile operation does not affect hunt groups set to Out of Service.

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

Field	Description
Day Service Time Profile	Default = <None> (No automatic night service) This field allows selection of a previously created Time Profile. That profile then specifies the times at which it should use the manually selected Service Mode settings. Outside the period defined in the time profile, the hunt group behaves as if set to Night Service mode. Note that when a hunt group is in Night Service due to it associated time profile, this is not reflected by the Service Mode on this tab. Note also that the manual controls for changing a hunt group's service mode cannot be used to take a hunt group out of time profile night service.
Night Service Destination	Default = <None> (Voicemail or Busy Tone) This field sets the alternate destination for calls when this hunt group is in Night Service mode. The destination can be a group, a user, a short code, or an Auto Attendant. Select a group or user from the drop down list. Manually enter a short code or an Auto Attendant name. If left blank, calls are redirected to voicemail if available or otherwise receive busy tone.
Out of Service Fallback Group	Default = <None> (Voicemail or Busy Tone) This field sets the alternate destination for calls when this hunt group is in Out of Service mode. The destination can be a group, a user, a short code, or an Auto Attendant. Select a group or user from the drop down list. Manually enter a short code or an Auto Attendant name. For Auto Attendant names, use the format **AA:Name**. If left blank, calls are redirected to voicemail if available or otherwise receive busy tone.
Mode	Default = In Service This field is used to manually select the current service mode for the hunt group. The options are: • **In Service**: When selected the hunt group is enabled. This is the default mode. • **Night Service**: When selected, calls are redirected using the **Night Service Fallback Group** setting. This setting can also be manually controlled using the short code and button programming features Set Hunt Group Night Service and Clear Hunt Group Night Service. • **Out of Service**: When selected, calls are redirected using the **Out of Service Fallback Group** setting. This setting can also be manually controlled using the short code and button programming features Set Hunt Group Out of Service and Clear Hunt Group Out of Service.

Hunt Group Fallback Controls

The following short code features and button programming actions can be used.

Feature/Action	Short Code	Default	Button
Set Hunt Group Night Service	Yes	*20*N#	Yes — Toggles
Clear Hunt Group Night Service	Yes	*21*N#	Yes

Table continues…

Set Hunt Group Out of Service	No	No	Yes — Toggles
Clear Hunt Group Out of Service	No	No	Yes

Note that for a hunt group using a time profile, these controls only are only applied when the hunt group is within the specified time profile period. When outside its time profile, the hunt group is in night service mode and cannot be overridden.

Related links

Add Groups on page 167

Voicemail

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

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

If voicemail is available and enabled for a hunt group, it is used in the following scenarios.

- **Voicemail Answer Time**: A call goes to voicemail when this timeout is reached, regardless of any announcement, overflow, queuing or other settings. The default timeout is 45 seconds.
- **Unanswered Calls**: A call goes to voicemail when it has been presented to all the available hunt group members without being answered. If overflow is being used, this includes be presented to all the available overflow group members.
- **Night Service**: A call goes to voicemail if the hunt group is in night service with no **Night Service Fallback Group** set.
- **Out of Service**: A call goes to voicemail if the hunt group is out of service with no **Out of Service Fallback Group** set.
- **Queue Limit Reached**: If queuing is being used, it overrides use of voicemail prior to expiry of the **Voicemail Answer Time**, unless the number of queued callers exceeds the set **Queue Limit**. By default there is no set limit.
- **Automatic Call Recording**: Incoming calls to a hunt group can be automatically recorded using the settings on the Hunt Group | Voice Recording tab.

When a caller is directed to voicemail to leave a message, the system indicates the target user or hunt group mailbox.

The mailbox of the originally targeted user or hunt group is used. This applies even if the call has been forwarded to another destination. It also includes scenarios where a hunt group call overflows or is in fallback to another group.

Voicemail Pro can be used to customize which mailbox is used separately from the mailbox indicated by the system.

By default no user is configured to receive message waiting indication when a hunt group voicemail mailbox contains new messages. Message waiting indication is configured by adding a **H groupname** record to a user's **SourceNumbers** tab (User | Source Numbers).

By default, no mechanism is provided for access to specific hunt group mailboxes. Access needs to be configured using either a short code, programmable button or source number.

- **Intuity Emulation Mailbox Mode**:For systems using Intuity emulation mode mailboxes, the hunt group extension number and voicemail code can be used during normal mailbox access.
- **Avaya Branch Gateway Mailbox Mode** or **IP Office Mailbox Mode**: For this mode of mailbox access, short codes or a Voicemail Collect button are required to access the mailbox directly.

The voicemail system (Voicemail Pro only) can be instructed to automatically forward messages to the individual mailboxes of the hunt group members. The messages are not stored in the hunt group mailbox.

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

Field	Description
Voicemail On	Default = On When on, the mailbox is used by the system to answer the any calls to the group that reach the **Voicemail Answer Time**. Note that selecting off does not disable use of the group mailbox. Messages can still be forward to the mailbox and recordings can be placed in it. The mailbox can also still be accessed to collect messages. When a caller is directed to voicemail to leave a message, the system indicates the target user or hunt group mailbox. • The mailbox of the originally targeted user or hunt group is used. This applies even if the call has been forwarded to another destination. It also includes scenarios where a hunt group call overflows or is in fallback to another group. • Voicemail Pro can be used to customize which mailbox is used separately from the mailbox indicated by the system.
Voicemail Answer Time	Default = 45 seconds. Range = Off, 1 to 99999 seconds. This setting sets how long a call should be presented to a hunt group, and its overflow groups if set, before going to voicemail. When exceeded the call goes to voicemail (if available) regardless of any announcements, overflow, queuing or any other actions. If set to **Off**, voicemail is used when all available members of the hunt group have been alerted for the no answer time.

Table continues…

Field	Description
Voicemail Code	Default = Blank. Range = 0 (no code) to 15 digits. A code used by the voicemail server to validate access to this mailbox. If remote access is attempted to a mailbox that has no voicemail code set, the prompt "Remote access is not configured on this mailbox" is played. The mailbox access code can be set through IP Office Manager or through the mailbox telephone user interface (TUI). The minimum password length is: • Voicemail Pro (Manager) - 0 • Voicemail Pro (Intuity TUI) - 2 • Embedded Voicemail (Manager) - 0 • Embedded Voicemail (Intuity TUI) - 0 Codes set through the Voicemail Pro telephone user interface are restricted to valid sequences. For example, attempting to enter a code that matches the mailbox extension, repeat the same number (1111) or a sequence of numbers (1234) are not allowed. If these types of code are required they can be entered through Manager. Manager does not enforce any password requirements for the code if one is set through Manager. • **Embedded Voicemail** For Embedded Voicemail running in IP Office mailbox mode, the voicemail code is used if set. • **IP Office mode** The voicemail code is required when accessing the mailbox from a location that is not set as a trusted number in the user's Source Numbers list. • **Intuity Emulation mode** By default the voicemail code is required for all mailbox access. The first time the mailbox is accessed the user will be prompted to change the password. Also if the voicemail code setting is left blank, the caller will be prompted to set a code when they next access the mailbox. The requirement to enter the voicemail code can be removed by adding a customized user or default collect call flow, refer to the Voicemail Pro manuals for full details. • **Trusted Source Access** The voicemail code is required when accessing the mailbox from a location that is not set as a trusted number in the user's Source Numbers list. • **Call Flow Password Request** Voicemail Pro call flows containing an action where the action's PIN code set to **$** will prompt the user for their voicemail code.
Voicemail Help	Default = Off This option controls whether users retrieving messages are automatically given an additional prompt "For help at any time press 8." If switched off, users can still press 8 for help. For voicemail systems running in Intuity emulation mode, this option has no effect. On those systems the default access greeting always includes the prompt "For help at any time, press *4" (*H in the US locale).

Table continues…

Field	Description
Broadcast	Default = Off. (Voicemail Pro only). When enabled, if a voicemail message is left for the hunt group, copies of the message are forwarded to the mailboxes of the individual group members. The original message in the hunt group mailbox is deleted unless it occurred as the result of call recording. This feature is not applied to recordings created by **Voice Question** actions.
UMS Web Services	Default = Off. This option is used with Voicemail Pro. If enabled, the hunt group mailbox can be accessed using either an IMAP email client or a web browser. Note that the mailbox must have a voicemail code set in order to use either of the UMS interfaces. **UMS Web Service** licenses are required for the number of groups configured. In the License section, double-clicking on the **UMS Web Services** license display a menu that allows you to add and remove users and groups from the list of those enabled for UMS Web Services without having to open the settings of each individual user or group.
Voicemail Email:	Default = Blank (No voicemail email features) This field is used to set the user or group email address used by the voicemail server for voicemail email operation. When an address is entered, the additional Voicemail Email control below are selectable to configure the type of voicemail email service that should be provided. Use of voicemail email requires the Voicemail Pro server to have been configured to use either a local MAPI email client or an SMTP email server account. For Embedded Voicemail, voicemail email is supportedand uses the system's SMTP settings. The use of voicemail email for the sending (automatic or manual) of email messages with wav files attached should be considered with care. A one-minute message creates a 1MB .wav file. Many email systems impose limits on emails and email attachment sizes. For example the default limit on an Exchange server is 5MB.

Table continues…

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

Related links

Add Groups on page 167

Voice Recording

Navigation: **Call Management** > **Group** > **Add/Edit Group** > **Voicemail Recording**

These settings are used to activate the automatic recording of incoming calls that match the incoming call route.

Call recording requires Voicemail Pro to be installed and running. Call recording also requires available conference resources similar to a 3-way conference.

Note the following:

- Calls to and from IP devices, including those using Direct media, can be recorded.
- Calls parked or held pause recording until the unparked or taken off hold (does not apply to SIP terminals).
- Recording is stopped if:
  - User recording stops if the call is transferred to another user.
  - User account code recording stops if the call is transferred to another user.
  - Hunt group recording stops if the call is transferred to another user who is not a member of the hunt group.
  - Incoming call route recording continues for the duration of the call on the system.

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

Field	Description
Record Inbound	Default = None Select whether automatic recording of incoming calls is enabled. The options are: • **None**: Do not automatically record calls. • **On**: Record the call if possible. If not possible to record, allow the call to continue. • **Mandatory**: Record the call if possible. If not possible to record, block the call and return busy tone. • **Percentages of calls**: Record a selected percentages of the calls.
Record Time Profile	Default = <None> (Any time) Used to select a time profile during which automatic call recording of incoming calls is applied. If no profile is selected, automatic recording of incoming calls is active at all times.

Table continues…

Field	Description
Recording (Auto)	Default = Mailbox Sets the destination for automatically triggered recordings. The options are: • **Mailbox** This option sets the destination for the recording to be a selected user or hunt group mailbox. The adjacent drop down list is used to select the mailbox. • **Voice Recording Library**: This options set the destination for the recording to be a VRL folder on the voicemail server. The ContactStore application polls that folder and collects waiting recordings which it then places in its own archive. Recording is still done by the Voicemail Pro. • **Voice Recording Library Authenticated**: This option is similar to Voice Recording Library above but instructs the voicemail server to create an authenticated recording. If the file contents are changed, the file is invalidated though it can still be played. This option is not currently supported with Linux based systems.

Related links

Add Groups on page 167

Announcements

Navigation: **Call Management** > **Group** > **Add/Edit Group** > **Announcements**

Announcements are played to callers waiting to be answered. This includes callers being presented to hunt group members, ie. ringing, and callers queued for presentation.

- The system supports announcements using Voicemail Pro or Embedded Voicemail.
- If no voicemail channel is available for an announcement, the announcement is not played.
- In conjunction with Voicemail Pro, the system allows a number of voicemail channels to be reserved for announcements. See **System Settings** > **System** > **Voicemail**.
- With Voicemail Pro, the announcement can be replaced by the action specified in a Queued (1st announcement) or Still Queued (2nd announcement) start point call flow. Refer to the *Voicemail Pro Installation and Maintenance* documentation for details.
- Calls can be answered during the announcement. If it is a mandatory requirement that announcements should be heard before a call is answered, then a Voicemail Pro call flow should be used before the call is presented.

  Note:

  Call Billing and Logging

  Acall becomes connected when the first announcement is played to it. That connected state is signaled to the call provider who may start billing at that point. The call will also be recorded as answered within the SMDR output once the first announcement is played.
- If a call is rerouted to a hunt group's Night Service Group or Out of Service Fallback Group, the announcements of the new group are applied.
- If a call overflows, the announcements of the original group are still applied, not those of the overflow group.
- For announcements to be used effectively, the hunt group's **Voicemail Answer Time** must be extended or **Voicemail On** must be unselected.

Recording the Group Announcement

Voicemail Pro provides a default announcement "I'm afraid all the operators are busy but please hold and you will be transferred when somebody becomes available". This default is used for announcement 1 and announcement 2 if no specific hunt group announcement has been recorded. Embedded Voicemail does not provide any default announcement. Voicemail Lite also provides the default announcements.

The maximum length for announcements is 10 minutes. New announcements can be recorded using the following methods.

Voicemail Lite: Access the hunt group mailbox and press 3. Then press either 3 to record the 1st announcement for the hunt group or 4 to record the 2nd announcement for the hunt group.

Voicemail Pro : The method of recording announcements depends on the mailbox mode being used by the voicemail server.

- **IP Office Mailbox Mode:** Access the hunt group mailbox and press 3. Then press either 3 to record the 1st announcement for the hunt group or 4 to record the 2nd announcement for the hunt group.
- **Intuity Emulation Mailbox Mode:** There is no mechanism within the Intuity telephony user interface (TUI) to record hunt group announcements. To provide custom announcements, hunt group queued and still queued start points must be configured with Voicemail Pro with the required prompts played by a generic action.

Embedded Voicemail: Embedded Voicemail does not include any default announcement or method for recording announcements. The Record Message short code feature is provided to allow the recording of announcements. The telephone number field of short codes using this feature requires the extension number followed by either ".1" for announcement 1 or ".2" for announcement 2. For example, for extension number 300, the short codes ***91N# | Record Message | N".1"** and ***92N# | Record Message | N".2"** could be used to allow recording of the announcements by dialing ***91300#** and ***92300#**.

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

Field	Description
Announcements On	Default = Off. This setting enables or disables announcements.
Wait before 1st announcement:	Default = 10 seconds. Range = 0 to 255 seconds. This setting sets the time delay from the calls presentation, after which the first announcement should be played to the caller. If **Synchronize Calls** is selected, the actual wait may differ, see below.
Flag call as answered	Default = Off. This setting is used by the CCC and CBC applications. By default they do not regarded a call as answered until it has been answered by a person or by a Voicemail Pro action with **Flag call as answered** selected. This setting allows calls to be marked as answered once the caller has heard the first announcement.

Table continues…

Field	Description
Post announcement tone	Default = Music on hold. Following the first announcement, you can select whether the caller should hear Music on Hold, **Ringing** or **Silence** until answered or played another announcement.
2nd Announcement	Default = On. If selected, a second announcement can be played to the caller if they have still not been answered.
Wait before 2nd announcement	Default = 20 seconds. Range = 0 to 255 seconds. This setting sets the wait between the 1st and the 2nd announcement. If **Synchronize Calls** is selected, the actual wait may differ, see below.
Repeat last announcement	Default = On. If selected, the last announcement played to the caller is repeated until they are answered or hang-up.
Wait before repeat	Default = 20 seconds. Range = 0 to 255 seconds. If **Repeat last announcement** is selected, this setting sets is applied between each repeat of the last announcement. If **Synchronize Calls** is selected, this value is grayed out and set to match the **Wait before 2nd announcement** setting.
Synchronize calls	Default = Off This option can be used to restrict how many voicemail channels are required to provide the announcements. When **Synchronize** calls is off, announcement are played individually for each call. This requires a separate voicemail channel each time an announcement is played to each caller. While this ensures accurate following of the wait settings selected, it does not make efficient use of voicemail channels. When **Synchronize calls** is on, if a required announcement is already being played to another caller, further callers wait until the announcement been completed and can be restarted. In addition, when a caller has waited for the set wait period and the announcement is started, any other callers waiting for the same announcement hear it even if they have not waited for the wait period. Using this setting, the maximum number of voicemail channels ever needed is 1 or 2 depending on the number of selected announcements. **Note:** **Interaction with Voicemail Pro Queued and Still Queued Start Points** If either custom **Queued** or **Still Queued** start point call flows are being used for the announcements, when **Synchronize Calls** is enabled those call flows will support the playing of prompts only. Voicemail Pro actions such as **Speak ETA**, **Speak Position**, **Menu**, **Leave Mail**, **Transfer** and **Assisted Transfer**, etc. are not supported.

Related links

[Add Groups](#) on page 167

SIP

Navigation: **Call Management** > **Group** > **Add/Edit Group** > **SIP**

Each hunt group can be configured with its own SIP URI information. For calls received on a SIP line where any of the line's SIP URI fields are set to **Use Internal Data**, if the call is presented to the hunt group that data is taken from these settings.

This form is hidden if there are no system multi-site network lines in the configuration or no SIP lines with a URI set to **Use Internal Data**.

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

Field	Description
SIP Name:	Default = Blank on Voicemail tab/Extension number on other tabs. The value from this field is used when the From field of the SIP URI being used for a SIP call is set to **Use Internal Data**.
SIP Display Name (Alias)	Default = Blank on Voicemail tab/Name on other tabs. The value from this field is used when the Display Name field of the SIP URI being used for a SIP call is set to **Use Internal Data**.
Contact	Default = Blank on Voicemail tab/Extension number on other tabs. The value from this field is used when the Contact field of the SIP URI being used for a SIP call is set to **Use Internal Data**.
Anonymous	Default = On on Voicemail tab/Off on other tabs. If the From field in the SIP URI is set to **Use Internal Data**, selecting this option inserts **Anonymous** into that field rather than the SIP Name set above.

Related links

Add Groups on page 167

Auto Attendant

Navigation: **Call Management** > **Auto Attendant**

These settings are used for embedded voicemail provided by the IP Office control unit. This is setup by adding an Avaya Embedded Voicemail memory card to the control unit and then selecting **Embedded Voicemail** as the **Voicemail Type**.

This tab and its settings are hidden unless the system has been configured to use Embedded Voicemail on the System | Voicemail tab.

For full details on configuration and operation of Embedded Voicemail auto-attendants refer to the IP Office Embedded Voicemail Installation Manual.

Up to 40 auto-attendant services can be configured.

Embedded voicemail services include auto-attendant, callers accessing mailboxes to leave or collect messages and announcements to callers waiting to be answered.

The IP500 V2 supports 2 simultaneous Embedded Voicemail calls by default but can be licensed for up to 6. The licensed limit applies to total number of callers leaving messages, collecting messages and or using an auto attendant.

In addition to basic mailbox functionality, Embedded Voicemail can also provide auto-attendant operation. Each auto attendant can use existing time profiles to select the greeting given to callers and then provide follow on actions relating to the key presses 0 to 9, * and #.

Time Profiles:

Each auto attendant can use up to three existing time profiles, on each for Morning, Afternoon and Evening. These are used to decide which greeting is played to callers. They do not change the actions selectable by callers within the auto attendant. If the time profiles overlap or create gaps, then the order of precedence used is morning, afternoon, evening.

Greetings:

Four different greetings are used for each auto attendant. One for each time profile period. This is then always followed by the greeting for the auto-attendant actions. By default a number of system short codes are automatically created to allow the recording of these greetings from a system extension. See below.

Actions:

Separate actions can be defined for the DTMF keys 0 to 9, * and #. Actions include transfer to a specified destination, transfer to another auto-attendant transfer to a user extension specified by the caller (dial by number) and replaying the greetings.

- The **Fax** action can be used to reroute fax calls when fax tone is detected by the auto-attendant.
- The **Dial by Name** action can be used to let callers specify the transfer destination.

Short Codes:

Adding an auto attendant automatically adds a number of system short codes. These use the **Auto Attendant** short code feature. These short codes are used to provide dialing access to record the auto attendant greetings.

Four system short codes (***81XX**, ***82XX**, ***83XX** and ***84XX**) are automatically added for use with all auto attendants, for the morning, afternoon, evening and menu options greetings respectively. These use a telephone number of the form **"AA:" N"** . **Y "** where **N** is the replaced with the auto attendant number dialed and **Y** is 1, 2, 3 or 4 for the morning, afternoon, evening or menu option greeting.

- An additional short code of the form (for example) ***80XX/Auto Attendant/"AA:"N** can be added manual if internal dialed access to auto attendants is required.
- To add a short code to access a specific auto attendant, the name method should be used.
- For IP Office deployed in a Enterprise Branch environment, the short codes *800XX, *801XX…*809XX, *850XX, and *851XX are automatically created for recording a Page prompt.

Routing Calls to the Auto Attendant:

The telephone number format **AA:Name** can be used to route callers to an auto attendant. It can be used in the destination field of incoming call routes and telephone number field of short codes set to the Auto Attend feature.

Related links

Call Management on page 96
Add Auto Attendant field descriptions on page 190

Add Auto Attendant field descriptions

Navigation: **Call Management** > **Auto Attendant** > **Add Auto Attendant**

Related links

Auto Attendant on page 188
Auto Attendant on page 190
Actions on page 192

Auto Attendant

Navigation: **Call Management** > **Auto Attendant** > **Add Auto Attendant** > **Auto Attendant**

These settings are used to define the name of the auto attendant service and the time profiles that should control which auto attendant greetings are played.

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

Field	Description
Name	Range = Up to 12 characters This field sets the name for the auto-attendant service. External calls can be routed to the auto attendant by entering AA:Name in the destination field of an Incoming Call Route.
Maximum Inactivity	Default = 8 seconds; Range = 1 to 20 seconds. This field sets how long after playing the prompts the Auto Attendant should wait for a valid key press. If exceeded, the caller is either transferred to the Fallback Extension set within the Incoming Call Route used for their call or else the caller is disconnected.
Enable Local Recording	Default = On. When off, use of short codes to record auto-attendant prompts is blocked. The short codes can still be used to playback the greetings.

Table continues…

Field	Description
Direct Dial-By-Number	Default = Off. This setting affects the operation of any key presses in the auto attendant menu set to use the **Dial By Number** action. If selected, the key press for the action is included in any following digits dialed by the caller for system extension matching. For example, if 2 is set in the actions to **Dial by Number**, a caller can dial 201 for extension 201. If not selected, the key press for the action is not included in any following digits dialed by the caller for system extension matching. For example, if 2 is set in the actions to **Dial by Number**, a caller must dial 2 and then 201 for extension 201.
Dial by Name Match Order	Default = First Name/Last Name. Determines the name order used for the Embedded Voicemail Dial by Name function. The options are: • **First then Last** • **Last then First**
AA Number	This number is assigned by the system and cannot be changed. It is used in conjunction with short codes to access the auto attendant service or to record auto attendant greetings.
Morning/ Afternoon/ Evening/Menu Options	Each auto-attendant can consist of three distinct time periods, defined by associated time profiles. A greeting can be recorded for each period. The appropriate greeting is played to callers and followed by the Menu Options greeting which should list the available actions. The options are: • **Time Profile** The time profile that defines each period of auto-attendant operation. When there are overlaps or gaps between time profiles, precedence is given in the order morning, afternoon and then evening. • **Short code** These fields indicate the system short codes automatically created to allow recording of the time profile greetings and the menu options prompt. • **Recording Name**: Default = Blank. Range = Up to 31 characters. This field appears next to the short code used for manually recording auto-attendant prompts. It is only used is using pre-recorded wav files as greeting rather than manually recording greetings using the indicated short codes. If used, note that the field is case sensitive and uses the name embedded within the wav file file header rather than the actual file name. This field can be used with all systems supporting Embedded Voicemail. The utility for converting .wav files to the correct format is provided with Manager and can be launched via File | Advanced | LVM Greeting Utility. Files then need to be manually transferred to the Embedded Voicemail memory card. For full details refer to the IP Office Embedded Voicemail Installation manual.

Related links

Add Auto Attendant field descriptions on page 190

Actions

Navigation: **Call Management** > **Auto Attendant** > **Add Auto Attendant** > **Actions**

This tab defines the actions available to callers dependant on which DTMF key they press. To change an action, select the appropriate row and click **Edit**. When the key is configured as required click **OK**.

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

Field	Description
Key	The standard telephone dial pad keys, 0 to 9 plus * and #. The option **Fax** can be used for a transfer to the required fax destination and will then be triggered by fax tone detection. If left as **Not Defined**, fax calls will follow the incoming call routes fallback settings once the auto-attendant Maximum Inactivity Time set on the Auto Attendant | Auto Attendant tab is reached.
Action The following actions can be assigned to each key.	
Centrex Transfer	Used to transfer the incoming call to an external telephone number defined in the **Transfer Number** field. This option is only supported with Embedded Voicemail.
Dial by Name	Callers are asked to dial the name of the user they require and then press #. The recorded name prompts of matching users are then played back for the caller to make a selection. The name order used is set by the **Dial by Name Match Order** setting on the Auto Attendant tab. Note the name used is the user's **Full Name** if set, otherwise their **User Name** is used. Users without a recorded name prompt or set to **Exclude From Directory** are not included. For Embedded Voicemail in IP Office mode, users can record their name by accessing their mailbox and dialing *05. For Embedded Voicemail in Intuity mode, users are prompted to record their name when they access their mailbox.
Dial By Number	This option allows callers with DTMF phones to dial the extension number of the user they require. No destination is set for this option. The prompt for using this option should be included in the auto attendant Menu Options greeting. A uniform length of extension number is required for all users and hunt group numbers. The operation of this action is affected by the auto attendant's Direct Dial-by-Number setting.
Normal Transfer	Can be used with or without a **Destination** set. When the **Destination** is not set, this action behaves as a **Dial By Number** action. With the **Destination** is set, this action waits for a connection before transferring the call. Callers can hear Music on Hold. Announcements are not heard.
Not Defined	The corresponding key takes no action.

Table continues…

Field	Description
Park & Page	The Park & Page feature is supported when the system **Voicemail Type** is designated as **Embedded Voicemail** or **Voicemail Pro**. Park & Page is also supported on systems where **Modular Messaging over SIP** is configured as the central voicemail system and the local **Embedded Voicemail** provides auto attendant operation. The Park & Page feature is an option in user mailboxes where a key is configured with the Park & Page feature. When an incoming call is answered by the voicemail system and the caller dials the DTMF digit for which Park & Page is configured, the caller hears the Park & Page prompt. IP Office parks the call and sends a page to the designated extension or hunt group. When Park & Page is selected in the **Action** drop-down box, the following fields appear: • **Park Slot Prefix –** the desired Park Slot prefix number. Maximum is 8 digits. A 0-9 will be added to this prefix to form a complete Park Slot. • **Retry count –** number of page retries; the range is 0 to 5. • **Retry timeout –** provided in the format M:SS (minute:seconds). The range can be set in 15-second increments. The minimum setting is 15 seconds and the maximum setting is 5 minutes. The default setting is 15 seconds. • **Page prompt –** short code to record the page prompt or upload the recorded prompt. (Prompt can be uploaded to the SD card in the same way the AA prompts are).
Replay Menu Greeting	Replay the auto-attendant greetings again.
Transfer	Transfer the call to the selected destination. This is an unsupervised transfer, if the caller is not answered they will be handled as per a direct call to that number.
Transfer to Attendant	This action can be used to transfer calls to another existing auto attendant.
Destination	Sets the destination for the action. Destination can be a user, a hunt group or a short code. If the destination field is left blank, callers can dial the user extension number that they require. Note however that no prompt is provided for this option so it should be included in the auto attendant Menu Options greeting.

Related links

Add Auto Attendant field descriptions on page 190

Chapter 6: System Settings

Navigation: **System Settings**

Related links

System Short Codes

Navigation: **System Settings** > **Short Codes**

Additional configuration information

This section provides the Short Code field descriptions.

For additional configuration information, see Short Code Features on page 712.

Main content pane

The **Short Codes** main content pane lists provisioned short codes. The contents of the list depends on the filter option selected. Click the icons beside a short code to edit or delete.

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

Click **Add/Edit Short Code** to open the Add Short Code window where you can provision a user. When you click **Add/Edit Short Code**, you are prompted to specify if the short code will be a global object or specific to a server.

Related links

System Settings on page 194
Add Short Code on page 195

Add Short Code

Navigation: **System Settings** > **Short Codes** > **Add/Edit Short Code**

These settings are used to create System Short Codes. System short codes can be dialed by all system users. However the system short code is ignored if the user dialing matches a user or user rights short code.

Warning:

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

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

Field	Description
Code	The dialing digits used to trigger the short code. Maximum length 31 characters.
Feature	Select the action to be performed by the short code.
Telephone Number	The number dialed by the short code or parameters for the short code feature. This field can contain numbers and characters. For example, it can contain Voicemail Pro start point names, user names, hunt group names and telephone numbers (including those with special characters). Maximum length 31 characters. The majority of North-American telephony services use 'en-bloc' dialing, ie. they expect to receive all the routing digits for a call as a single simultaneous set of digits. Therefore the use of a ; is recommended at the end of all dialing short codes that use an **N**. This is also recommended for all dialing where secondary dial tone short codes are being used.

Table continues…

Field	Description
Line Group ID	Default = 0. For short codes that result in the dialing of a number, that is short codes with a **Dial** feature, this field is used to enter the initially routing destination of the call. The drop down can be used to select the following from the displayed list: • **Outgoing Group ID**: The Outgoing Group ID's current setup within the system configuration are listed. If an **Outgoing Group ID** is selected, the call will be routed to the first available line or channel within that group. • **ARS**: The ARS records currently configured in the system are listed. If an ARS record is selected, the call will be routed by the setting within that ARS record. Refer to ARS Overview.
Locale	Default = Blank. For short codes that route calls to voicemail, this field can be used to set the prompts locale that should be used if available on the voicemail server.
Force Account Code	Default = Off. For short codes that result in the dialing of a number, this field trigger the user being prompted to enter a valid account code before the call is allowed to continue.
Force Authorization Code	Default = Off. This option is only shown on systems where authorization codes have been enabled. If selected, then for short codes that result in the dialing of a number, the user is required to enter a valid authorization code in order to continue the call.

Related links

System Short Codes on page 194

Incoming Call Route

Navigation: **System Settings** > **Incoming Call Route**

Main content pane

The **Incoming Call Route** main content pane lists provisioned incoming call routes. Click the icons beside a route to edit or delete.

Click **Add/Edit Incoming Call Route** to add an incoming call route. When you click **Add/Edit Incoming Call Route**, you are prompted to specify a server where the route will be configured.

Click **MSN Configuration** to populate the incoming call route table with MSN or DID numbers. When you click **MSN Configuration**, you are prompted to specify a server.

Related links

System Settings on page 194
Add Incoming Call Route on page 197
Incoming Call Route MSN Configuration on page 206

Add Incoming Call Route

Navigation: **System Settings** > **Incoming Call Route** > **Add/Edit Incoming Call Route**

Incoming call routes are used to determine the destination of voice and data calls received by the system. On systems where a large number incoming call routes need to be setup for DID numbers, the MSN/DID Configuration tool can be used.

Calls received on IP, S0 and QSIG trunks do not use incoming call routes. Routing for these is based on incoming number received as if dialed on-switch. Line short codes on those trunks can be used to modify the incoming digits.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Determining which incoming call route is used is based on the call matching a number of possible criteria. In order of highest priority first, the criteria, which if set must be matched by the call in order for the call to use that route are:

1. The **Bearer Capability** indicated, if any, with the call. For example whether the call is a voice, data or video call.
2. The **Incoming Group ID** of the trunk or trunk channel on which the call was received.
3. The **Incoming Number** received with the call.
4. The **Incoming Sub Address** received with the call.
5. The **Incoming CLI** of the caller.

Multiple Matches

If there is a match between more than one incoming call route record, the one added to the configuration first is used.

Incoming Call Route Destinations

Each incoming route can include a fallback destination for when the primary destination is busy. It can also include a time profile which control when the primary destination is used. Outside the time profile calls are redirected to a night service destination. Multiple time profiles can be associated with an incoming call route. Each time profile used has its own destination and fallback destination specified.

Incoming Call Routing Examples

Example 1

For this example, the customer has subscribes to receive two 2-digit DID numbers. They want calls on one routed to a Sales hunt group and calls on the other to a Services hunt group. Other calls should use the normal default route to hunt group Main. The following incoming call routes were added to the configuration to achieve this:

Line Group	Incoming Number	Destination
0	77	Sales

Table continues…

0	88	Services
0	blank	Main

Note that the incoming numbers could have been entered as the full dialed number, for example 7325551177 and 7325551188 respectively. The result would still remain the same as incoming number matching is done from right-to-left.

Line Group	Incoming Number	Destination
0	7325551177	Sales
0	7325551188	Services
0	blank	Main

Example 2

In the example below the incoming number digits 77 are received. The incoming call route records 677 and 77 have the same number of matching digit place and no non-matching places so both a potential matches. In this scenario the system will use the incoming call route with the Incoming Number specified for matching.

Line Group	Incoming Number	Destination
0	677	Support
0	77	Sales
0	7	Services
0	blank	Main

Example 3

In the following example, the 677 record is used as the match for 77 as it has more matching digits than the 7 record and no non-matching digits.

Line Group	Incoming Number	Destination
0	677	Support
0	7	Services
0	blank	Main

Example 4

In this example the digits 777 are received. The 677 record had a non-matching digit, so it is not a match. The 7 record is used as it has one matching digit and no non-matching digits.

Line Group	Incoming Number	Destination
0	677	Support
0	7	Services
0	blank	Main

Example 5

In this example the digits 77 are received. Both the additional incoming call routes are potential matches. In this case the route with the shorter Incoming Number specified for matching is used and the call is routed to **Services**.

Line Group	Incoming Number	Destination
0	98XXX	Support
0	8XXX	Services
0	blank	Main

Example 6

In this example two incoming call routes have been added, one for incoming number 6XXX and one for incoming number 8XXX. In this case, any three digit incoming numbers will potential match both routes. When this occurs, potential match that was added to the system configuration first is used. If 4 or more digits were received then an exact matching or non-matching would occur.

Line Group	Incoming Number	Destination
0	6XXX	Support
0	8XXX	Services
0	blank	Main

Related links

Incoming Call Route on page 196
Incoming Call Route General Settings on page 199
Incoming Call Route Voice Recording on page 203
Incoming Call Route Destinations on page 204

Incoming Call Route General Settings

Navigation: **System Settings** > **Incoming Call Route** > **Add/Edit Incoming Call Route**

Additional configuration information

For additional information on the **Tag** setting, see Call Tagging on page 588.

Incoming call routes are used to match call received with destinations. Routes can be based on the incoming line group, the type of call, incoming digits or the caller's ICLID. If a range of MSN/DID numbers has been issued, this form can be populated using the MSN Configuration tool. In Manager, see **Tools** > **MSN Configuration**.

Default Blank Call Routes

By default the configuration contains two incoming calls routes; one set for **Any Voice** calls (including analog modem) and one for **Any Data** calls. While the destination of these default routes can be changed, it is strongly recommended that the default routes are not deleted.

- Deleting the default call routes, may cause busy tone to be returned to any incoming external call that does not match any incoming call route.
- Setting any route to a blank destination field, may cause the incoming number to be checked against system short codes for a match. This may lead to the call being rerouted off-switch.

Calls received on IP, S0 and QSIG trunks do not use incoming call routes. Routing for these is based on incoming number received as if dialed on-switch. Line short codes on those trunks can be used to modify the incoming digits.

If there is no matching incoming call route for a call, matching is attempted against system short codes and finally against voicemail nodes before the call is dropped.

SIP Calls

For SIP calls, the following fields are used for call matching:

- **Line Group ID** This field is matched against the **Incoming Group** settings of the SIP URI (Line | SIP URI). This must be an exact match.
- **Incoming Number** This field can be used to match the called details (TO) in the SIP header of incoming calls. It can contain a number, SIP URI or Tel URI. For SIP URI's the domain part of the URI is removed before matching by incoming call routing occurs. For example, for the SIP URI mysip@example.com , only the user part of the URI, ie. mysip, is used for matching.

The Call Routing Method setting of the SIP line can be used to select whether the value used for incoming number matching is taken from the **To Header** or the **Request URI** information provided with incoming calls on that line.

Incoming CLI This field can be used to match the calling details (FROM) in the SDP header of incoming SIP calls. It can contain a number, SIP URI, Tel URI or IP address received with SIP calls. For all types of incoming CLI except IP addresses a partial record can be used to achieve the match, records being read from left to right. For IP addresses only full record matching is supported.

Configuration Settings

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

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Incoming Call Matching Fields:

The following fields are used to determine if the Incoming Call Route is a potential match for the incoming call. By default the fields are used for matching in the order shown starting with **Bearer Capability**.

Field	Description
Bearer Capability	Default = Any Voice The type of call selected from the list of standard bearer capabilities. The options are: • **Any** • **Any Voice** • **Any Data** • **Speech** • **Audio 3K1** • **Data 56K** • **Data 64K** • **Data V110** • **Video**
Line Group ID	Default = 0. Range = 0 to 99999. Matches against the Incoming Line Group to which the trunk receiving the call belongs. For Server Edition systems, the default value **0** is not allowed. You must change the default value and enter the unique **Line Group ID** for the line.
Incoming Number	Default = Blank (Match any unspecified) Matches to the digits presented by the line provider. A blank record matches all calls that do not match other records. By default this is a right-to-left matching. The options are: • *** = Incoming CLI Matching Takes Precedence** • **– = Left-to-Right Exact Length Matching** Using a **-** in front of the number causes a left-to-right match. When left-to-right matching is used, the number match must be the same length. For example -96XXX will match a DID of 96000 but not 9600 or 960000. • **X = Single Digit Wildcard** Use **X**'s to enter a single digit wild card character. For example **91XXXXXXXX** will only match DID numbers of at least 10 digits and starting with 91, **-91XXXXXXXX** would only match numbers of exactly 10 digits starting with 91. Other wildcard such as **N**, **n** and **?** cannot be used. Where the incoming number potentially matches two incoming call routes with X wildcards and the number of incoming number digits is shorter than the number of wildcards, the one with the shorter overall **Incoming Number** specified for matching is used. • **i = ISDN Calling Party Number 'National'** The **i** character does not affect the incoming number matching. It is used for Outgoing Caller ID Matching, see notes below.
Incoming Sub Address	Default = Blank (Match all) Matches any sub address component sent with the incoming call. If this field is left blank, it matches all calls.

Table continues…

Field	Description
Incoming CLI	Default = Blank (Match all) Enter a number to match the caller's ICLID provided with the call. This field is matched left-to-right. The number options are: • Full telephone number. • Partial telephone number, for example just the area code. • **!** : Matches calls where the ICLID was withheld. • **?** : for number unavailable. • Blank for all.

Call Setting Fields:

For calls routed using this Incoming Call Route, the settings of the following fields are applied to the call regardless of the destination.

Field	Description
Locale	Default = Blank (Use system setting) This option specifies the language prompts, if available, that voicemail should use for the call if it is directed to voicemail.
Priority	Default = 1-Low. Range = 1-Low to 3-High. This setting allows incoming calls to be assigned a priority. Other calls such as internal calls are assigned priority **1-Low** In situations where calls are queued, high priority calls are placed before calls of a lower priority. This has a number of effects: • Mixing calls of different priority is not recommended for destinations where Voicemail Pro is being used to provided queue ETA and queue position messages to callers since those values will no longer be accurate when a higher priority call is placed into the queue. Note also that Voicemail Pro will not allow a value already announced to an existing caller to increase. • If the addition of a higher priority call causes the queue length to exceed the hunt group's Queue Length Limit, the limit is temporarily raised by 1. This means that calls already queued are not rerouted by the addition of a higher priority call into the queue. A timer can be used to increase the priority of queued calls, see the setting **System | Telephony | Telephony | Call Priority Promotion TimeSystem Settings** > **System** > **Telephony** > **Call Priority Promotion Time**. The current priority of a call can be changed through the use of the **p** short code character in a short code used to transfer the call.
Tag	Default = Blank (No tag). Allows a text tag to be associated with calls routed by this incoming call route. This tag is displayed with the call within applications and on phone displays.

Table continues…

Field	Description
Hold Music Source	Default = System source. The system can support several music on hold sources. See **System Settings** > **System** > **Telephony** > **Tones and Music**. If the system has several hold music sources available, this field allows selection of the source to associate with calls routed by this incoming call route. The new source selection will then apply even if the call is forwarded or transferred away from the Incoming Call Route destination. If the call is routed to another system in a multi-site network, the matching source on that system is used if available. The hold music source associated with a call can also be changed by a hunt group's Hold Music Source setting.
Ring Tone Override	Default = Blank If ring tones have been configured in **System Settings** > **System** > **Telephony** > **Ring Tones**, they are available in this list. Setting a ring tone override applies a unique ring tone for the incoming call route.

Outgoing Caller ID Matching

In cases where a particular Incoming Number is routed to a specific individual user, the system will attempt to use that Incoming Number as the user's caller ID when they make outgoing calls if no other number is specified. This requires that the Incoming Number is a full number suitable for user as outgoing caller ID and acceptable to the line provider.

When this is the case, the character **i** can also be added to the Incoming Number field. This character does not affect the incoming call routing. However when the same Incoming Number is used for an outgoing caller ID, the calling party number plan is set to ISDN and the type is set to National. This option may be required by some network providers.

For internal calls being forwarded or twinned, if multiple incoming call route entries match the extension number used as caller ID, the first entry created is used. This entry should start with a "-" character (meaning fixed length) and provide the full national number. These entries do not support wildcards. If additional entries are required for incoming call routing, they should be created after the entry required for reverse lookup.

Related links

Add Incoming Call Route on page 197

Incoming Call Route Voice Recording

Navigation: **System Settings** > **Incoming Call Route** > **Add/Edit Incoming Call Route**

These settings are used to activate the automatic recording of incoming calls that match the incoming call route.

Call recording requires Voicemail Pro to be installed and running. Call recording also requires available conference resources similar to a 3-way conference.

Note the following:

- Calls to and from IP devices, including those using Direct media, can be recorded.
- Calls parked or held pause recording until the unparked or taken off hold (does not apply to SIP terminals).

- Recording is stopped if:
  - User recording stops if the call is transferred to another user.
  - User account code recording stops if the call is transferred to another user.
  - Hunt group recording stops if the call is transferred to another user who is not a member of the hunt group.
  - Incoming call route recording continues for the duration of the call on the system.

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

Field	Description
Record Inbound	Default = None Select whether automatic recording of incoming calls is enabled. The options are: • **None**: Do not automatically record calls. • **On**: Record the call if possible. If not possible to record, allow the call to continue. • **Mandatory**: Record the call if possible. If not possible to record, block the call and return busy tone. • **Percentages of calls**: Record a selected percentages of the calls.
Record Time Profile	Default = <None> (Any time) Used to select a time profile during which automatic call recording of incoming calls is applied. If no profile is selected, automatic recording of incoming calls is active at all times.
Recording (Auto)	Default = Mailbox Sets the destination for automatically triggered recordings. The options are: • **Mailbox** This option sets the destination for the recording to be a selected user or hunt group mailbox. The adjacent drop down list is used to select the mailbox. • **Voice Recording Library**: This options set the destination for the recording to be a VRL folder on the voicemail server. The ContactStore application polls that folder and collects waiting recordings which it then places in its own archive. Recording is still done by the Voicemail Pro. • **Voice Recording Library Authenticated**: This option is similar to Voice Recording Library above but instructs the voicemail server to create an authenticated recording. If the file contents are changed, the file is invalidated though it can still be played. This option is not currently supported with Linux based systems.

Related links

Add Incoming Call Route on page 197

Incoming Call Route Destinations

Navigation: **System Settings** > **Incoming Call Route** > **Add/Edit Incoming Call Route**

The system allows multiple time profiles to be associated with an incoming call route. For each time profile, a separate Destination and Fallback Extension can be specified.

When multiple records are added, they are resolved from the bottom up. The record used will be the first one, working from the bottom of the list upwards, that is currently 'true', ie. the current day and time or date and time match those specified by the Time Profile. If no match occurs the Default Value options are used.

Once a match is found, the system does not use any other destination set even if the intended Destination and Fallback Extension destinations are busy or not available.

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

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Description
Time Profile	This column is used to specify the time profiles used by the incoming call routes. It displays a drop-down list of existing time profiles from which a selection can be made. To remove an existing entry, select it by clicking on the button on the left of the row, then right-click on the row and select **Delete**. The **Default Value** entry is fixed and is used if no match to a time profile below occurs.
Destination	Default = Blank Either enter the destination manually or select the destination for the call from the drop-down list. The dr box which contains all available extensions, users, groups, RAS services and voicemail. System short codes and dialing numbers can be entered manually. Once the incoming call is matched the call is passed to that destination. The following options appear in the drop-down list: • **Voicemail** allows remote mailbox access with voicemail. Callers are asked to enter the extension ID of the mailbox required and then the mailbox access code. • Local user names. • Local hunt groups names. • **AA**: **Name** directs calls to an Embedded Voicemail auto-attendant services. In addition to short codes, extension and external numbers, the following options can be also be entered manually: • **VM:Name** Directs calls to the matching start point in Voicemail Pro. • A **.** matches the Incoming Number field. This can be used even when X wildcards are being used in the Incoming Number field. • A **#** matches all **X** wildcards in the **Incoming Number** field. For example, if the Incoming Number was -91XXXXXXXXXX, the **Destination** of # would match XXXXXXXXXX. • Text and number strings entered here are passed through to system short codes, for example to direct calls into a conference. Note that not all short code features are supported. • If necessary, quote marks can be used to stop characters in the destination string being interpreted as special characters.

Table continues…

Field	Description
Fallback Extension	Default = Blank (No fallback) Defines an alternate destination which should be used when the current destination, set in the **Destination** field cannot be obtained. For example if the primary destination is a hunt group returning busy and without queuing or voicemail.

Related links

Add Incoming Call Route on page 197

Incoming Call Route MSN Configuration

Navigation: **System Settings** > **Incoming Call Route** > **MSN Configuration**

Used to populate the **Incoming Call Route** table with a range of MSN or DID numbers.

Setting	Description
MSN/DID	The first number in the set of MSN numbers for which you have subscribed. **Note:** If you require to find an exact match between the MSN numbers and the destination numbers, enter a minus (-) sign before the first MSN number.
Destination	Where incoming calls with matching digits should be routed. The drop-down list contains the extensions and groups on the system.
Line Group ID	Specifies the incoming line group ID of the trunks to which the DID routing is applied.
Presentation Digits	Set to match the number of digits from the MSN/DID number that the central office exchange will actually present to the system.
Range	How many MSN or DID number routes to create in sequence using the selected MSN/DID and Destination as start points. Only routing to user extensions is supported when creating a range of records.

Related links

Incoming Call Route on page 196

Time Profiles

Navigation: **System Settings** > **Time Profiles**

Additional configuration information

This section provides the **Time Profiles** field descriptions.

For additional configuration information, see:

- Configuring Time Profiles on page 516

- the button action Time Profile on page 927

Main content pane

The **Time Profiles** main content pane lists provisioned time profiles. The contents of the list depends upon the filter options selected. Click the icons beside a profile to edit or delete.

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

Click **Add/Edit Time Profile** to add a time profile. When you click **Add/Edit Time Profile**, you are prompted to add to time profile as a common object or on a specific server.

Related links

System Settings on page 194
Add Time Profile on page 207

Add Time Profile

Navigation: **System Settings** > **Time Profiles** > **Add/Edit Time Profile**

Additional configuration information

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 518.

Configuration settings

When configuring a time profile, you must enter the **Name** on the **Time Profile** page and then click **Add/Edit Time Profile Entry** to open the Recurrence pattern window.

For a time profile with multiple records, for example a week pattern and some calendar records, the profile is valid when any entry is valid. For Server Edition, this type of configuration record can be saved as a template and new records created from a template.

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

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Description
Name	Range = Up to 15 characters This name is used to select the time profile from within other tabs.

Table continues…

Field	Description
Manual Override	Default = Off. You can manually override a time profile. The override settings allow you to mix timed and manual settings. The options are: • **Active Until Next Timed Inactive**: Use for time profiles with multiple intervals. Select to make the current timed interval active until the next inactive interval. • **Inactive Until Next Timed Active**: Use for time profiles with multiple intervals. Select to make the current active timed interval inactive until the next active interval. • **Latch Active**: Set the time profile to active. Timed inactive periods are overridden and remain active. The setting is retained over a reboot. • **Latch Inactive**: Set the time profile to inactive. Timed active periods are overridden and remain active. The setting is retained over a reboot.
Time Entry List This list shows the current periods during which the time profile is active. Clicking on an existing entry will display the existing settings and allows them to be edited if required. To remove an entry, selecting it and then click on **Remove** or right-click and select **Delete**.	
Recurrence Pattern (Weekly Time Pattern)	When a new time entry is required, click **Add Recurring** and then enter the settings for the entry using the fields displayed. Alternately right-click and select **Add Recurring Time Entry**. This type of entry specific a time period and the days on which it occurs, for example 9:00 - 12:00, Monday to Friday. A time entry cannot span over two days. For example you cannot have a time profile starting at 18:00 and ending 8:00. If this time period is required two Time Entries should be created - one starting at 18:00 and ending 11:59, the other starting at 00:00 and ending 8:00. • **Start Time** The time at which the time period starts. • **End Time** The time at which the time period ends. Note that the endtime is at the end of the minute, for example 11:00 is interpreted as 11:00:59, not 11:00:00. • **Days of Week** The days of the week to which the time period applies.
Recurrence Pattern (Calendar Date)	When a new calendar date entry is required, click **Add Date** and then enter the settings required. Alternately right-click and select **Add Calendar Time Entry**. Calendar records can be set for up to the end of the next calendar year. • **Start Time** The time at which the time period starts. • **End Time** The time at which the time period ends. • **Year** Select either the current year or the next calendar year. • **Date** To select or de-select a particular day, double-click on the date. Selected days are shown with a dark gray background. Click and drag the cursor to select or de-select a range of days.

Related links

Time Profiles on page 206

Directory

Navigation: **System Settings** > **System Directory**

Additional configuration information

This section provides the Directory field descriptions.

For additional configuration information, see Centralized System Directory on page 521.

Main content pane

The **System Directory** main content pane lists provisioned directory records. Click the icons beside a record to edit or delete.

Click **Add/Edit Directory Entry** to open the Add Directory window and configure a directory record.

Related links

System Settings on page 194
Add Directory Entry on page 209

Add Directory Entry

Navigation: **System Settings** > **System Directory** > **Add/Edit Directory Entry**

Additional configuration information

For additional configuration information, see Centralized System Directory on page 521.

Configuration settings

Use these settings to create directory records that are stored in the system's configuration. Directory records can also be manually imported from a CSV file. The system can also use Directory Services to automatically import directory records from an LDAP server at regular intervals.

A system can also automatically import directory records from another system. Automatically imported records are used as part of the system directory but are not part of the editable configuration. Automatically imported records cannot override manually entered records.

For a Server Edition network, these settings can only be configured at the network level and they are stored in the configuration of the Primary Server. All other systems in the network are configured to share the directory settings of the Primary Server through their Manager settings at **System | Directory Services | HTTP**.

Directory Special Characters

The following characters are supported in directory records. They are supported in both system configuration records and in imported records.

- **? = Any Digit** Directory records containing a **?** are only used for name matching against the dialed or received digits on outgoing or incoming. They are not included in the directory of numbers to dial available to users through their phones or applications. The wildcard can be used in any position but typically would be used at the end of the number.

In the following example, any calls where the dialed or received number is 10 digits long and starts 732555 will have the display name Homdel associated with them.

- **Name**: Holmdel
- **Number**: 9732555????

- **(and) brackets = Optional Digits** These brackets are frequently used to enclose an optional portion of a number, typically the area code. Only one pair of brackets are supported in a number. Records containing digits inside ( ) brackets are used for both name matching or user dialling. When used for name matching, the dialed or received digits are compared to the directory number with and without the ( ) enclosed digits. When used for dialling from a phone or application directory, the full string is dialed with the ( ) brackets removed.

  The following example is a local number. When dialed by users they are likely to dial just the local number. However on incoming calls, for the CLI the telephony provider includes the full area code. Using the ( ) to enclose the area code digits, it is possible for the single directory record to be used for both incoming and outgoing calls.

  - **Name**: Raj Garden
  - **Number**: 9(01707)373386

- **Space and - Characters** Directory records can also contain spaces and - characters. These will be ignored during name matching and dialing from the directory.

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

Field	Description
Index	Range = 000 to 999 or None. This value is used with system speed dials dialed from M and T-Series phones. The value can be changed but each value can only be applied to one directory record at any time. Setting the value to **None** makes the speed dial inaccessible from M and T-Series phones, however it may still be accessible from the directory functions of other phone types and applications. The Speed Dial short code feature can be used to create short codes to dial the number stored with a specific index value.
Name	Enter the text, to be used to identify the number. Names should not begin with numbers.
Number	Enter the number to be matched with the above name. Any brackets or - characters used in the number string are ignored. The directory number match is done on reading from the left-hand side of the number string. The number is processed against the applicable user and system short codes. Note that if the system has been configured to use an external dialing prefix, that prefix should be added to directory numbers.

Related links

Directory on page 209

Locations

Navigation: **System Settings** > **Locations**

Additional configuration information

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

For additional configuration information, see:

- Emergency Call on page 526
- Configuring Call Access Control on page 531
- PreventingToll Bypass on page 569
- Configuring Location Based Extension Resiliancy on page 666

Main content pane

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

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

Click **Add/Edit Location** to open the Location page where you can provision a location. When you click **Add/Edit Location**, you are prompted to specify if the location will be a global object or specific to a server.

Related links

System Settings on page 194
Add Location on page 211
Address on page 213

Add Location

Navigation: **System Settings** > **Locations** > **Add/Edit Location** > **Locations**

Configuring locations allows you to specify named locations for groups of phones, IP Office systems, or IP Trunks. The IP Office system must also be assigned a location. Multiple systems in an SCN or Server Edition group of systems may reside in the same location. In an SCN environment, locations must be configured at the top level and therefore, all systems must be configured with the same settings, except when the emergency ARS needs to be set at the system level.

Once locations have been defined, extensions can be allocated to them in the extension configuration. IP phones can be identified by the IP address that they register from. Each location can have only one subnet defined, but phones outside that subnet can be explicitly assigned that location.

The Location page allows you to define a physical location and associate a network address with a physical location. Locations can then be allocated to extensions. Linking a location to an extension, enables the physical location of a phone to be identified when an emergency call is made.

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

Field	Description
Location Name	Default = Blank. A meaningful location name, clearly identifying the geographical position of the phone.
Location ID	Default = Based on existing configured locations, the next incremental value is assigned. This field is read only.
Subnet Address	Default = Blank. The IP address associated with this location. The subnet where this IP address resides must be unique across all configured locations. Overlapping IP address ranges between locations will cause extensions to use the first match found which may not be the correct location.
Subnet Mask	Default = Blank. The subnet mask for this IP address.
Emergency ARS	Default = None. The ARS (Alternate Route Selection) that defines how emergency calls from this location are routed. The drop down list contains all available ARS entries using the format **ARS Route ID: Route Name**. For example **50: Main**.
Parent Location for CAC	Default = None. The options are: • **None** The default setting. • **Cloud** The parent location is an internet address external to the IP Office network. When set to **Cloud**, the **Call Admission Control** (CAC) settings are disabled. Calls to this location from other configured locations are counted as external, yet no CAC limits are applied to the location itself.
Call Admission Control The CAC settings, when not unlimited, restrict the number of calls into and out of the location, The following Call Admission Control settings can be configured.	
Total Maximum Calls	Default = Unlimited. Range = 1 - 99, Unlimited. Limit of all calls to or from other configured locations and the cloud.
External Maximum Calls	Default = Unlimited. Range = 1 - 99, Unlimited. Limit of calls to or from the cloud in this location.
Internal Maximum Calls	Default = Unlimited. Range = 1 - 99, Unlimited. Limit of calls to or from other configured locations in this location.
Time Settings The display of location based time is only supported on 1100, 1200, 1600 and 9600 Series (96x0 and 96x1) phones and D100, E129 and B179 telephones.	
Time Zone	Default = Same as System Select a time zone from the list.

Table continues…

Field	Description
Local Time Offset from UTC	Default is based on the currently selected time zone. Set the time for this location by entering the offset from UTC.
Automatic DST	Default is based on the currently selected time zone. When set to On, the system automatically corrects for daylight saving time (DST) changes as configured in the **Clock Forward/Back Settings** below.
Clock Forward/ Back Settings **(Start Date — End Date (DST Offset))**	Default is based on the currently selected time zone. Click **Edit** to configure the time and date for DST clock corrections. In the Daylight Time Settings window, you can configure the following information: • **DST Offset**: the number of hours to shift for DST. • **Clock Forward/Back**: Select **Go Forward** to set the date when the clock will move forward. Select **Go Backwards** to set the date when the clock will move backward. • **Local Time To Go Forward**: The time of day to move the clock forward or backward. • **Date for Clock Forward/Back**: Set the year, month and day for moving the clock forwards and backwards. Once you click **OK**, the forward and back dates, plus the DST offset, are displayed using the format **(Start Date — End Date (DST Offset))**.
Fallback System	Default = No override. The drop down list contains all configured IP Office Lines and the associated IP Office system. The group of extensions associated with this location can fallback to the alternate system selected.

Related links

Locations on page 210

Address

Navigation: **System Settings** > **Locations** > **Add/Edit Location** > **Address**

Enter address information to define a specific location. The address fields are based on the standards RFC 4119 and RFC 5139.

If **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Advanced** > **Send Location Info** is set to **Emergency Calls** then the location defined here is sent as part of the INVITE message when emergency calls are made.

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

Field	Description	Example
Country Code	The country is identified by the two letter ISO 3166 code.	US

Table continues…

Field	Description	Example
A1	National subdivisions (state, region, province, prefecture).	New York
A2	County, parish, gun (JP), district (IN).	King's County
A3	City, township, shi (JP).	New York
A4	City division, borough, city district, ward, chou (JP).	Manhattan
A5	Neighborhood, block.	Morningside Heights
A6	Street.	Broadway
RD	Primary road or street	Broadway
RDSEC	Trailing street suffix.	SW
RDBR	Road branch.	Lane 7
RDSUBBR	Road sub-branch.	Alley 8
PRD	Leading street direction.	N
POD	Trailing street suffix.	NE
STS	Street suffix.	Avenue, Platz, Street
PRM	Road pre-modifier.	Old
POM	Road post-modifier.	Extended
HNO	House number, numeric part only.	123
HNS	House number suffix.	A, 1/2
LMK	Landmark or vanity address.	Low Library
BLD	Building (structure).	Hope Theatre
LOC	Additional location information.	Room 543
PLC	Place type.	Office
FLR	Floor.	5
UNIT	Unit (apartment, suite).	12a
ROOM	Room.	450F
SEAT	Seat (desk, cubicle, workstation).	WS 181
NAM	Name (residence, business, or office occupant).	Joe's Barbershop
ADDCODE	Additional Code	13203000003
PCN	Postal community name.	Leonia
PC	Postal code.	10027-0401
POBOX	Post office box (P.O. box)	U40

Related links

Locations on page 210

Licenses

Navigation: **System Settings** > **Licenses**

Additional configuration information

This section provides the Licenses field descriptions.

For additional configuration information, see the following.

- Applying Licenses on page 485.
- Converting from Nodal Licensing to Centralized Licensing on page 498
- Migrating ADI Licenses to PLDS on page 499
- “Licenses” in *Avaya IP Office™ Platform Solution Description*.

Main content pane

Clicking **System Settings** > **Licenses** opens the Systems page with a list of all IP Office systems. Click on the three bar menu icon to the right of a system to view the licensing information for that system.

Related links

System Settings on page 194
License on page 215
Remote Server on page 217
Configuring IP Office using the Dashboard on page 38
Configuration dashboard on page 37

License

Navigation: **System Settings** > **Licenses** > **Server Menu** > **Manage Licenses**

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

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>License Mode</td><td>Identifies the status of the system licenses. The two license configuration types are nodal and WebLM. Nodal licenses are licenses that are present on the system. WebLM licenses means licenses obtained from the WebLM server.

The possible states are:
• Normal Mode Normal nodal licensing mode. In this mode, WebLM is not configured and only nodal licensing is allowed.
• Server Error This mode occurs when transitioning to WebLM licensing. WebLM has been configured but the server is not available.
• Configuration Error This mode occurs when transitioning to WebLM licensing. WebLM has been configured and the server is available, but there are not enough licenses available to license all of the configured features. Only nodal licenses are valid on Standard mode IP500 V2 systems.
• WebLM Normal Mode The system is fully licensed. WebLM has been configured and there are enough licenses available to license all of the configured features.
• WebLM Error Mode Action is required to correct the License Mode. Refer to the License Status column and the Error List section at the bottom of the screen to determine why the system is in License Error Mode. A 30-day grace period provides access to the capacities and features of the installed license when the system is in License Error Mode.
• WebLM Restricted Mode When the system is in License Error Mode, if the problem is not resolved with the 30-day grace period, the system will enter License Restricted Mode. When in this mode, configuration changes are blocked, except for fixing the licensing errors. If a feature license cannot be acquired from the WebLM server, the feature will not function.
<table>
<tr><th>Type</th><th>Mode</th><th>WebLM Configured</th><th>Virtual License and Grace Period (30 days)</th></tr>
<tr><td>Nodal</td><td>Normal</td><td>No</td><td>No</td></tr>
<tr><td>WebLM</td><td>Server Error</td><td>Yes</td><td>No</td></tr>
<tr><td>WebLM</td><td>Configuration Error</td><td>Yes</td><td>No</td></tr>
<tr><td>WebLM</td><td>Normal</td><td>Yes</td><td>No</td></tr>
<tr><td>WebLM</td><td>Error</td><td>Yes</td><td>Yes</td></tr>
<tr><td>WebLM</td><td>Restricted</td><td>Yes</td><td>No</td></tr>
</table></td></tr>
<tr><td>Licensed Version</td><td>Indicates the software version the system is currently licensed for.</td></tr>
<tr><td>PLDS Host ID</td><td>The ID used when generating PLDS nodal license files.

Not used with WebLM licensing. WebLM licensing uses the host ID of the WebLM server.</td></tr>
<tr><td>PLDS File Status</td><td>If a PLDS nodal license file is loaded, this field indicates if the file is valid or not.</td></tr>
<tr><td>Select Licensing</td><td>Indicates that the system has a valid Select license.</td></tr>
<tr><td>Feature</td><td>Identifies the licenses installed on the system.</td></tr>
</table>

Table continues…

Name	Description
Key	This is the license key string supplied. It is a unique value based on the feature being licensed and the either the system's **Dongle Serial Number** or **System Identification** depending on the type of system. Not applicable when using PLDS or WebLM licensing. This field is not displayed if there are no ADI licenses.
Instance	For information only. Some licenses enable a number of port, channels or users. When that is the case, the number of such is indicated here. Multiple licenses for the same feature are usually cumulative.
Status	For information only. This field indicates the current validation status of the license key. • **Unknown** This status is shown for licenses that have just been added to the configuration shown in Manager. Once the configuration has been sent back to the system and then reloaded, the status will change to one of those below. • **Valid**: The license is valid. • **Invalid**: The license was not recognized. It did not match the PLDS host ID. • **Dormant**: The license is valid but is conditional on some other pre-requisite licenses. • **Obsolete**: The license is valid but is one no longer used by the level of software running on the system.
Expiry Date	For information only. Trial licenses can be set to expire within a set period from their issue. The expiry date is shown here.
Source	The source of the license file. The options are: • **ADI Nodal**: ADI licenses added locally to the system. This may appear on upgraded systems. • **PLDS Nodal**: PLDS licenses added locally to the system. • **WebLM**: Licenses obtained from the WebLM server. • **Virtual**: Licenses created by the system. This may appear on upgraded systems. • **Virtual Grace**: Licenses created by the system while in WebLM error mode.

Additional Configuration Information

Click **PLDS License** > **Send To IP Office** > **OK** to open the **Select PLDS License File** dialog from where you can upload a PLDS license to IP Office. You can browse to a location on your system and select a file to upload.

Select an existing license and click **PLDS License** > **Delete From IP Office** > **OK** to delete the selected license.

Related links

Licenses on page 215

Remote Server

Navigation: **System Settings** > **Licenses** > **Server Menu** > **Remote Server**

This tab is used for:

- IP500 V2 systems in a Enterprise Branch deployments which are using WebLM licensing
- Server Edition systems to specify which method of centralized licensing is used.

Offline Editing

The **Reserved Licenses** setting can be edited online. The remaining settings must be edited offline. Changes to these settings require a reboot of the system.

To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

The following field two fields control which source the system uses for its licenses. The field shown depends on the type of system:

Field	Description
Licence Source	Default = WebLM. This field is available on Server Edition systems. All systems in the network must use the same source for licensing. The options are: • **WebLM**: Licenses are obtained from the WebLM service. The PLDS license file is uploaded to the WebLM service. All servers in the network make license reservation requests to the WebLM service. On Server Edition systems, a **Deploy** button appears when you select **WebLM** as **License Source**. Click the **Deploy** button to browse and select a license file to deploy. • **Local / Primary Server**: The PLDS license file is uploaded to the IP Office service, not WebLM. Depending on the particular license, some are obtained by reservation requests to the primary server, others are obtained from the server's own license file.
Enable Remote Server	Default = Off. This field is available on non-Server Edition IP500 V2 systems. The options are: • If disabled, the system is licensed locally by uploading a license file to the system. • If enabled, the system uses licenses requested from a remote WebLM server. This option is only supported for systems in a branch enterprise supported via Avaya System Manager.

The additional fields displayed depend on the license source selection above:

Local/Primary Server Licensed Server Settings

Field	Description
License Server IP Address	Default = 127.0.0.1 on Primary. On Secondary and expansion systems, the default is the Primary IP address. This field is available when the **Licence Source** is set to **Local Primary Server**. This field contains the IP address of the Server Edition Primary server.

WebLM Licensed Primary Server Settings

Field	Description
Domain Name (URL)	Default = Blank for IP500 V2 systems and for Server Edition Primary hosted deployments. For Server Edition, the IP address of the Primary Server. • For Enterprise Branch deployments, the domain name or IP address of the WebLM server or the domain name of System Manager if the system is under System Manager control. • For Server Edition deployments, the domain name or IP address of the Primary Server. • For Server Edition hosted deployments, the domain name of the WebLM server. The format can be the FQDN or the IP address prefixed with https://.
Path	Default = WebLM/LicenseServer. The path on the web server of the WebLM resource.
Port Number	Default = 52233. The port number of the WebLM server.
WebLM Client ID	An ID based on MAC address of the system. This is a read only field used by the WebLM server to identify the system.
WebLM Node ID	An ID based on MAC address and hostname of the system. This is a read only field used by the WebLM server to identify the system.

WebLM Licensed Server (non-Primary) Settings

Field	Description
Enable proxy via Primary IP Office line	Default = On. Available on Server Edition Secondary and Expansion systems. • Enables retrieval of licenses from the WebLM server through the IP Office Line connection to the Server Edition Primary server. • If the check box is cleared, the WebLM request is done directly to the WebLM server. Note that this field is not available if the node is not configured as a WebSocket client to the Server Edition Primary server.
Primary IP Address	Default = The IP address of the Server Edition Primary server. Available on Server Edition Secondary and Expansion systems when **Enable proxy via Primary IP Office line** is enabled
WebLM Client ID	An ID based on MAC address of the system. This is a read only field used by the WebLM server to identify the system.
WebLM Node ID	An ID based on MAC address and hostname of the system. This is a read only field used by the WebLM server to identify the system.

Reserved Licenses

These fields are used to reserve licenses from the license server, WebLM or, if using nodal licensing, the Primary server. There are two types of reservation field; manual and automatic.

- Manual fields can be used to set the number of licenses that the server should request from those available on the primary/WebLM server.
- Automatic fields are set to match other aspects of the server configuration, for example the number of configured power users. Note that these values may not change until after the configuration is saved and then reloaded.

WebLM Reserved Licenses — Manual	Primary Server	Secondary Server	Expansion (Linux)	Expansion (IP500 V2)
SIP Trunk Sessions	Yes	Yes	Yes	Yes
SM Trunk Sessions	Yes	Yes	Yes	Yes
Voicemail Pro Ports	Yes	Yes	-	-
VMPro Recordings Administrators	Yes	Yes	-	-
VMPro TTS Professional	Yes	Yes	-	-
Wave Users	-	-	-	Yes
CTI Link Pro	Yes	Yes	Yes	Yes
UMS Web Services	Yes	Yes	Yes	Yes
MAC Softphones	Yes	Yes	Yes	Yes
Avaya Contact Center Select	Yes	Yes	-	-
Third Party Recorder	Yes	Yes	-	-
VM Media Manager	Yes	Yes	Yes	-
Customer Service Supervisor	Yes	Yes	Yes	Yes
Customer Service Agent	Yes	Yes	Yes	Yes

Nodal Reserved Licenses — Manual	Primary Server	Secondary Server	Expansion (Linux)	Expansion (IP500 V2)
SIP Trunk Sessions	Yes	Yes	Yes	Yes

WebLM/Nodal Reserved Licenses — Automatic	Primary Server	Secondary Server	Expansion (Linux)	Expansion (IP500 V2)
Server Edition	Yes	Yes	Yes	Yes
Avaya IP Endpoints	Yes	Yes	Yes	Yes
3rd Party IP Endpoints	Yes	Yes	Yes	Yes
Receptionist	Yes	Yes	Yes	Yes

Table continues…

Office Worker	Yes	Yes	Yes	Yes
Power User	Yes	Yes	Yes	Yes
Avaya Softphone	Yes	Yes	Yes	Yes
Web Collaboration	Yes	Yes	Yes	Yes
Universal PRI Additional Channels	-	-	-	Yes
IPSec Tunneling	-	-	-	Yes

Related links

Licenses on page 215

System

Navigation: **System Settings** > **System**

The System page lists all the systems in the IP Office Server Edition solution. There is one System record for each system being managed. Click on the icon to the right of the record to open the system configuration pages.

Related links

System Settings on page 194
System on page 221
Voicemail on page 228
System Events on page 236
SMTP on page 244
DNS on page 245
SMDR on page 245
LAN1 on page 246
LAN2 on page 262
VoIP on page 263
VoIP Security on page 265
Access Control Lists on page 267
Directory Services on page 267
Telephony on page 272
Contact Center on page 285
Avaya Cloud Services on page 286

System

Navigation: **System Settings** > **System** > **System**

Additional configuration information

For additional information on time settings, see System Date and Time on page 515.

Configuration settings

These settings can be edited online with the exception of **Locale** and **Favor RIP Routes over Static Routes**. These settings must be edited offline and requires a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Name	Default: = System MAC Address. A name to identify this system. This is typically used to identify the configuration by the location or customer's company name. Some features such as Gatekeeper require the system to have a name. This field is case sensitive and within any network of systems must be unique. Do not use <, >, |, \0, :, *, ?, . or /.
Contact Information	Default = Blank. This field is only be edited by service user with administrator rights. If Contact Information is entered, it will set the system under 'special control'. If the contact information is set using a standalone version of Manager, warnings that "This configuration is under special control" are given when the configuration is opened again. This can be used to warn other users of Manager that the system is being monitored for some specific reason and provide them with contact details of the person doing that monitoring.
Locale	Sets default telephony and language settings based on the selection. It also sets various external line settings and so must be set correctly to ensure correct operation of the system. See *Avaya IP Office™ Platform Locale Settings*. For individual users, the system settings can be overridden through their own locale setting Select **Call Management** > **Users** > **Add/Edit Users** > **User** > **Local**.
Location	Default = None. Specify a location to associate the system with a physical location. Associating a system with a location allows emergency services to identify the source of an emergency call. The drop down list contains all locations that have been defined in the Location page.
Customize Locale Settings The **Customize** locale matches the Saudi Arabia locale but with the following additional controls shown below. For other locales, these are set on .	
Tone Plan	Default = Tone Plan 1 The tone plan control tones and ringing patterns. The options are: • **Tone Plan 1**: United States. • **Tone Plan 2**: United Kingdom. • **Tone Plan 3**: France. • **Tone Plan 4**: Germany. • **Tone Plan 5**: Spain.

Table continues…

Field	Description
CLI Type	Used to set the CLI detection used for incoming analogue trunks. The options are: • **DTMF** • **FSK V23** • **FSK BELL202**
Device ID	Server Edition Only. Displays the value set for **Device ID** on the System | System Events | Configuration tab. If an SSL VPN is configured, Avaya recommends that the Device ID match an SSL VPN service Account Name. Each SSL VPN service account name has an associated SSL VPN tunnel IP address. Having the displayed Device ID match an SSL VPN service account name helps identify a particular SSL VPN tunnel IP address to use for remotely managing IP Office.
TFTP Server IP Address	Default = 0.0.0.0 *(Disabled. On Server Edition Systems, the default on Secondary and Expansion servers is the Primary Server address.)* If the **Phone File Server Type** below is set to **Custom**, this address is included as the TFTP file server address sent in the system's DHCP response to phones. The address 255.255.255.255 can be used to broadcast for the first available TFTP server on the network. Manager can act as a TFTP server and provides files from its configured binaries directory. This requires the application setting **File | Preferences | Preferences | Enable BootP and TFTP Servers** to be enabled. On IP500 V2 systems, the LAN1 IP Address can be entered to specify the system's own memory card memory card as the TFTP file source. This requires the security setting **Security Settings | Unsecured Interfaces | Applications Controls | TFTP Directory Read** to be enabled.
HTTP Server IP Address	Default = 0.0.0.0 (Disabled). This address, if set, is used in a number of scenarios: • **DHCP Responses:** If the **Phone File Server Type** below is set to **Custom**, this address is included as the HTTP file server address sent in the system's DHCP response to phones. • **HTTP Redirection:** If **HTTP Redirection** below is enabled, 96x1 H.323 phone binary file requests sent to the system are redirected to this address. • **H175 Phones/Vantage Phones:** Phone firmware file requests sent to the system from these types of phone always redirected to this address.

Table continues…

Field	Description
Phone File Server Type	Default = Memory Card (IP500 V2)/Disk (Linux system). For IP phones (H.323 and SIP) using the system as their DHCP server, the DHCP response can include the address of a file server from which the phone should request files. The setting of this field controls which address is used in the DHCP response. The options are: • **Custom**: The DHCP response the system provides to phones contains the addresses set in the **TFTP Server IP Address** and **HTTP Server IP Address** fields. • **Disk**: *(Linux systems only)* The system will respond to file requests from phones using files on its own hard disk. The DHCP response the system provides to phones contains its own LAN address as the TFTP and HTTP file server address. • **Memory Card**: *(IP500 V2 only)* The system will respond to file requests from phones using files on its own memory card. The DHCP response the system provides to phones contains its own LAN address as the TFTP and HTTP file server address. This is supported for up to 50 IP phones total. • **Manager**: *(IP500 V2 only)* The system will forward any H.323 phone file request to the configured **Manager PC IP Address** set below. The DHCP response the system provides to phones contains the system's LAN address as the HTTP file server address. - HTTP-TFTP Relay is support when using Manager as the TFTP server (not supported by Linux based systems). This is done by setting the **TFTP Server IP Address** to the address of the Manager PC and the **HTTP Server IP Address** to the control unit IP address. This method is supported for up to 5 IP phones total.
HTTP Redirection	Default = Off. This setting allows 96x1 phones to use the system as the file server when requesting their upgrade and settings files but have the requests for their large firmware files redirected to the address set by the **HTTP Server IP Address** field. This field is available when the **Phone File Server Type** is set to **Memory Card** or **Disk**. • H175 and Vantage phone firmware requests are always redirected to the **HTTPS Server IP Address** regardless of this and the **Phone File Server Type** settings.
Manager PC IP Address	Default = 0.0.0.0 (Broadcast). This address is used when the **Phone File Server Type** is set to **Manager**.
Avaya HTTP Clients Only	Default = Off. When selected, the system only responds to HTTP requests from sources it identifies as another system, an Avaya phone or application.
Enable SoftPhone HTTP Provisioning	Default = Off. This option must be enabled if the IP Office Video Softphone is being supported.

Table continues…

Field	Description
Use Preferred Phone Ports	Default = Off When selected, the system allows users to configure firewalls to block ports 80 and 443 if alternate mechanism for administration is provided. Phones can use either port 411 or 8411 if supported. Legacy phones that still require 80 and 443 can continue to use those ports through IP Office HTTP server. Where possible, HTTP requests from phones received on ports 80 and 443 must result in the phone proceed to use 8411/411, However, files continue to be served on the ports 80 and 443 to allow functionality of non-compliant phones. Configuration files served to phones, that are not behind an SBC, defines 8411 for HTTP and additionally 411 for TLS if the phone supports it and the phone is remote, or incoming request is already secure. When cleared, phones can continue to connect through all the four ports. DHCP provided HTTP IP addresses are served.
Favor RIP Routes over Static Routes	Default = Off RIP can be enabled on the system LAN1 and LAN2 interfaces and on specific Services. When this setting is on, the RIP route to a destination overrides any static route to the same destination in the system's IP Routes, regardless of the RIP route's metric. The only exception is RIP routes with a metric of 16 which are always ignored. **Note:** If a previously learnt RIP route fails, the system applies a metric of 16 five minutes after the failure. When off, any RIP route to a destination for which a static route has been configured is ignored. This option is not supported on Linux based systems.
Automatic Backup	Default = On. This command is available with IP500 V2 systems. When selected, as part of its daily backup process, the system automatically copies the folders and files from the **System SD** card's `/primary` folder to its `/backup` folder. Any matching files and folders already present in the **/backup** folder are overwritten.
Provider	Default = Not visible. This field is visible only if the system has been branded by addition of a special license for a specific equipment provider. The branding is fixed, that is it remains even if the license is subsequently removed. The number shown is a unique reference to the particular equipment provider for whom the system has been branded. When branded, the equipment provider's name is displayed on idle phone displays and other provider related features are enabled.

Table continues…

Field	Description
Time Setting Config Source	Time and date settings are only shown for IP500 V2 based systems. The time and date for Linux based servers are set through the server's **Platform View** menus (**Settings | System | Date and Time**). For IP500 V2 systems, the time is either set manually, obtained using Time protocol (RFC868) requests or obtained using Network Time Protocol (RFC958) request. This field is used to select which method is used and to apply ancillary settings based on the selected method. • **None:** The system to not make any time requests. The system time and date can be be set and changed using by a user with system phone rights (see System Phone Features on page 639). However, the system still automatically apply daylight saving changes to the manually set time. • **Voicemail Pro/Manager:** Both the Voicemail Pro service and the Manager program can act as RFC868 Time servers for the system. Use of other RFC868 server sources is not supported. They provide both the UTC time value and the local time as set on the PC. The system makes a request to the specified address following a reboot and every 8 hours afterwards. This option should not be used with a Unified Communication Module as in that scenario the voicemail server is being hosted by and getting its time from the IP Office. • **SNTP:** Use a list of SNTP servers to obtain the UTC time. The records in the list are used one at a time in order until there is a response. The system makes a request to the specified addresses following a reboot and every hour afterwards.
Time Settings — Voicemail Pro/Manager These settings are shown for IP500 V2 based systems where the **Time Setting Config Source** has been set to **Voicemail Pro/Manager**.	
IP Address	Default = 0.0.0.0 (Broadcast) The address to which the RFC868 request is sent. 0.0.0.0 means default operation. In this mode, following a reboot the control unit makes time requests on its LAN interfaces. It first makes a request to the IP address set and, if it receives no reply, then makes a broadcast request. If you are running Manager when the voicemail server starts, voicemail does not start as a time server. It is therefore recommended that you have no copy of Manager running when you start or restart the voicemail server. Manager can be disabled from acting as a RFC868 time server by deselecting the **Enable Time Server** option (File | Preferences | Edit | Preferences).
Time Offset	Default = 00:00. This value is not normally set as any time changes, including daylight saving changes, that occur on the PC will be matched by the system.
Time Settings — None/SNTP These settings are shown for IP500 V2 based systems where the **Time Setting Config Source** has been set to **None** or **SNTP**.	

Table continues…

Field	Description
Time Server Address	Default = Blank Displayed when the **Time Setting Config Source** is set to **SNTP**. Enter a list of IP addresses, host names, or fully qualified domain names (FQDN) for the SNTP servers. Separate each record with a space. The use of broadcast addresses is not supported. The list is used in order of the records until a response is received.
Time Zone	Select a time zone from the list. This sets the default time offset and DST to match the chosen time zone.
Local Time Offset from UTC	Default is based on the currently selected time zone. This setting is used to set the local time difference from the UTC time value provided by an SNTP server. For example, if the system is 5 hours behind UTC, this field should be configured with **-05:00** to make the adjustment. The time offset can be adjusted in 15 minute increments. If also using the daylight time saving settings below, use this offset to set the non-DST local time.
Automatic DST	Default is based on the currently selected time zone. When set to On, the system automatically corrects for daylight saving time (DST) changes as configured in the **Clock Forward/Back Settings** below.
Clock Forward/ Back Settings **(Start Date — End Date (DST Offset))**	Default is based on the currently selected time zone. Click **Edit** to configure the time and date for DST clock corrections. In the Daylight Time Settings window, you can configure the following information: • **DST Offset**: the number of hours to shift for DST. • **Clock Forward/Back**: Select **Go Forward** to set the date when the clock will move forward. Select **Go Backwards** to set the date when the clock will move backward. • **Local Time To Go Forward**: The time of day to move the clock forward or backward. • **Date for Clock Forward/Back**: Set the year, month and day for moving the clock forwards and backwards. Once you click **OK**, the forward and back dates, plus the DST offset, are displayed using the format **(Start Date — End Date (DST Offset))**.
File Writer IP Address	Default = 0.0.0.0 (Disabled) This field set the address of the PC allowed to send files to the System SD card installed in the system using HTTP or TFTP methods other than embedded file management. • On non-Linux based systems, this field sets the address of the PC allowed to send files to the memory card using HTTP or TFTP methods other than embedded file management. • For Linux based systems it is applied to non-embedded file management access to the `/opt/ipoffice` folder on the server. An address of 255.255.255.255 allows access from any address. If embedded file management is used, this address is overwritten by the address of the PC using embedded file management (unless set to 255.255.255.255).

Table continues…

Field	Description
Dongle Serial Number	Displayed for pre-Release 10.0 IP500 V2 systems using ADI licensing only. For system's using PLDS licensing, see the **PLDS Host ID** (**License | License**). This field is for information only. It shows the serial number of the feature key dongle against which the system last validated its licenses. **Local** is shown for a serial port, Smart Card or System SD feature key plugged directly into the control unit. **Remote** is shown for a parallel or USB feature key connected to a feature Key Server PC. The serial number is printed on the System SD card and prefixed with **FK**.
System Identification	Displayed for Linux based systems. This field is for information only. This is the unique system reference that is used to validate licenses issued for this particular system. For a physical server this is a unique value based on the server hardware. For a virtual server this value is based on several factors including the LAN1 and LAN2 IP addresses, the host name and the time zone. If any of those are changed, the System ID changes and any existing licenses become invalid.
AVPP IP Address	Default = 0.0.0.0 (Disabled) Where Avaya 3600 Series SpectraLink wireless handsets are being used with the system, this field is used to specify the IP address of the Avaya Voice Priority Processor (AVPP)

Related links

System on page 221

Voicemail

Navigation: **System Settings** > **System** > **Voicemail**

Additional configuration information

For information on configuration Voicemail Pro resiliency, see Server Edition Resiliency on page 653.

Configuration settings

The following settings are used to set the system's voicemail server type and location. Fields are enabled or grayed out as appropriate to the selected voicemail type. Refer to the appropriate voicemail installation manual for full details.

These settings can be edited online with the exception of **Voicemail Type** and **Voicemail IP Address**. These settings must be edited offline and requires a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Voicemail Type	Defaults: Non-Server Edition = Embedded Voicemail, Primary Server = Voicemail Pro, Server Edition Secondary Server with independent voicemail or for Outbound Contact Express = Voicemail Pro, Server Edition Others: Centralized Voicemail. Sets the type of voicemail system being used. The options are: • **None**: No voicemail operation. • **Analogue Trunk MWI**: Select this option to support receiving a message waiting indicator (MWI) signal from analog trunks terminating on the ATM4U-V2 card. MWI is a telephone feature that turns on a visual indicator on a telephone when there are recorded messages. • **Avaya Aura Messaging**: Select this option if you want to configure the system to use Avaya Aura Messaging as the central voicemail system. If you choose this option, you are still able to use Embedded Voicemail or Voicemail Pro at each branch to provide auto-attendant operation and announcements for waiting calls. When selected, access to voicemail is routed via an SM line to the numbers specified in the **AAM Number** field. The optional **AAM PSTN Number** can be configured for use when the SM Line is not in service. For a setup where the voicemail box numbers configured on Avaya Aura Messaging or Modular Messaging are same as the caller's DID, the short code to route the PSTN call should be such that the caller-id is withheld ("W" in the telephone-number of the shortcode). This is to make sure that, during rainy day - the voicemail system does not automatically go to the voicemail box of the caller based on the caller id. • **Call Pilot**: Select this option if you want to configure the system to use CallPilot over SIP as the central voicemail system. If you choose this option, you are still able to use **Embedded Voicemail** or Voicemail Pro at each branch to provide auto-attendant operation and announcements for waiting calls. When selected, access to voicemail is routed via SM line to the numbers specified in the **CallPilot Number** field. **Note:** The **CallPilot PSTN Number** field and associated **Enable Voicemail Instructions Using DTMF** check box are not supported. IP Office cannot access the CallPilot system over the PSTN when the Session Manager line is down. **Note:** Users can access their CallPilot voicemail by dialing the Voicemail Collect short code. Access to CallPilot voicemail from Auto Attendant cannot be enabled by setting a Normal Transfer action to point to the Voicemail Collect short code. If desired, it can be enabled by setting a Normal Transfer action to point to the CallPilot number. • **Centralized Voicemail** Select this option when using a Voicemail Pro system installed and licensed on another system in a multi-site network. The outgoing line group of the H.323 IP line connection to the system with the Voicemail Pro should be entered as the **Voicemail Destination**. In a Server Edition network this option is

Table continues…

Field	Description
	used on the Secondary Server and expansion systems to indicate that they use the Primary Server for as their voicemail server. • **Distributed Voicemail**: This option can be used when additional Voicemail Pro voicemail servers are installed in a multi-site network and configured to exchange messages with the central voicemail server using email. This option is used if this system should use one of the additional servers for its voicemail services rather than the central sever. When selected, the **Voicemail Destination** field is used for the outgoing H.323 IP line to the central system and the **Voicemail IP Address** is used for the IP address of the distributed voicemail server the system should use. This option is not supported by Server Edition systems. • **Embedded Voicemail** On systems with an Avaya memory card, select this option to run Embedded Voicemail which stores messages and prompts on the memory card. It also supports internal Auto Attendant configuration through the system configuration. The IP500 V2 supports 2 simultaneous Embedded Voicemail calls by default but can be licensed for up to 6. The licensed limit applies to total number of callers leaving messages, collecting messages and or using an auto attendant. This option is not supported by Server Edition systems. • **Group Voicemail** This option is used to support third-party voicemail systems attached by extension ports in the group specified as the **Voicemail Destination**. This option is not supported by Server Edition systems. • **Modular Messaging over SIP** Select this option if you want to configure the system to use Modular Messaging over SIP as the central voicemail system. If you choose this option, you are still able to use Embedded Voicemail or Voicemail Pro at each branch to provide auto-attendant operation and announcements for waiting calls. When selected, access to voicemail is routed via an SM line to the numbers specified in the **MM Number** field. The optional **MM PSTN Number** can be configured for use when the SM Line is not in service. **Note:** Embedded Voicemail and Voicemail Pro are available only in Distributed branch deployments. They are not available when there are centralized users configured for a IP Officee system that is deployed as either a Centralized branch or a mixed branch. The Embedded Voicemail option uses the Essential Edition and the Additional Voicemail Ports licenses to control the number of ports that can be used. These licenses are also used to control the number of ports on systems where Embedded Voicemail is configured to provide local Auto Attendant and announcements while the selected option for voicemail is one of the central voicemail options through the Session Manager (i.e. Avaya Aura Messaging, Modular Messaging, or CallPilot). Similarly, the Voicemail Pro option uses the Preferred Edition and the Incremental Voicemail Ports licenses to control the number of ports that can be used. These licenses are also used to control the number of ports on systems where Voicemail

Table continues…

Field	Description
	Pro is configured to provide local Call Flow processing while the selected option for voicemail is Avaya Aura Messaging, Modular Messaging or CallPilot. - When the system routes a call to the voicemail server it indicates the locale for which matching prompts should be provided if available. The locale sent to the voicemail server by the system is determined as show below. If the required set of prompts is not available, the voicemail will fallback to another appropriate language and finally to English (refer to the appropriate voicemail installation manual for details). - **Short Code Locale**: The short code locale, if set, is used if the call is routed to voicemail using the short code. - **Incoming Call Route Locale**: The incoming call route locale, if set, is used if caller is external. - **User Locale**: The user locale, if set, is used if the caller is internal. - **System Locale**: If no user or incoming call route locale is set, the system locale is used unless overridden by a short code locale. - Systems using Embedded Voicemail, if the required set of upgraded language prompts to match the locale is not present on the system SD card, Manager will display an error. The required prompt set can be uploaded from Manager using the Add/Display VM Locales option. • **Remote Audix Voicemail**: Select this option if using a remote Avaya Intuity Audix or MultiMessage voicemail system. Requires entry of an **Audix Voicemail** license in Licenses. This option is not supported by Server Edition systems. • **Voicemail Pro** Select this option when using Voicemail Pro. The IP address of the PC being used should be set as the **Voicemail IP Address**. In a Server Edition network this option is used on the Primary Server. It can also be used on the Secondary Server if the Secondary server is connected to its own voice mail server or if the Secondary Server is part of an Outbound Contact Express deployment. Use of Voicemail Pro requires licenses for the number of simultaneous calls to be supported. Licenses are not required for an Outbound Contact Express deployment. • **Voicemail Mode**: Default = IP Office Mode. Embedded Voicemail on IP500 V2 systems can use either **IP Office Mode** or **Intuity Mode** key presses for mailbox functions. End users should be provided with the appropriate mailbox user guide for the mode selected. You can switch between modes without losing user data, such as passwords, greetings, or messages. The following user guides are available from the Avaya support web site: • IP Office Essential Edition - Embedded Voicemail User Guide (Intuity Mode) • IP Office Essential Edition - Embedded Voicemail User Guide (IP Office Mode) • IP Office Voicemail Pro Mailbox User Guide (Intuity Mode) • IP Office Voicemail Pro Mailbox User Guide (IP Office Mode)

Table continues…

Field	Description
Add/Display VM Locales	For new IP500 V2 SD cards and cards recreated using Manager, the following Embedded Voicemail languages set are placed onto cards by default. Using this option displays the list of languages that can be uploaded from Manager. Those languages already present or not supported are greyed out. If a locale is selected for the system, a user, a short code or an incoming call route which is not present on the SD card, Manager will display an error. This command can be used to upload the required language prompts to correct the error.
Voicemail Destination	Defaults: Non-Server Edition = Blank, Server Edition = IP trunk connection to the Primary Server. • When the **Voicemail Type** is set to **Remote Audix Voicemail**, **Centralized Voicemail** or **Distributed Voicemail**, this setting is used to enter the outgoing line group of the line configured for connection to the phone system hosting the central voicemail server. • When the **Voicemail Type** is set to **Group Voicemail**, this setting is used to specify the group whose user extensions are connected to the 3rd party voicemail system. • When the **Voicemail Type** is set to **Analogue Trunk MWI**, this setting is used to specify the phone number of the message center. All analogue trunks configured for **Analogue Trunk MWI** must have the same destination.
Voicemail IP Address	Defaults: Non-Server Edition = 255.255.255.255, Primary Server = Primary Server IP Address. This setting is used when the **Voicemail Type** is set to **Voicemail Pro** or **Distributed Voicemail**. It is the IP address of the PC running the voicemail server that the system should use for its voicemail services. If set as 255.255.255.255, the control unit broadcasts on the LAN for a response from a voicemail server. If set to a specific IP address, the system connects only to the voicemail server running at that address. If the system is fitted with an Unified Communication Module hosting Voicemail Pro, the field should be set to 169.254.0.2.
Backup Voicemail IP Address	Defaults: Primary Server = Secondary Server IP Address, All others = 0.0.0.0 (Off). This option is supported with Voicemail Pro. An additional voicemail server can be setup but left unused. If contact to the voicemail server specified by the **Voicemail IP Address** is lost, responsibility for voicemail services is temporarily transferred to this backup server address.
Phone-context	Default = Blank. Available when **CallPilot** is selected as the **Voicemail Type**. The appropriate string, for example CDP or UDP, according to the CS 1000 network dial plan configuration for the CallPilot mailbox. IP Office includes this string, along with the redirecting extension number, in the History-Info header of the SIP message that it sends to leave voicemail on CallPilot. The information in the History-Info header identifies the CallPilot mailbox to which the voicemail is sent. For more information about CS 1000 dial plans, see the CS 1000 documentation.

Table continues…

Field	Description
Audix UDP	Available if the voicemail type Remote Audix Voicemail is selected. Needs to be completed with a four digit number from the Universal Dial Plan of the Avaya Communication Manager system.
Voicemail Channel Reservation	These settings allow the channels between the system and Voicemail Pro to be reserved for particular functions. Unreserved channels can be used for any function but reserved channels cannot be used for any function other than that indicated. These settings are not available unless the configuration includes validated licenses for the total number of voicemail channels. Note that the voicemail server also restricts the maximum number of channels that can be used for some services that would be taken from the **Unreserved Channels** pool. Alarms and callbacks are each limited to up to 2 (IP500 V2) or 5 (Server Edition) channels at any time. Outcalling and conference invites are each limited to up to 5 (IP500 V2) or 12 (Server Edition) channels at any time. • **Unreserved Channels**: This setting cannot be changed and by default will show the total number of licensed voicemail channels. This number will decrease as channels are reserved for the following functions. • **Mailbox Access**: Default = 0 This setting sets the number of channels reserved for users accessing mailboxes to collect messages. • **Auto-Attendant:**: Default = 0 This setting sets the number of channels reserved for users directed to Voicemail Pro short code and module start points. • **Voice Recording**: Default = 0 This setting sets the number of channels reserved for voice recording other than mandatory voice recording (see below). If no channels are available recording does not occur though recording progress may be indicated. • **Mandatory Voice Recording**: Default = 0 This setting sets the number of channels reserved for mandatory voice recording. When no channels are available for a call set to mandatory recording, the call is barred and the caller hears busy tone. • **Announcements:** Default = 0 This setting sets the number of channels reserved for announcements. When no channels are available calls continue without announcements.
Maximum Record Time	Default = 120 seconds. Range = 30 to 180 seconds. This field is only available when **Embedded Voicemail** is selected as the **Voicemail Type**. The value sets the maximum record time for messages and prompts.
Messages Button Goes to Visual Voice	Default = On. Visual Voice allows phone users to check their voicemail mailboxes and perform action such as play, delete and forward messages through menus displayed on their phone. By default, on phones with a **MESSAGES** button, the navigation is via spoken prompts. This option allows that to be replaced by Visual Voice on phones that support Visual Voice menus. For further details see the button action Visual Voice on page 935 .

Table continues…

Field	Description
Outcalling Control	Default = Off *(Outcalling allowed)*. This setting is used to enable or disable system wide outcalling on **Embedded Voicemail** and Voicemail Pro. When selected, all outcalling and configuration of outcalling is disabled. For Voicemail Pro, outcalling can also be disabled at the individual user mailbox level using the Voicemail Pro client.
DTMF Breakout Allows system defaults to be set. These are then applied to all user mailboxes unless the users own settings differ. The Park & Page feature is supported when the system voicemail type is configured as **Embedded Voicemail** or **Voicemail Pro**. Park & Page is also supported on systems where Avaya Aura Messaging, Modular Messaging over SIP, or CallPilot (for IP Office Aura Edition with CS 1000 deployments) is configured as the central voice mail system and the local Embedded Voicemail or Voicemail Pro provides auto attendant operation. The Park & Page feature allows a call to be parked while a page is made to a hunt group or extension. This feature can be configured for Breakout DTMF 0, Breakout DTMF 2, or Breakout DTMF 3.	
Reception/Breakout (DTMF 0)	The number to which a caller is transferred if they press 0while listening to the mailbox greeting rather than leaving a message (***0** on Embedded Voicemail in IP Office Mode). For voicemail systems set to Intuity emulation mode, the mailbox owner can also access this option when collecting their messages by dialing ***0**. If the mailbox has been reached through a Voicemail Pro call flow containing a **Leave Mail** action, the option provided when **0** is pressed are: • For IP Office mode, the call follows the **Leave Mail** action's **Failure** or **Success** results connections depending on whether the caller pressed **0** before or after the record tone. • For Intuity mode, pressing **0** always follows the **Reception/Breakout (DTMF 0)** setting. • When Park & Page is selected for a DTFM breakout, the following drop-down boxes appear: - **Paging Number**: Displays a list of hunt groups and users (extensions). Select a hunt group or extension to configure this option. - **Retries**: The range is 0 to 5. The default setting is 0. - **Retry Timeout**Provided in the format M:SS (minute:seconds). The range can be set in 15-second increments. The minimum setting is 15 seconds and the maximum setting is 5 minutes. The default setting is 15 seconds
Breakout (DTMF 2)	The number to which a caller is transferred if they press 2while listening to the mailbox greeting rather than leaving a message (***2** on Embedded Voicemail in IP Office Mode).
Breakout (DTMF 3)	The number to which a caller is transferred if they press 3while listening to the mailbox greeting rather than leaving a message (***3** on Embedded Voicemail in IP Office Mode).

Table continues…

Field	Description
Voicemail Code Complexity Defines the requirements for the voicemail code. For IP Office systems that have **Voicemail Type** set to **Centralized**, the **Voicemail Code Complexity** settings must be the same as the IP Office system that is connected to Voicemail Pro.	
Enforcement	Default = On. When on, a user PIN is required. The enforcement is not forced during upgrade but after checking, it can not be cleared.
Minimum Length	Default = 6. Maximum 31 digits. Older configurations can continue to have 4 digits with a maximum of 20 digits.
Complexity	Default = On. When on, the following complexity rules are enforced. • The user extension number cannot be used. • A PIN consisting of repeated digits is not allowed (111111). • A PIN consisting of a sequence, forward or reverse, is not allowed (123456, 564321). The number of users having invalid Voicemail Code complexity is highlighted below this field in red colored text.
Call Recording These setting relate to call recording. Call recording is only supported when using a Voicemail Pro voicemail server.	
Auto Restart Paused Recording (secs)	Default = 15 seconds. Range = Never or 5 to 999 seconds. If recording, manual or automatic, of a call is halted using a Pause Recording button, this timer determines when recording is restarted if the button is not pressed again.
Hide Auto Recording	Default = On (USA)/Off (Rest of World) During call recording by Voicemail Pro, some Avaya phones display REC or similar to show that the call is being recorded. When on, hide auto recording suppresses this recording indication.
SIP Settings	For Enterprise Branch deployments, these settings are used for calls made or received on a SIP line where any of the line's SIP URI fields are set to use internal data. For Embedded Voicemail and Voicemail Pro, for calls made or received on a SIP line where any of the line's SIP URI fields are set to **Use Internal Data**, that data is taken from these settings. These options are shown if the system has SIP trunks and is set to use **Embedded Voicemail**, **Voicemail Lite/Pro**, **Centralized Voicemail** or **Distributed Voicemail**.
SIP Name	Default = Blank on Voicemail tab/Extension number on other tabs. The value from this field is used when the From field of the SIP URI being used for a SIP call is set to **Use Internal Data**.

Table continues…

Field	Description
SIP Display Name (Alias)	Default = Blank on Voicemail tab/Name on other tabs. The value from this field is used when the Display Name field of the SIP URI being used for a SIP call is set to **Use Internal Data**
Contact	Default = Blank on Voicemail tab/Extension number on other tabs. The value from this field is used when the Contact field of the SIP URI being used for a SIP call is set to **Use Internal Data**.
Anonymous	Default = On on Voicemail tab/Off on other tabs. If the From field in the SIP URI is set to **Use Internal Data**, selecting this option inserts **Anonymous** into that field rather than the SIP Name set above.

Voicemail Language Prompts

When the system routes a call to the voicemail server it indicates the locale for which matching prompts should be provided if available. The locale sent to the voicemail server by the system is determined as show below. If the required set of prompts is not available, the voicemail will fallback to another appropriate language and finally to English (refer to the appropriate voicemail installation manual for details).

- **Short Code Locale**: The short code locale, if set, is used if the call is routed to voicemail using the short code.
- **Incoming Call Route Locale**: The incoming call route locale, if set, is used if caller is external.
- **User Locale**: The user locale, if set, is used if the caller is internal.
- **System Locale**: If no user or incoming call route locale is set, the system locale is used unless overridden by a short code locale.

Systems using Embedded Voicemail, if the required set of upgraded language prompts to match the locale is not present on the system SD card, Manager will display an error. The required prompt set can be uploaded from Manager using the Add/Display VM Locales option.

Related links

System on page 221

System Events

Navigation: **System Settings** > **System** > **System Events**

The system supports a number of methods by which events occurring on the system can be reported. These are in addition to the real-time and historical reports available through the System Status Application (SSA).

Related links

System on page 221
SNMP Settings on page 237
Add SNMP Trap on page 238

SNMP Settings

Navigation: **System Settings** > **System-SNMP** > **SNMP Settings**

This form is used for general configuration related to system alarms.

Note that the QoS Parameters are only available in Manager.

Configuration Settings

These settings can only be edited offline. Changes to these settings require a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
SNMP Agent Configuration	
SNMP Enabled	Default = Off. Enables support for SNMP. This option is not required if using SMTP or Syslog.
Community (Read-only)	Default = Blank. The SNMP community name to which the system belongs.
SNMP Port	Default = 161. Range = 161, or 1024 to 65535. The port on which the system listens for SNMP polling.
Device ID	This is a text field used to add additional information to alarms. If an SSL VPN is configured, Avaya recommends that the Device ID match an SSL VPN service Account Name. Each SSL VPN service account name has an associated SSL VPN tunnel IP address. Having the displayed Device ID match an SSL VPN service account name helps identify a particular SSL VPN tunnel IP address to use for remotely managing IP Office.
Contact	This is a text field used to add additional information to alarms.
Location	This is a text field used to add additional information to alarms.
QoS Parameters These parameters are used if the setting **System Settings** > **System** > **System Events** > **Enable RTCP Monitor on Port 5005** is set to On. They are used as alarm thresholds for the QoS data collected by the system for calls made by Avaya H.323 phones and for phones using VCM channels. If a monitored call exceeds any of the threshold an alarm is sent to the System Status application. Quality of Service alarms can also be sent from the system using Alarms. • The alarm occurs at the end of a call. If a call is held or parked and then retrieved, an alarm can occur for each segment of the call that exceeded a threshold. • Where a call is between two extensions on the system, it is possible that both extensions will generate an alarm for the call. • An alarm will not be triggered for the QoS parameters recorded during the first 5 seconds of a call.	
Round Trip Delay (msec)	Default = 350. Less than 160ms is high quality. Less than 350ms is good quality. Any higher delay will be noticeable by those involved in the call. Note that, depending on the compression codec being used, some delay stems from the signal processing and cannot be removed: G.711 = 40ms, G.723a = 160ms, G.729 = 80ms.

Table continues…

Field	Description		
Jitter (msec)	Default =20. Jitter is a measure of the variance in the time for different voice packets in the same call to reach the destination. Excessive jitter will become audible as echo.		
Packet Loss (%)	Default = 3.0. Excessive packet loss will be audible as clipped words and may also cause call setup delays.		
		Good Quality	**High Quality**
	Round Trip Delay	< 350ms	< 160ms
	Jitter	< 20ms	< 20ms
	Packet Loss	< 3%	< 1%

Related links

System Events on page 236

Add SNMP Trap

Navigation: **System Settings** > **System-SNMP** > **Add/Edit SNMP Trap**

Offline Editing

These settings must be edited offline.

To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

This form is used to configure what can cause alarms to be sent using the different alarm methods.

- Up to 5 alarm traps can be configured for use with the SNMP settings on the **System | System Events | Configuration** tab.
- Up to 3 email alarms can be configured for sending using the systems **System | SMTP** settings. The email destination is set as part of the alarm configuration below.
- Up to 2 alarms can be configured for sending to a Syslog destination that is included in the alarm settings.

Configuration Settings

These settings can only be edited offline. Changes to these settings require a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
New Alarm	This area is used to show and edit the alarm.
Destination To use SNMP or Email the appropriate settings must be configured on the Configuration sub-tab. Note that the Destination type is grayed out if the maximum number of configurable alarms destinations of that type has been reached. Up to 5 alarm destinations can be configured for SNMP, 3 for SMTP email, and 2 for Syslog	

Table continues…

Field	Description
Trap	If selected, the details required in addition to the selected Events are: • **Server Address**: Default = Blank. The IP address or fully qualified domain name (FQDN) of the SNMP server to which trap information is sent. • **Port**: Default = 162. Range = 0 to 65535. The SNMP transmit port. • **Community**: Default = Blank The SNMP community for the transmitted traps. Must be matched by the receiving SNMP server. • **Format**: Default = IP Office. The options are: - **IP Office** SNMP event alarms format in accordance with IP Office. - **SMGR** SNMP event alarms format in accordance with SMGR.
Syslog	If selected, the details required in addition to the selected Events are: • **IP Address**: Default = Blank. The IP address of the Syslog server to which trap information is sent. • **Port**: Default = 514. Range = 0 to 65535. The Syslog destination port. • **Protocol**: Default = UDP. Select UDP or TCP. • **Format**: Default = Enterprise. The options are: - **Enterprise** Syslog event alarms format in accordance with Enterprise. - **IP Office** Syslog event alarms format in accordance with IP Office.
Email	If selected, the details required in addition to the selected Events are: **Email**: The destination email address.
Minimum Security Level	Default = Warnings. The options are: • **Warnings**: All events, from Warnings to Critical, are sent. • **Minor**: Minor, major, and critical events are sent. Warnings are not sent. • **Major**: Major and critical events are sent. Warnings and minor events will not be sent. • **Critical**: Only critical events are sent.
Events	Default = None Sets which types of system events should be collected and sent. The table below lists the alarms associated with each type of event. Text in italics in the messages is replaced with the appropriate data. Items in [] brackets are included in the message if appropriate. The subject line of SMTP email alarms takes the form "System name: IP address - System Alarm".

Type	Events	Event State	Message
Entity	**Application**	Voicemail operation	The Voicemail server is now operational.
		Voicemail Failure	The Voicemail server is down.

Table continues…

Type	Events	Event State	Message
		Voicemail Event - storage OK	The Voicemail server storage is OK.
		Voicemail Event - storage nearly full	The Voicemail server storage is nearly full.
		Voicemail Event - storage full	storage full The Voicemail server storage is full.
	Service	Feature license missing	Attempt to use a feature for which no license is installed. License Type: <name>
		All licenses in use	The following licenses are all in use. License Type: <name>
		Clock source changed	8kHz clock source changed. Details will be provided.
		Logon failed	Logon failure reason will be provided.
		No free channels available	No free channels were available. Outgoing group ID: <number>
		Hold music file failure	Failed to load Hold Music source file.
		All resources in use	The following system resources are all in use: <resource type> will be provided.
		OEM card slot error	System running secondary software or error description with OEM card will be provided.
		Network interconnect failure	Details of the network interconnection failure will be provided.
		SIP message too large	SIP message Rx error - too large - ignored.
	Contact Flash Card	Change	The PC card in *name* has changed.
	Expansion Module	Operational	Expansion module *name* link is up.
		Failure	Expansion module *name* link is down.
		Error	Expansion module *name* link has a link error.
		Change	Expansion module *name* link has changed.
	Trunk	Operational	Trunk number (name) [on expansion module number] is now operational.

Table continues…

Type	Events	Event State	Message
		Failure	Trunk number (name) [on expansion module number] is down.
	Trunk	Trunk seize failure	Seize failure: Channel [number] or Port [number].
		Incoming call outgoing trunk failure	Incoming call outgoing trunk: Channel [number] or Port [number].
		CLI not delivered	CLI not delivered: Channel [number] or Port [number].
		DDI incomplete	DDI incomplete. Expected Number of digits: .
		LOS	LOS
		OOS	OOS
		Red Alarm	Red Alarm
		Blue Alarm	Blue Alarm
		Yellow Alarm	Yellow Alarm
		IP connection failure	IP connection failure. IP Trunk Line Number: <number> or Remote end IP address: <IP address>
		Small Community Network invalid connection	Small Community Network invalid connection. IP trunk line number: <number> or remote end IP address: <IP address>
	Link	Device changed	Device changed. Home Extension Number: .
		LDAP server communication failure	LDAP server communication failure
		Resource down	Link/resource down. Module type, number and name will be provided.
		SMTP server communication failure	SMTP server communication failure
		Voicemail Pro connection failure	Voicemail Pro connection failure
		Dialer connection failure	The Dialer connection has been lost.
	VCM	Operational	VCM module *name* is now operational.
		Failure	VCM module *name* has failed.
Memory Card	**Invalid Card**		

Table continues…

Type	Events	Event State	Message
	Free Capacity		
Generic	**Generic**	Non-primary location boot alarm	System running backup software.
		Invalid SD Card	Incompatible or Invalid (System or Optional) SD Card fitted.
		Network link failure	Network Interface *name* (ip address) has been disconnected.
		Network link operational	Network Interface *name* (ip address) has been connected.
		System warm start	System has been restarted (warm start).
		System cold start	System has restarted from power fail (cold start).
		SNMP Invalid community	Invalid community specified in SNMP request.
License	**License Server**	Server Operational	The license server is now operational.
		Server failure	The license server is no longer operational.
	License Key Failure	License Key Failure	
Loopback	**Loopback**	Near end line loopback	Trunk number (*name*) [on expansion module *number*] is in near end loopback.
		Near end payload loopback	Trunk number (*name*) [on expansion module *number*] is in near end loopback with payload.
		Loopback off	Trunk number (*name*) [on expansion module *number*] has no loopback.
Phone Change	**Phone Change**	Phone has been unplugged	The phone with id *n* has been removed from extension *extension* (*unit*, port *number*).
		Phone has been plugged in	The phone with type *type* (*id number*) has been plugged in for extension *extension* (*unit*, port *number*).
Quality of Service	**QoS Monitoring**	If Enable RTCP Monitor on Port 5005 is selected, any monitored calls that exceeds the set QoS Parameters causes an alarm.	
Syslog	**Basic Audit**	Events as written to the system Audit Trail. Available on Syslog output only.	

Table continues…

Type	Events	Event State	Message
	Extended Audit	Configuration change information. Each message contains one configuration or security settings object attribute change, and optionally the previous and new values.	
	System Monitor	If selected, System monitor traces are packed into Syslog traces.	
System	**Configuration**	CCR group agent is not targeted. **Note:** CCR is not supported in IP Office release 9.1 and later.	CCR Group agent not targeted as it is not an CCR Agent. Group: <name> Agents: <name1, ..., name n>.
		Small Community Network dial plan conflict	Small Community Network dial plan conflict
		No incoming call route for call	The following line had no Incoming Call Route for a call. Line: <number> or Line Group ID: <number>.
		Installed hardware failure	Installed hardware failure details will be provided.
	System Shutdown		
	Running Backup		
	Emergency Calls	Emergency call successful	Successful Emergency Call | Emergency call! Location:*location* Dialled:*dialled number* Called:*number* sent on the line CallerID: *ID* Usr:*user* Extn:*extension*
		Emergency call failed	Failed Emergency Call | Emergency *call*! Location:*location* Dialled:*dialled number*FailCause:*cause* Usr:*user* Extn: *extension*

Alarm Types

Note the following.

- **Voicemail Pro Storage Alarms**: The alarm threshold is adjustable through the Voicemail Pro client.
- **Embedded Voicemail Storage Alarms**: A disk full alarm is generated when the Embedded Voicemail memory card reaches 90% full. In addition a critical space alarm is generated at 99% full and an OK alarm is generated when the disk space returns to below 90% full.
- **Loopback**: This type of alarm is only available for systems with a United States locale.

The list of IP Office alarms is available on the Admin CD in the folder `\snmp_mibs\IPOffice`.

Related links

System Events on page 236

SMTP

Navigation: **System Settings** > **System** > **SMTP**

Offline Editing

These settings must be edited offline.

To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Configuration Settings

SMTP can be used as the method of sending system alarms. The email destination is set as part of the email alarms configured in **System Settings** > **System-SNMP** > **Add/Edit SNMP Trap**.

SMTP can be used with Embedded Voicemail for Voicemail Email. The voicemail destination is set by the user's Voicemail Email address.

Field	Description
Server Address	Default = Blank This field sets the IP address of the SMTP server being used to forward SNMP alarms sent by email.
Port	Default = 25. Range = 0 to 65534. This field set the destination port on the SMTP server.
Email From Address	Default = Blank This field set the sender address to be used with mailed alarms. Depending of the authentication requirements of the SMTP server this may need to be a valid email address hosted by that server. Otherwise the SMTP email server may need to be configured to support SMTP relay.
Use STARTTLS	Default = Off. (Release 9.0.3). Select this field to enable TLS/SSL encryption. Encryption allows voicemail-to-email integration with hosted email providers that only permit SMTP over a secure transport.
Server Requires Authentication	Default = Off This field should be selected if the SMTP server being used requires authentication to allow the sending of emails. When selected, the User Name and Password fields become available
User Name	Default = Blank This field sets the user name to be used for SMTP server authentication.
Password	Default = Blank This field sets the password to be used for SMTP server authentication.

Table continues…

Field	Description
Use Challenge Response Authentication (CRAM-MD5)	Default = Off. This field should be selected if the SMTP uses CRAM-MD5.

Related links

System on page 221

DNS

Navigation: **System Settings** > **System** > **DNS**

DNS is a mechanism through which the URL's requested by users, such as www.avaya.com, are resolved into IP addresses. These requests are sent to a Domain Name Server (DNS) server, which converts the URL to an IP address. Typically the internet service provider (ISP) will specify the address of the DNS server their customers should use.

WINS (Windows Internet Name Service) is a similar mechanism used within a Windows network to convert PC and server names to IP addresses via a WINS server.

If the system is acting as a DHCP server, in addition to providing clients with their own IP address settings it can also provide them with their DNS and WINS settings if requested by the client.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Related links

System on page 221

SMDR

Navigation: **System Settings** > **System** > **SMDR**

Using a specified IP address, the system can send a call record for each completed call.

Note:

Outbound Contact Express does not generate SMDR records.

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

Field	Description
Output	Default = No Output. Select the type of call record that the system should output via IP. The options are: • **No Output** • **SMDR Only** : Send call records using the SMDR settings below.
SMDR: Station Message Detail Recorder Communications This fields are available when SMDR is selected as the output. For information on SMDR record details, see the appendix.	
IP Address	Default = 0.0.0.0 (Listen). The destination IP address for SMDR records. The address 0.0.0.0 puts the control unit in listen mode on the specified TCP port. When a connection is made on that port, all SMDR records in the buffer are provided.
TCP Port	Default = 0. The destination IP port for SMDR records.
Records to Buffer	Default = 500. Range = 10 to 3000. The system can cache up to 3000 SMDR records if it detects a communications failure with destination address. If the cache is full, the system will begin discarding the oldest records for each new record.
Call Splitting for Diverts	Default = Off. When enabled, for calls forwarded off-switch using an external trunk, the SMDR produces separate initial call and forwarded call records. This applies for calls forwarded by forward unconditional, forward on no answer, forward on busy, DND or mobile twinning. It also applies to calls forwarded off-switch by an incoming call route. The two sets of records will have the same Call ID. The call time fields of the forward call record are reset from the moment of forwarding on the external trunk.

Related links

System on page 221

LAN1

Navigation: **System Settings** > **System** > **LAN1**

Used to configure the behavior of the services provided by the system's first LAN interface.

Up to 2 LAN's (LAN1 and LAN2) can be configured. The control unit has 2 RJ45 Ethernet ports, marked as LAN and WAN. These form a full-duplex managed layer-3 switch. Within the system configuration, the physical LAN port is LAN1, the physical WAN port is LAN2.

Configuring both interfaces with the same IP address on the same subnet is not supported. However, no warning is issued when this configuration is implemented.

Related links

System on page 221
Settings on page 247
VoIP on page 248
Network Topology on page 257
DHCP Pools on page 261

Settings

Navigation: **System Settings** > **System** > **LAN1** > **Settings**

Configuration Settings

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
IP Address	Default = 192.168.42.1 or DHCP client. This is the IP address of the Control Unit on LAN1. If the control unit is also acting as a DHCP server on the LAN, this address is the starting address for the DHCP address range.
IP Mask	Default = 255.255.255.0 or DHCP client. This is the IP subnet mask used with the IP address.
Primary Trans. IP Address	Default = 0.0.0.0 (Disabled) This setting is only available on control units that support a LAN2. Any incoming IP packets without a service or session are translated to this address if set.
RIP Mode	Default = None. Routing Information Protocol (RIP) is a method by which network routers can exchange information about device locations and routes. Routes learnt using RIP are known as 'dynamic routes'. The system also supports 'static routes' though its IP Route records. For Server Edition systems this setting is only available on Expansion System (V2) systems. The options are: • **None**: The LAN does not listen to or send RIP messages • **Listen Only (Passive)**: Listen to RIP-1 and RIP-2 messages in order to learn RIP routes on the network. • **RIP1**: Listen to RIP-1 and RIP-2 messages and send RIP-1 responses as a sub-network broadcast. • **RIP2 Broadcast (RIP1 Compatibility)**: Listen to RIP-1 and RIP-2 messages and send RIP-2 responses as a sub-network broadcast. • **RIP2 Multicast**: Listen to RIP-1 and RIP-2 messages and send RIP-2 responses to the RIP-2 multicast address.

Table continues…

Field	Description
Enable NAT	Default = Off This setting controls whether NAT should be used for IP traffic from LAN1 to LAN2. This setting should not be used on the same LAN interface as a connected WAN3 expansion module.
Number of DHCP IP Addresses	Default = 200 or DHCP client. Range = 1 to 999. This defines the number of sequential IP addresses available for DHCP clients.
DHCP Mode	Default = DHCP Client. This controls the control unit's DHCP mode for the LAN. When doing DHCP: • LAN devices are allocated addresses from the bottom of the available address range upwards. • Dial In users are allocated addresses from the top of the available range downwards. • If the control unit is acting as a DHCP server on LAN1 and LAN2, Dial in users are allocated their address from the LAN1 pool of addresses first. The options are: • **Server**: When this option is selected, the system will act as a DHCP Server on this LAN, allocating address to other devices on the network and to PPP Dial in users. • **Disabled** When this option is selected, the system will not use DHCP. It will not act as a DHCP server and it will not request an IP address from a DHCP server on this LAN. • **Dial In** When this option is selected, the system will allocate DHCP addresses to PPP Dial In users only. On systems using DHCP pools, only addresses from a pool on the same subnet as the system's own LAN address will be used. • **Client** When this option is selected, the system will request its IP Address and IP Mask from a DHCP server on the LAN. **Note:** Do not use this option with a limited time lease line. • **Advanced**: The system can be configured with a number of DHCP Pools from which it can issue IP addresses.

Related links

LAN1 on page 246

VoIP

Navigation: **System Settings** > **System** > **LAN1** > **VoIP**

Additional configuration information

For more information on remote H.323 extensions, see “Configuring Remote H.323 Extensions” in the chapter **Configure general system settings** in *Administering Avaya IP Office™ Platform with Web Manager*.

Configuration settings

Used to set the system defaults for VoIP operation on the LAN interface.

The following settings can be edited online.

- **Auto-create Extn**
- **Auto-create User**
- **H.323 Signalling over TLS**
- **Remote Call Signalling Port**
- **Auto-create Extn/User**
- **Enable RTCP Monitoring on Port 5005**
- **RTCP collector IP address for phones**
- **Scope**
- **Initial keepalives**
- **Periodic timeout**
- **VLAN**
- **1100 Voice VLAN Site Specific Option Number (SSON)**
- **1100 Voice VLAN IDs**

The remaining settings must be edited offline. Changes to these settings requires a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
H.323 Gatekeeper Enable Default = Off This settings enables gatekeeper operation.	

Table continues…

Field	Description
H.323 Signalling over TLS	Default = Disabled. For hosted deployments, default = Preferred. When enabled, TLS is used to secure the registration and call signalling communication between IP Office and endpoints that support TLS. The H.323 phones that support TLS are 9608, 9611, 9621, and 9641running firmware version 6.6 or higher. When enabled, certificate information is configured in the `46xxSettings.txt` file on IP Office and automatically downloaded to the phone. When IP Office receives a request from the phone for an identity certificate, IP Office searches it's trusted certificate store and finds the root CA that issued it's identity certificate. IP Office then provides the root CA as an auto-generated certificate file named `Root-CA-xxxxxxxx.pem`. For information on IP Office certificates, see **Security Manager** > **Certificates**. The options are: • **Disabled**: TLS is not used. • **Preferred**: Use TLS when connecting to a phone that supports TLS. • **Enforced**: TLS must be used. If the phone does not support TLS, the connection is rejected. When set to **Enforced**, the **Remote Call Signalling Port** setting is disabled. If TLS security is enabled (**Enforced** or **Preferred**), it is recommended that you enable a matching level of media security on **System Settings** > **System** > **VoIP Security**.
H.323 Remote Extn Enable	Default = Off. The system can be configured to support remote H.323 extensions in the case where NAT is used in the connection path. This could be the case where the IP Office is located behind a corporate NAT/Firewall router and/or the H.323 phone is located behind residential NAT enable router. The use of this option and the interaction and configuration of external third party elements is beyond the scope this help file. In the case where the public IP address of the corporate router is unknown, the LAN's Network Topology settings should be used to configure a STUN Server. Enabling **H.323 Remote Extn Enable** allows configuration of the **RTP Port number Range (NAT)** settings. Currently, only 9600 Series phones are supported as H.323 remote extensions.

Table continues…

Field	Description
Auto-create Extn	Default = Off The field to set up auto creation of extensions for H.323 phones registering themselves with the System as their gatekeeper. If selected, the system displays the **Auto Create Extension Password** window prompting you to type a Password and Confirm Password. This password is used for subsequent auto creation of extensions. A message `H.323 Auto-Create Extension option is active` is flashed next to the **Auto Create Extension** field till the option is cleared. SIP Extensions use a separate setting, see below. This setting is not supported on systems configured to use WebLM server licensing. If using resilience backup to support Avaya IP phones, **Auto-create Extn** and **Auto-create User** should not be left enabled after initial configuration or any subsequent addition of new extensions and users. Leaving auto-create options enabled on a system that is a failover target may cause duplicate extension/user records on the multi-site network under multiple failure scenarios. For security, any auto-create settings set to On are automatically set to Off after 24 hours.
SIP Trunks Enable	Default = On. This settings enables support of SIP trunks. It also requires entry of **SIP Trunk Channels** licenses. Enabling **SIP Trunks Enable** allows configuration of the **RTP Port number Range (NAT)** settings.
SIP Registrar Enable Default = Off. Used to set the system parameters for the system acting as a SIP Registrar to which SIP endpoint devices can register. Separate SIP registrars can be configured on LAN1 and LAN2. Registration of a SIP endpoint requires an available **IP Endpoints** license. SIP endpoints are also still subject to the extension capacity limits of the system.	

Table continues…

Field	Description
SIP Remote Extn Enable	Default = Off. The system can be configured to support remote SIP extensions in the case where NAT is used in the connection path. This could be the case where the IP Office is located behind a corporate NAT/Firewall router and/or the SIP phone is located behind residential NAT enable router. This option cannot be enabled on both LAN1 and LAN2. The use of this option and the interaction and configuration of external third party elements is beyond the scope this help file. In the case where the public IP address of the corporate router is unknown, the LAN's Network Topology settings should be used to configure a STUN Server. Enabling **SIP Remote Extn Enable** allows configuration of: • the **Remote UDP Port**, **Remote TCP Port**, **Remote TLS Port** settings • the **Port Number Range (NAT)** settings Currently, only Avaya Equinox™ for Windows, Avaya Equinox™ for iOS, one-X Mobile iOS and one-X Mobile Android SIP clients are supported as SIP remote extensions.
Allowed SIP User agents	Default = Block blacklist only The drop-down menu to select which SIP devices are allowed to register with the IP Office system. Depending on the selection, IP Office allows registration of SIP User Agents specified using the **System** > **VOIP** > **Access Control Lists** tab. The options are: • **Allow All**: Do not block any devices based on the UI strings. • **Block Blacklist Only**: Block devices whose UA string is listed in the **SIP UA Blacklist**. • **Avaya Clients & Whitelisted**: Only allow devices with an Avaya UA string or whose UA string is listed in the **SIP UA Whitelist**. • **Avaya Clients Only**: Only allow clients with an Avaya UA string. • **Whitelisted only**: Only allow devices whose UA string is listed in the **SIP UA Whitelist**.

Table continues…

Field	Description
Auto-create Extn/User	Default = Off. The field to set up auto creation of extensions for SIP phones registering themselves with the SIP registrar. If selected, the system displays the **Auto Create Extension Password** window prompting you to type a Password and Confirm Password. This password is used for subsequent auto creation of extensions. A message `SIP Auto-Create Extension/User option is active` is flashed next to the **Auto Create Extension/User** field till the option is cleared. This setting is not supported on systems configured to use WebLM server licensing. For security, any auto-create settings set to On are automatically set to Off after 24 hours. **Note:** This setting is not applicable to the Avaya A175 Desktop Video Device with the Avaya Communicator.
SIP Domain Name	Default = Blank This value is used by SIP endpoints for registration with the IP Office system. SIP endpoints register with IP Office using their SIP address that consists of their phone number and IP Office SIP domain. Since IP Office does not allow calls from unauthorized entities, the SIP domain does not need to be resolvable. However, the SIP domain should be associated with FQDN (Fully Qualified Domain Name) for security purposes. The entry should match the domain suffix part of the SIP Registrar FQDN below, for example, `example.com`. If the field is left blank, registration uses the LAN 1, LAN2, or public IP address. **Note:** For Avaya SIP telephones supported for resilience, the **SIP Domain Name** must be common to all systems providing resilience.
SIP Registrar FQDN	Default = Blank This is the SIP registrar fully qualified domain name, for example, `server1.example.com`, to which the SIP endpoint should send its registration request. This address must be resolvable by DNS to the IP address of the IP Office system or to the IP address, such as that of an Avaya SBCE, through which the SIP endpoints reach the IP Office system.
Challenge Expiry Time (secs)	Default = 10. The challenge expiry time is used during SIP extension registration. When a device registers, the system SIP Registrar will send a challenge back to the device and waits for an appropriate response. If the response is not received within this timeout the registration is failed.

Table continues…

Field	Description
Layer 4 Protocol	Default = TCP and UDP. This field is used to select which protocols are supported for SIP connections: TCP, UDP, or TLS. • **UDP Port**: Default = 5060. The port to use for SIP UDP support if UDP is selected as the **Layer 4 Protocol** above. • **TCP Port**: Default = 5060. The port to use for SIP TCP support if TCP is selected as the **Layer 4 Protocol** above. • **TLS Port**: Default = 5061. The port to use for SIP TLS support. • **Remote UDP Port**: Default = 5060. The port to use for SIP UDP support if UDP is selected as the Layer 4 Protocol for remote SIP extension. • **Remote TCP Port**: Default = 5060. The port to use for SIP TCP support if TCP is selected as the Layer 4 Protocol for remote SIP extension. • **Remote TLS Port**: Default = 5061. The port to use for SIP TLS support if TLS is selected as the Layer 4 Protocol for remote SIP extension. **Note:** The E129 phone does not support UDP. In IP Office release 10 and higher, UDP support has been removed from the configuration file sent to the phone. For the E129 phone, you must enable TCP.
RTP	
Port Number Range	For each VoIP call, a receive port for incoming Real Time Protocol (RTP) traffic is selected from a defined range of possible ports, using the even numbers in that range. The Real Time Control Protocol (RTCP) traffic for the same call uses the RTP port number plus 1, that is the odd numbers. For control units and Avaya H.323 IP phones, the default port range used is 49152 to 53246. On some installations, it may be a requirement to change or restrict the port range used. It is recommended that only port numbers between 49152 and 65535 are used, that being the range defined by the Internet Assigned Numbers Authority (IANA) for dynamic usage. **Important:** The minimum and maximum settings of the port range should only be adjusted after careful consideration of the customer network configuration and existing port usage. For pre-Release 8.1 systems, the gap between the minimum and maximum port values must be at least 1024. For Release 8.1 and higher, the gap between the minimum and maximum port values must be at least 254.
Port Range (minimum)	IP500 V2 default = 46750. Range = 46750 to 50750. Linux default = 40750. Range = 40750 to 50750 This sets the lower limit for the RTP port numbers used by the system.
Port Range (maximum)	IP500 V2 default = 50750. Range = 46750 to 50750. Linux default = 50750. Range = 47000 to 50750 This sets the upper limit for the RTP port numbers used by the system.

Table continues…

Field	Description
Port Number Range (NAT) These settings are available when either **H.323 Remote Extn Enable**, **SIP Trunks Enable**, or **SIP Remote Extn Enable** is set to On. This option is not supported if **System Settings** > **System** > **LAN1** > **Network Topology** is set to **Symmetric Firewall** or **Open Internet**.	
Port Range (minimum)	IP500 V2 default = 46750. Range = 46750 to 50750. Linux default = 40750. Range = 40750 to 50750 This sets the lower limit for the RTP port numbers used by the system.
Port Range (maximum)	IP500 V2 default = 50750. Range = 46750 to 50750. Linux default = 50750. Range = 40750 to 50750 This sets the upper limit for the RTP port numbers used by the system.
Enable RTCP Monitor On Port 5005	Default = On. For 1600, 4600, 5600 and 9600 Series H.323 phones, the system can collect VoIP QoS (Quality of Service) data from the phones. For other phones, including non-IP phones, it can collect QoS data for calls if they use a VCM channel. The QoS data collected by the system is displayed by the System Status Application. This setting is mergeable. However, it only affects H.323 phones when they register with the system. Therefore, any change to this setting requires H.323 phones that have already been registered to be rebooted. Avaya H.323 phones can be remotely rebooted using the System Status Application. The QoS data collected includes: RTP IP Address, Codec, Connection Type, Round Trip Delay, Receive Jitter, Receive Packet Loss. This setting is not the same as the RTCPMON option within Avaya H.323 phone settings. The system does not support the RTCPMON option.
RTCP collector IP address for phones	Default = Blank. This setting is used to manually set the destination for the RTCP Monitor data described above **Enable RTCP Monitor On Port 5005** field above. This enables you to send the data collected to a third party QoS monitoring application. The **Enable RTCP Monitor On Port 5005** must be turned Off to enable this field. Changes to this setting requires a reboot of the phones.
Keepalives These settings are used to facilitate NAT traversal of RTP/RTCP packets and are applicable to all RTP/RTCP session on the network interface. You should enable these settings on interfaces connected to NAT devices if you are using SIP trunks and/or H323 and SIP remote workers.	
Scope	Default = Disabled Select whether the sending of keepalive packets should be disabled or sent for RTP or for both RTP and RTCP.

Table continues…

Field	Description
Periodic timeout	Default = 0 (Off). Range = 0 to 180 seconds. Sets how long the system will wait before sending a keepalive if no other packets of the select **SCOPE** are seen.
Initial keepalives	Default = Disabled. If enabled, keepalives can also been sent during the initial connection setup.
DiffServ Settings When transporting voice over low speed links it is possible for normal data packets (1500 byte packets) to prevent or delay voice packets (typically 67 or 31 bytes) from getting across the link. This can cause unacceptable speech quality. Therefore it is important that all traffic routers and switches in a network to have some form of Quality of Service mechanism (QoS). QoS routers are essential to ensure low speech latency and to maintain sufficient audible quality. The system applies the DiffServ settings to outgoing traffic on any SIP lines which have **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Transport** > **Use Network Topology Info** set to match the LAN interface. The system supports the DiffServ (RFC2474) QoS mechanism. This uses a Type of Service (ToS) field in the IP packet header. The hex and decimal entry fields for the following values are linked, the hex value being equal to the decimal multiplied by 4.	
DSCP (Hex)	Default = B8 (Hex)/46 (decimal). Range = 00 to FF (Hex)/0 to 63 (decimal) The DiffServ Code Point (DSCP) setting applied to VoIP calls. By default, the same setting is used for audio and video. If desired, you can configure separate values for audio and video. For correct operation, especially over WAN links, the same value should be set at both ends.
Video DSCP (Hex)	Default = B8 (Hex)/46 (decimal). Range = 00 to FF (Hex)/0 to 63 (decimal) The DiffServ Code Point (DSCP) setting applied to video VoIP calls. For correct operation, especially over WAN links, the same value should be set at both ends.
DSCP Mask (Hex)	Default = FC (Hex)/63 (decimal). Range = 00 to FF (Hex)/0 to 63 (decimal) Allows a mask to be applied to packets for the DSCP value.
SIG DSCP (Hex)	Default = 88 (Hex)/34 (decimal). Range = 00 to FF (Hex)/0 to 63 (decimal) This setting is used to prioritize VoIP call signaling.
DHCP Settings	
Primary Site Specific Option Number (4600/5600)	Default = 176. Range = 128 to 254. A site specific option number (SSON) is used as part of DHCP to request additional information. 176 is the default SSON used by 4600 Series and 5600 Series IP phones.
Secondary Site Specific Option Number (1600/9600)	Default = 242. Range = 128 to 254. Similar to the primary SSON. 242 is the default SSON used by 1600 and 9600 Series IP phones requesting installation settings via DHCP.

Table continues…

Field	Description
VLAN	Default = Not present. This option is applied to H.323 phones using the system for DHCP support. If set to **Disabled**, the L2Q value indicated to phones in the DHCP response is 2 (disabled). If set to **Not Present**, no L2Q value is included in the DHCP response.
1100 Voice VLAN Site Specific Option Number (SSON)	Default = 232. This is the SSON used for responses to 1100/1200 Series phones using the system for DHCP.
1100 Voice VLAN IDs	Default = Blank. For 1100/1200 phone being supported by DHCP, this field sets the VLAN ID that should be provided if necessary. Multiple IDs (up to 10) can be added, each separated by a + sign.

Related links

LAN1 on page 246

Network Topology

Navigation: **System Settings** > **System** > **LAN1** > **Network Topology**

STUN (Simple Traversal of UDP through NAT) is a mechanism used with overcome the effect of NAT firewalls. The network address translation (NAT) action performed by this type of firewall can have negative effects on VoIP calls.

Test packets are sent by the system to the address of the external STUN server, those packets crossing the firewall in the process. The STUN server replies and includes copies of the packets it received in the reply. By comparing the packet sent and received, it is possible for the system to determine the type of NAT firewall and to modify future packets to overcome the effects of the firewall.

These settings are used for SIP trunk connections from the LAN, H.323 and SIP remote extensions. For further details of system SIP operation refer to the SIP Line section. The use of STUN is unnecessary if the SIP ITSP uses a Session Border Controller (SBC). Use of SIP requires entry of SIP Trunk Channels licenses.

The following fields can be completed either manually or the system can attempt to automatically discover the appropriate values. To complete the fields automatically, only the STUN Server IP Address is required. STUN operation is then tested by clicking Run STUN. If successful the remaining fields are filled with the results.

Configuration Settings

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
STUN Server IP Address	Default = Blank Enter the IP address or fully qualified domain name (FQDN) of the SIP ITSP's STUN server. The system will send basic SIP messages to this destination and from data inserted into the replies can try to determine the type NAT changes being applied by any firewall between it and the ITSP.
STUN Port	Default = 3478. Defines the port to which STUN requests are sent if STUN is used.

Table continues…

Field	Description
Firewall/NAT Type	Default = Unknown The settings here reflect different types of network firewalls. The options are: • **Blocking Firewall** • **Symmetric Firewall**: SIP packets are unchanged but ports need to be opened and kept open with keep-alives. If this type of NAT is detected or manually selected, a warning 'Communication is not possible unless the STUN server is supported on same IP address as the ITSP' will be displayed as part of the manager validation. • **Open Internet**: No action required. If this mode is selected, settings obtained by STUN lookups are ignored. The IP address used is that of the system LAN interface. • **Symmetric NAT**: A symmetric NAT is one where all requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host. SIP Packets need to be mapped but STUN will not provide the correct information unless the IP address on the STUN server is the same as the ITSP Host. If this type of NAT/Firewall is detected or manually selected, a warning 'Communication is not possible unless the STUN server is supported on same IP address as the ITSP' will be displayed as part of the manager validation. • **Full Cone NAT**: A full cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address. SIP packets need to be mapped to NAT address and Port; any Host in the internet can call in on the open port, that is the local info in the SDP will apply to multiple ITSP Hosts. No warning will be displayed for this type of NAT because the system has sufficient information to make the connection). • **Restricted Cone NAT**: A restricted cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Unlike a full cone NAT, an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X. SIP packets needs to be mapped. Responses from hosts are restricted to those that a packet has been sent to. So if multiple ITSP hosts are to be supported, a keep alive will need to be sent to each host. If this type of NAT/ Firewall is detected or manually selected, no warning will be displayed for this type of NAT. • **Port Restricted Cone NAT**: A port restricted cone NAT is like a restricted cone NAT, but the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P. SIP packets needs to be mapped. Keep-alives must be sent to all ports that will be the source of a packet for each ITSP host IP address. If this type of NAT/Firewall

Table continues…

Field	Description
	is detected or manually selected, no warning will be displayed for this type of NAT. However, some Port Restricted NAT's have been found to be more symmetric in behavior, creating a separate binding for each opened Port, if this is the case the manager will display a warning 'Communication is not possible unless the STUN server is supported on same IP address as the ITSP' as part of the manager validation. • **Static Port Block**: Use the RTP Port Number Range specified on the VoIP tab without STUN translation. Those ports must be fixed as open on any NAT firewall involved • **One-To-One NAT**: This setting supports IP Office cloud deployments where the Primary server is behind a NAT that performs IP address translation but not port mappings. All required ports must be open on the NAT. When set to **One-To-One NAT**, the following configuration settings are applied and cannot be edited. - The **LAN | Network Topology | Public Port** values are set to 0. - **LAN | VoIP | SIP Registrar Enable** remote protocol port values are set to equal their corresponding local protocol port values. - The **LAN | VoIP | RTP | Port Number Range (NAT) Minimum** and **Maximum** values are set to equal the corresponding **Port Number Range** values. • **Unknown**
Binding Refresh Time (seconds)	Default = 0 (Never). Range = 0 to 3600 seconds. Having established which TCP/UDP port number to use, through either automatic or manual configuration, the system can send recurring 'SIP OPTIONS requests' to the remote proxy terminating the trunk. Those requests will keep the port open through the firewall. Requests are sent every x seconds as configured by this field. **Note:** If a binding refresh time has not been set you may experience problems receiving inbound SIP calls as they are unable to get through the Firewall. In these circumstances make sure that this value has been configured.
Public IP Address	Default = 0.0.0.0 This value is either entered manually or discovered by the Run STUN process. If no address is set, the system LAN1 address is used.
Public Port	Default = 0 The public port value for **UDP**, **TCP**, and **TLS**. For each protocol, this value is either entered manually or discovered by the Run STUN process.
Run STUN	This button tests STUN operation between the system LAN and the STUN Server IP Address set above. If successful the results are used to automatically fill the remaining fields with appropriate values discovered by the system. Before using Run STUN the SIP trunk must be configured. When this option is used, a information icon is shown against the fields to indicate that the values were automatically discovered rather than manually entered.

Table continues…

Field	Description
Run STUN on startup	Default = Off This option is used in conjunction with values automatically discovered using Run STUN. When selected, the system will rerun STUN discovery whenever the system is rebooted or connection failure to the SIP server occurs.

Related links

LAN1 on page 246

DHCP Pools

Navigation: **System Settings** > **System** > **LAN1** > **DHCP Pools**

DHCP pools allows for the configuration of of IP address pools for allocation by the system when acting as a DHCP server. On an IP500 V2 system, you can configure up to 8 pools. On Server Edition Linux systems, you can configure up to 64 pools.

By default the DHCP settings (IP Address, IP Mask and Number of DHCP IP Addresses) set on the LAN Settings tab are reflected by the first pool here. For support of PPP Dial In address requests, at least one of the pools must be on the same subnet as the system's LAN. Only addresses from a pool on the same subnet as the system's own LAN address will be used for PPP Dial In.

When these actions are performed, the DHCP (Server or DialIn) is re-initialized which triggers a reboot of the Avaya DHCP Clients (H.323 and SIP) in order to force the Avaya DHCP clients to renew their IP address lease and apply the new settings. For the remaining Avaya and non-Avaya DHCP clients, you must manually reboot the devices in order to force the IP Addresses lease renewal. Otherwise, the devices continue to use the allocated IP addresses until the IP addresses lease time out expires. IP address lease time out is set to three days.

The DHCP server re-initialization causes a reboot of all Avaya DHCP clients and not only of the DHCP clients that have obtained an IP Address within the modified DHCP Pool IP range. Note that IP Office supports phone reboot only for E129 and B179 SIP phone models.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Apply to Avaya IP Phones Only	Default = Off. When set to On, the DHCP addresses are only used for requests from Avaya IP phones. Other devices connected to the system LAN will have to use static addresses or obtain their address from another DHCP server. In addition to the above control, Avaya IP phones will only complete DHCP against a DHCP server configured to supports a Site Specific Option Number (SSON) that matches that set on the phone. The SSON numbers supported by the system DHCP are set on the VoIP sub-tab. Once set to On and the configuration has been merged, you must manually reboot the non-Avaya DHCP Client devices in order to force IP addresses lease renewal and to make the settings new values effective. Otherwise the non-Avaya DHCP Client devices will continue to use the allocated IP addresses until the IP addresses lease time out expires. IP address lease time out is set to three days.
DHCP Pool	Up to 8 pools can be added. The first pool matches the IP Address, IP Mask and Number of DHCP IP Addresses on the LAN Settings sub-tab. When adding or editing pools, Manager will attempt to warn about overlaps and conflicts between pools. The options are: • **Start Address** Sets the first address in the pool. • **Subnet Mask**: Default = 255.255.255.0 Sets the subnet mask for addresses issued from the pool. • **Default Router**: Default = 0.0.0.0 For pools issuing IP addresses on the same subnet as the system LAN's, **0.0.0.0** instructs the system to determined the actual default router address to issue by matching the IP address/subnet mask being issued in the IP Routing table. This matches the default behaviour used by systems without multiple pools. For pools issuing addresses not on the same subnet as the system LAN's, the default router should be set to the correct value for devices on that subnet. • **Pool Size**: Default = 0 Set the number of DHCP client addresses available in the pool.

Related links

LAN1 on page 246

LAN2

Navigation: **System Settings** > **System** > **LAN2**

These settings used to configure the system's second LAN interface. The fields available for LAN2 are the same as for LAN1 except for the following additional field.

These settings can only be edited offline. Changes to these settings require a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Firewall	Default = <None> (No firewall) Allows the selection of a system firewall to be applied to traffic routed from LAN2 to LAN1.

Related links

System on page 221

VoIP

Navigation: **System Settings** > **System** > **VoIP**

This tab is used to set the codecs available for use with all IP (H.323 and SIP) lines and extensions and the default order of codec preference.

- Avaya H.323 telephones do not support G.723 and will ignore it if selected.
- For systems with H.323 lines and extensions, one of the G.711 codecs must be selected and used.
- G.723 and G.729b are not supported by Linux based systems.
- The number of channels provided by an IP500 VCM 32 or IP500 VCM 64 card, up to a maximum of 32 or 64 respectively, depends on the actual codecs being used. This also applies to IP500 VCM 32 V2 and IP500 VCM 64 V2 cards. The following table assumes that all calls using the VCM use the same codec.

Codec	IP500 VCM 32 IP500 VCM 32 V2	IP500 VCM 64 IP500 VCM 64 V2
G.711	32	64
G.729a	30	60
G.723	22	44
G.722	30	60

Paging from an IP device uses the preferred codec of that device. It is the system administrator's responsibility to ensure all the target phones in the paging group support that codec.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Ignore DTMF Mismatch For Phones	Default = On. When set to On, the following settings are visible and configurable: • **Call Management** > **Extensions** > **Edit Extension** > **H323 VoIP** > **Requires DTMF** • **Call Management** > **Extensions** > **Edit Extension** > **SIP VoIP** > **Requires DTMF** When set to On, during media checks, the system ignores DTMF checks if the call is between two VoIP phones and the extension setting **Requires DTMF** is set to **Off**. The two phones can be located on different systems in a Server Edition or SCN deployment. **Note:** Direct media may still not be possible if other settings, such as codecs, NAT settings, or security settings, are mismatched.
Allow Direct Media Within NAT Location	Default = Off. When set to On, the system allows direct media between devices that reside behind the same NAT. Devices are behind the same NAT if their public IP addresses are the same. **Note:** Direct media may still not be possible if other settings, such as codecs, NAT settings, or security settings, are mismatched. The default behavior is to allow direct media between all types of devices (H323 and SIP remote workers and IP Office Lines behind a NAT). In the case of routers that have H323 or SIP ALG, it can be desirable to allow direct media only between certain categories of devices. This can be configured by adding the NoUser Source Number MEDIA_NAT_DM_INTERNAL. For information, see **Call Management** > **Users** > **Add/Edit Users** > **Source Numbers**.
RFC2833 Default Payload	Default = 101. Range = 96 - 127. This field specifies the default value for RFC2833 dynamic payload negotiation. Service providers that do not support dynamic payload negotiation may require a fixed value.

Table continues…

Field	Description
Available Codecs	This list shows the codecs supported by the system and those selected as usable. Those codecs selected in this list are then available for use in other codec lists shown in the configuration settings. For example the adjacent **Default Selection** list and the individual custom selection list on IP lines and extensions. **Warning:** Removing a codec from this list automatically removes it from the codec lists of any individual lines and extensions that are using it. The supported codecs (in default preference order) are: **G.711 A-Law**, **G.711 U-Law**, **G.722**, **G.729** and **G.723.1**. The default order for G.711 codecs will vary to match the system's default companding setting. **G.723.1** and **G.729b** are not supported on Linux based systems.
Default Codec Selection	By default, all IP (H.323 and SIP) lines and extensions added to the system have their **Codec Selection** setting set to **System Default**. That setting matches the codec selections made in this list. The buttons between the two lists can be used to move codecs between the **Unused** and the **Selected** parts of the list and to change the order of the codecs in the selected codecs list.

Related links

System on page 221

VoIP Security

Navigation: **System Settings** > **System** > **VoIP Security**

Use to set system level media security settings. These settings apply to all lines and extensions on which SRTP is supported and which have their **Media Security** settings configured to be **Same as System**. Individual lines and extensions have media security settings that can override system level settings.

Simultaneous SIP extensions that do not have physical extensions in the configuration use the system security settings.

SM lines and all centralized user extensions must have uniform media security settings.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Name	Description
Default Extension Password	Default = Existing default extension password The field provides you with option to view and edit the existing default extension password. The default extension password is set up during IP Office installation either by the administrator or is randomly generated by the system. The system generated random password is of 10 digits. Use the Eye icon to see the existing default password. The password must be between 9 to 13 digits. The feature is not available in IP Office Basic Edition systems.

Table continues…

Name	Description
Confirm Default Extension Password	If you are changing the default extension password, type the new default password.
Media Security	Default = Disabled. Secure RTP (SRTP) can be used between IP devices to add additional security. These settings control whether SRTP is used for this system and the settings used for the SRTP. The options are: • **Same as System**: Matches the system setting at **System Settings** > **System** > **VoIP Security**. • **Disabled**: Media security is not required. All media sessions (audio, video, and data) will be enforced to use RTP only. • **Preferred**: Media security is preferred. Attempt to use secure media first and if unsuccessful, fall back to non-secure media. • **Enforced**: Media security is required. All media sessions (audio, video, and data) will be enforced to use SRTP only. **Warning:** Selecting **Enforced** on a line or extension that does not support media security will result in media setup failures. If media security is enabled (**Enforced** or **Preferred**), it is recommended that you enable a matching level of security using **System Settings** > **System** > **LAN1** > **VoIP** > **H.323 Signalling over TLS**.
Media Security Options	Not displayed if **Media Security** is set to **Disabled**. The options are: • **Encryptions**: Default = RTP This setting allows selection of which parts of a media session should be protected using encryption. The default is to encrypt just the RTP stream (the speech). • **Authentication**: Default = RTP and RTCP This setting allows selection of which parts of the media session should be protected using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Currently not adjustable. • **Crypto Suites**: Default = SRTP_AES_CM_128_SHA1_80. There is also the option to select SRTP_AES_CM_128_SHA1_32.
Strict SIPS	(Enterprise Branch deployments) Default = Off. This option provides a system-wide configuration for call restrictions based on SIPS URI. When this option is off, calls are not rejected due to SIPS. A call is sent according to the configuration of the outgoing trunk or line that it is routed to, regardless of the way the call came in, even if the call came in as a SIP invite with SIPS URI and is being sent with a SIP URI onto a non-secure SIP trunk. When this option is on, an incoming SIP invite with SIPS URI if targeted to a SIP trunk (SM line or SIP line) is rejected if the target trunk is not configured with SIPS in the URI Type field.

Related links

System on page 221

Access Control Lists

Navigation: **System Settings** > **System** > **VoIP**

Name	Description
SIP UA Blacklist	The field to add SIP User Agent (UA) strings. The strings listed here are used to block the registration of SIP devices when the system's Allowed SIP User Agents setting is set to Block Blacklist only. Use the Add button to add a **Blacklist Entry Name** to the list.
SIP UA Whitelist	The field to add SIP UA Whitelist strings. SIP User Agent (UA) strings listed here are used to allow the registration of SIP devices when the system's Allowed SIP User Agents setting is set to Avaya Clients & Whitelisted or Whitelisted Only. Use the Add button to add a **Whitelist Entry Name** to the list.
IP Whitelist	The system can automatically blacklist traffic from an IP address based on too many failed registration attempts from that address. This list can be used to create a list of addresses which should not be blacklisted. This may be useful when there are multiple devices registering from behind the same single public IP address, a scenario where there may be a higher incidence of unintended registration failures during initial setup. Use the Add button to add a **IP Address Entry Value** to the list.

Related links

System on page 221

Directory Services

Navigation: **System Settings** > **System** > **Directory Services**

Related links

System on page 221
LDAP on page 267
HTTP on page 271

LDAP

Navigation: **System Settings** > **System** > **Directory Services** > **LDAP**

Additional configuration information

For additional configuration information, see Centralized System Directory on page 521.

Configuration settings

The system supports LDAP Version 2. LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files

and devices in a network, whether on the Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network. LDAP is lighter because in its initial version, it did not include security features.

The system supports the import of directory records from one system to another using HTTP. That includes using HTTP to import records that another system has learnt using LDAP. HTTP import, which is simpler to configure, can be used to relay LDAP records with LDAP configured on just one system.

LDAP records can contain several telephone numbers. Each will be treated as a separate directory record when imported into the system directory.

In a network, a directory tells you where in the network something is located. On TCP/IP networks, including the Internet, the Domain Name System (DNS) is the directory system used to relate the domain name to a specific network address. However, you may not know the domain name. LDAP allows you to search for an individual without knowing where they're located (although additional information will help with the search).

An LDAP directory is organized in a simple "tree" hierarchy consisting of the following levels:

- The "root" directory (the starting place or the source of the tree), which branches out to
- Countries, each of which branches out to
- Organizations, which branch out to
- Organizational units (divisions, departments, and so forth), which branches out to (includes an entry for)
- Individuals (which includes people, files, and shared resources such as printers)

An LDAP directory can be distributed among many servers. Each server can have a replicated version of the total directory that is synchronized periodically. An LDAP server is called a Directory System Agent (DSA). An LDAP server that receives a request from a user takes responsibility for the request, passing it to other DSA's as necessary, but ensuring a single coordinated response for the user.

LDAP Directory Synchronization allows the telephone number Directory held in the Control Unit to be synchronized with the information on an LDAP server. The feature can be configured to interoperate with any server that supports LDAP Version 2.

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

Field	Description
LDAP Enabled	Default = Off This option turns LDAP support on or off. The system uses LDAP Version 2. If the server being queried is an LDAP Version 3 server, support for LDAP Version 2 requests may need to be enabled on that server (all LDAP Version 3 servers support LDAP Version 2 but do not necessarily have it enabled by default).

Table continues…

Field	Description
User Name	Default = Blank Enter the user name to authenticate connection with the LDAP database. To determine the domain-name of a particular Windows 2000 user look on the "Account" tab of the user's properties under "Active Directory Users and Computers". Note that this means that the user name required is not necessarily the same as the name of the Active Directory record. There should be a built-in account in Active Directory for anonymous Internet access, with prefix "IUSR_" and suffix server_name (whatever was chosen at the Windows 2000 installation). Thus, for example, the user name entered is this field might be: IUSR_CORPSERV@example.com
Password	Default = Blank Enter the password to be used to authenticate connection with the LDAP database. Enter the password that has been configured under Active Directory for the above user. Alternatively an Active Directory object may be made available for anonymous read access. This is configured on the server as follows. In "Active Directory Users and Computers" enable "Advanced Features" under the "View" menu. Open the properties of the object to be published and select the "Security" tab. Click "Add" and select "ANONYMOUS LOGON", click "Add", click "OK", click "Advanced" and select "ANONYMOUS LOGON", click "View/Edit", change "Apply onto" to "This object and all child objects", click "OK", "OK", "OK". Once this has been done on the server, any record can be made in the User Name field in the System configuration form (however this field cannot be left blank) and the Password field left blank. Other non-Active Directory LDAP servers may allow totally anonymous access, in which case neither User Name nor Password need be configured.
Server IP Address	Default = Blank Enter the IP address of the server storing the database.
Server Port	Default = 389 This setting is used to indicate the listening port on the LDAP server.
Authentication Method	Default = Simple Select the authentication method to be used. The options are: • **Simple**: clear text authentication • **Kerberos**: Not used.

Table continues…

Field	Description
Resync Interval (secs)	Default = 3600 seconds. Range = 60 to 99999 seconds. The frequency at which the system should resynchronize the directory with the server. This value also affects some aspects of the internal operation. The LDAP search inquiry contains a field specifying a time limit for the search operation and this is set to 1/16th of the resync interval. So by default a server should terminate a search request if it has not completed within 225 seconds (3600/16). The client end will terminate the LDAP operation if the TCP connection has been up for more than 1/8th of the resync interval (default 450 seconds). This time is also the interval at which a change in state of the "LDAP Enabled" configuration item is checked.

Search Base/Search Filter	Default = Blank These 2 fields are used together to refine the extraction of directory records. Basically the Base specifies the point in the tree to start searching and the Filter specifies which objects under the base are of interest. The search base is a distinguished name in string form (as defined in RFC1779).
	The Filter deals with the attributes of the objects found under the Base and has its format defined in RFC2254 (except that extensible matching is not supported). If the Search Filter field is left blank the filter defaults to "(objectClass=*)", this will match all objects under the Search Base. The following are some examples applicable to an Active Directory database.
	• To get all the user phone numbers in a domain:
	`Search Base: cn=users,dc=acme,dc=com`
	`Search Filter: (telephonenumber=*)`
	• To restrict the search to a particular Organizational Unit (eg office) and get cell phone numbers also:
	`Search Base: ou=holmdel,DC=example,DC=com`
	`Search Filter: (|(telephonenumber=*)(mobile=*))`
	• To get the members of distribution list "group1":
	`Search Base: cn=users,dc=example,dc=com`
	`Search Filter: (&(memberof=cn=group1,cn=users,dc=example,dc=com) (telephonenumber=*))`

Table continues…

Field	Description
Number Attributes	: Default = see below Enter the number attributes the server should return for each record that matches the Search Base and Search Filter. Other records could be ipPhone, otherIpPhone, facsimileTelephoneNumber, otherfacsimileTelephone Number, pager or otherPager. The attribute names are not case sensitive. Other LDAP servers may use different attributes. By default the record is "telephoneNumber,otherTelephone,homePhone=H,otherHomePhone=H,mobile=M ,otherMobile=M", as used by Windows 2000 Server Active Directory for Contacts. The optional "=string" sub-fields define how that type of number is tagged in the directory. Thus, for example, a cell phone number would appear in the directory as: John Birbeck M 7325551234

Related links

Directory Services on page 267

HTTP

Navigation: **System Settings** > **System** > **Directory Services** > **HTTP**

Additional configuration information

For additional configuration information, see Centralized System Directory on page 521.

Configuration settings

The system can use HTTP to import the directory records held by another system. Note that support for HTTP can be disabled. The setting **System Settings** > **System** > **System** > **Avaya HTTP Clients Only** can restrict a system from responding to HTTP requests. The system's **Unsecured Interface** security settings also included controls for HTTP access (**HTTP Directory Read** and **HTTP Directory Write**).

For Server Edition, on Secondary Server, Expansion System (L) and Expansion System (V2) systems, the HTTP settings are automatically defaulted to obtain the system directory from the Primary Server.

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

Field	Description
Directory Type	Default = None (No HTTP import)/IP Office SCN on Server Edition. Set whether HTTP import should be used and the method of importation. The options are: • **None**: Do not use HTTP import. • **IP Office**: Import from the system at the IP address set in the **Source** field. • **IP Office SCN**: Import from a system in a multi-site network. The **Source** field is used to select the **Outgoing Line** ID that matches the H.323 line to the remote system.

Table continues…

Field	Description
Source	Default = Blank/9999 on Server Edition. The form of this field changes according to the **Directory Type** selection above. For **IP Office** this field requires the IP address of the other system. For IP Office SCN, the outgoing group ID of the IP Office line to the remote system is used.
List	Default = All. This field sets what types of directory record should be imported. The options are: • **All**: Import the full set of directory records from the remote system. • **Config Only**: Import just directory records that are part of the remote system's configuration. Note that these will be treated as imported records and will not be added to the local systems own configuration records. • **LDAP Only**: Import just directory records that the remote system has obtained as the result of its own LDAP import. This allows LDAP directory records to be relayed from one system to another. • **HTTP Only**: Import just directory records that the remote system has obtained as the result of its own HTTP import. This allows HTTP directory records to be relayed from one system to another.
URI	Default = /system/dir/complete_dir_list?sdial=true This field is for information only and cannot be adjusted. The path shown changes to match the **List** setting above.
Resync Interval (secs)	Default = 3600 seconds. Set how often the system should request an updated import. When a new import is received, all previously imported records are discarded and the newly imported records are processed.
HTTPS Enabled	Default = On. Turns HTTPS support on or off for directory record import.
Port Number	Default = 443. The port used for the Directory import. When **HTTPS Enabled** is set to On, the default value is 443. When **HTTPS Enabled** is set to Off, the default value is 80.

Related links

Directory Services on page 267

Telephony

Navigation: **System Settings** > **System** > **Telephony**

Used to set the default telephony operation of the system. Some settings shown here can be overridden for individual users through their User | Telephony tab. The settings are split into a number of sub-tabs.

Related links

System on page 221
Telephony on page 273
Park and Page on page 280
Tones and Music on page 281
Ring Tones on page 281
SM on page 282
Call Log on page 284
TUI on page 285

Telephony

Navigation: **System Settings** > **System** > **Telephony**

Additional configuration information

- The **Directory Overrides Barring** setting allows you to control barred numbers. For additional configuration information, see Call Barring on page 570.
- The **Inhibit Off-Switch Forward/Transfer** stops any user from transferring or forwarding calls externally. For additional information, see Off-Switch Transfer Restrictions on page 643.
- For additional information regarding the **Media Connection Preservation** setting, see Media Connection Preservation on page 551.

Configuration settings

Used to configure a wide range of general purpose telephony settings for the whole system.

These settings can be edited online with the exception of **Companding LAW** and **Media Connection Preservation**. These settings must be edited offline and requires a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Analog Extensions These settings apply only to analog extension ports provided by the system. For Server Edition this field is only available on Expansion System (V2) systems	
Default Outside Call Sequence	Default = Normal This setting is only used with analog extensions. It sets the ringing pattern used for incoming external calls. For details of the ring types see **System Settings** > **System** > **Telephony** > **Ring Tones**. This setting can be overridden by a user's **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Settings** > **Outside Call Sequence** setting. Note that changing the pattern may cause fax and modem device extensions to not recognize and answer calls.

Table continues…

Field	Description
Default Inside Call Sequence	Default = Ring Type 1 This setting is only used with analog extensions. It sets the ringing pattern used for incoming internal calls. For details of the ring types see **System Settings** > **System** > **Telephony** > **Ring Tones**. This setting can be overridden by a user's **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Settings** > **Inside Call Sequence** setting.
Default Ring Back Sequence	Default = Ring Type 2 This setting is only used with analog extensions. It sets the ringing pattern used for ringback calls such as hold return, park return, voicemail ringback, and Ring Back when Free. For details of the ring types see **System Settings** > **System** > **Telephony** > **Ring Tones**. This setting can be overridden by a user's **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Settings** > **Ringback Call Sequence** setting.
Restrict Analog Extension Ringer Voltage	Default = Off. Supported on IP500 V2 systems only. If selected, the ring voltage on analogue extension ports on the system is limited to a maximum of 40V Peak-Peak. Also when selected, the message waiting indication (MWI) settings for analog extension are limited to **Line Reversal A**, **Line Reversal B** or **None**. Any analog extension already set to another MWI setting is forced to **Line Reversal A**.
Dial Delay Time (secs)	Default = 4 (USA/Japan) or 1 (ROW). Range = 1 to 30 seconds. This setting sets the time the system waits following a dialed digit before it starts looking for a short code match. In situations where there are potential short codes matches but not exact match, it also sets the delay following the dialing of a digit before dialing complete is assumed.
Dial Delay Count	Default = 0 digits (USA/Japan) or 4 digits (ROW). Range = 0 to 30 digits. This setting sets the number of digits dialed after which the system starts looking for a short code match regardless of the **Dial Delay Time**.
Default No Answer Time (secs)	Default = 15 seconds. Range = 6 to 99999 seconds. This setting controls the amount of time before an alerting call is considered as unanswered. How the call is treated when this time expires depends on the call type. For calls to a user, the call follows the user's Forward on No Answer settings if enabled. If no forward is set, the call will go to voicemail if available or else continues to ring. This timer is also used to control the duration of call forwarding if the forward destination does not answer. It also controls the duration of ringback call alerting. This setting is overridden by the **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Settings** > **No Answer Time** setting for a particular user if different. For calls to hunt groups, this setting controls the time before the call is presented to the next available hunt group member. This setting is overridden by the **Call Management** > **Group** > **Add/Edit Group** > **Group** > **No Answer Time** setting for a particular hunt group if different.

Table continues…

Field	Description
Hold Timeout (secs)	Default = Locale specific. Range = 0 (Off) to 99999 seconds. This setting controls how long calls remain on hold before recalling to the user who held the call. Note that the recall only occurs if the user has no other connected call. Recalled calls will continue ringing and do not follow forwards or go to voicemail.
Park Timeout (secs)	Default = Locale specific. Range 0 (Off) to 99999 seconds. This setting controls how long calls remain parked before recalling to the user who parked the call. Note that the recall only occurs if the user has no other connected call. Recalled calls will continue ringing and do not follow forwards or go to voicemail.
Ring Delay	Default = 5 seconds. Range = 0 to 98 seconds. This setting is used when any of the user's programmed appearance buttons is set to Delayed ringing. Calls received on that button will initially only alert visually. Audible alerting will only occur after the ring delay has expired. This setting can be overridden by a ring delay set for an individual user (**Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Multi-line Options** > **Ring Delay**).
Call Priority Promotion Time (secs)	Default = Disabled. Range = Disabled, 10 to 999 seconds. When calls are queued for a hunt group, higher priority calls are placed ahead of lower priority calls, with calls of the same priority sort by time in queue. External calls are assigned a priority (**1-Low**, **2-Medium** or **3-High**) by the Incoming Call Route that routed the call. Internal calls are assigned a priority of **1-Low**. This option can be used to increase the priority of a call each time it has remained queued for longer than this value. The calls priority is increased by 1 each time until it reaches 3-High. In situations where calls are queued, high priority calls are placed before calls of a lower priority. This has a number of effects: • Mixing calls of different priority is not recommended for destinations where Voicemail Pro is being used to provided queue ETA and queue position messages to callers since those values will no longer be accurate when a higher priority call is placed into the queue. Note also that Voicemail Pro will not allow a value already announced to an existing caller to increase. • If the addition of a higher priority call causes the queue length to exceed the hunt group's Queue Length Limit, the limit is temporarily raised by 1. This means that calls already queued are not rerouted by the addition of a higher priority call into the queue.
Default Currency	Default = Locale specific. This setting is used with ISDN Advice of Charge (AOC) services. Note that changing the currency clears all call costs stored by the system except those already logged through SMDR. The currency is displayed in the system SMDR output.

Table continues…

Field	Description
Default Name Priority	Default = Favor Trunk. For SIP trunks, the caller name displayed on an extension can either be that supplied by the trunk or one obtained by checking for a number match in the extension user's personal directory and the system directory. This setting determines which method is used by default. For each SIP line, this setting can be overridden by the line's own **Name Priority** setting if required. Select one of the following options: • **Favor Trunk**: Display the name provided by the trunk. For example, the trunk may be configured to provide the calling number or the name of the caller. The system should display the caller information as it is provided by the trunk. If the trunk does not provide a name, the system uses the **Favor Directory** method. • **Favor Directory**: Search for a number match in the extension user's personal directory and then in the system directory. The first match is used and overrides the name provided by the SIP line. If no match is found, the name provided by the line, if any, is used.
Media Connection Preservation	Default = Enabled. When enabled, attempts to maintain established calls despite brief network failures. Call handling features are no longer available when a call is in a preserved state. When enabled, Media Connection Preservation applies to SCN links and Avaya H.323 phones that support connection preservation.
Phone Failback	Default = Automatic. Applies to H.323 phones that support resiliency. The options are: • **Automatic** • **Manual** Phones are permitted to failover to the secondary gatekeeper when the IP Office Line link to the primary gatekeeper is down. When set to **Automatic**, if a phone's primary gatekeeper has been up for more than 10 minutes, the system causes the phone to failback if the phone is not in use. If the phone is in use, the system will reattempt failback 10 seconds after the phone ceases to be in use. When set to **Manual**, phones remain in failover until manually restarted or re-registered, after which the phone attempts to fail back. **Note:** Manual failback is not supported on SIP phones.
Login Code Complexity Defines the requirements for the login code.	
Enforcement	Default = On. When on, a user PIN is required.

Table continues…

Field	Description
Minimum Length	Default = 6. Maximum 15 digits. The number of users with login codes less than six digits is displayed below the field in red colored text.
Complexity	Default = On. When on, the following complexity rules are enforced. • The user extension number cannot be used. • A PIN consisting of repeated digits is not allowed (111111). • A PIN consisting of forward or backward sequence are not allowed. Examples: 123456, 654321. The number of users with invalid Code Complexity is highlighted below the field in red colored text.
Send RTCP to an RTCP Collector	When the check box is selected, system RTCP reporting is enabled. For IP Office Release 10.0 and higher, in addition to having the individual phones send RTCP call quality reports, the system can also send RTCP reports for calls.
Server Address	This Sets the address of the third-party QoS monitoring application to which the system sends RTCP reports.
UDP Port Number	The destination port. The default for this filed is 5005.
RTCP reporting interval (secs)	This setting sets the time interval at which the system sends RTCP reports.
Companding Law	These settings should not normally be changed from their defaults. They should only be used where 4400 Series phones (ULAW) are installed on systems which have A-Law digital trunks. **A-Law or U-Law>** PCM (Pulse Code Modulation) is a method for encoding voice as data. In telephony, two methods of PCM encoding are widely used, A-Law and U-Law (also called Mu-Law or μ-Law). Typically U-Law is used in North America and a few other locations while A-Law is used elsewhere. As well as setting the correct PCM encoding for the region, the A-Law or U-Law setting of a system when it is first started affects a wide range of regional defaults relating to line settings and other values. For IP500 V2 systems, the encoding default is set by the type of Feature Key installed when the system is first started. The cards are either specifically A-Law or U-Law.
DSS Status	Default = Off This setting affects Avaya display phones with programmable buttons. It controls whether pressing a DSS key set to another user who has a call ringing will display details of the caller. When off, no caller information is displayed.

Table continues…

Field	Description
Auto Hold	Default = On (Off for the United States locale). Used for users with multiple appearance buttons. When on, if a user presses another appearance button during a call, their current call is placed on hold. When off, if a users presses another appearance button during a call, their current call is disconnected.
Show Account Code	Default = On This setting controls the display and listing of system account codes. • **When on:** When entering account codes through a phone, the account code digits are shown while being dialed. • **When off**: When entering account codes through a phone, the account code digits are replaced by s characters on the display.
Inhibit Off-Switch Forward/Transfer	Default = On When enabled, this setting stops any user from transferring or forwarding calls externally.
Restrict Network Interconnect	Default = Off. When this option is enabled, each trunk is provided with a **Network Type** option that can be configured as either **Public** or **Private**. The system will not allow calls on a public trunk to be connected to a private trunk and vice versa, returning number unobtainable indication instead. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Include location specific information	Default = Off. When set to On, this setting is available in the trunk configuration settings when **Network Type** is set to **Private**. Set to **On** if the PBX on the other end of the trunk is toll compliant.
Drop External Only Impromptu Conference	Default = On. If selected, when the last remaining internal user in a conference exits the conference, the conference is ended, regardless of whether it contains any external callers. If not selected, the conference is automatically ended when the last internal party or trunk that supports reliable disconnect exits the conference. The Inhibit Off-Switch Forward/Transfer option above is no longer applied to conference calls.
Visually Differentiate External Call	Default = Off. This setting is applied to the lamp flashing rate used for bridged appearance and call coverage appearance buttons on 1400, 1600 and 9600 Series phones and on their button modules. When selected, external calls alerting on those buttons will use a slow flash (200ms on/50ms off). If not selected or if the call is internal, normal flashing (500ms on/500ms off) is used.

Table continues…

Field	Description
Unsupervised Analog Trunk Disconnect Handling	Default = Off. When using analog trunks, various methods are used for trunk supervision, ie. to detect when the far end of the trunk has disconnected and so disconnect the local end of the call. Depending on the locale, the system uses Disconnect Clear signalling and or Busy Tone Detection. This setting should only be enabled if it is know that the analog trunks do not provide disconnect clear signalling or reliable busy tone. For Server Edition this field is only available on Expansion System (V2) systems. When enabled: • Disconnect Clear signalling detection is disabled. Busy tone detection remains on. • Unsupervised transfers and trunk-to-trunk transfers of analog trunk calls are not allowed. The **Allow Analog Trunk to Trunk Connect** setting on analog trunks (Line | Analog Options) is disabled. • If Voicemail Pro is being used for external call transfers, **Supervised Transfer** actions should be used in call flows rather than **Transfer** actions. • All systems in the network must have this setting set to match each other.
High Quality Conferencing	Default = On. Supports the use of the G.722 codec. IP lines and extensions using G.722 are provided with wide band audio. If **High Quality Conferencing** is enabled, when several wide band audio devices are in the same conference, the system will ensure that the audio between them remains wide band, even if the conference also contains other lines and devices using narrow band audio (analog devices, digital devices and IP devices using codecs other than G.722).
Digital/Analogue Auto Create User	Default = On. (IP500 V2 only. Default = Off for Server Edition/On for others) When enabled, an associated user is created for each digital/analogue extension created. Digital/analogue extension creation occurs on initial start up, reset of configuration, or addition of new digital/analogue expansion units or plug-in modules.
Directory Overrides Barring	Default = On. When enabled, barred numbers are not barred if the dialed number is in the External Directory.

Table continues…

Field	Description
Advertize Callee State To Internal Callers	Default = Off. When enabled, for internal calls, additional status information is communicated to the calling party. Not supported for SIP endpoints except for J100 Series phones (not including the J129). • When calling another internal phone and the called phone is set to Do Not Disturb or on another call, the calling phone displays “Do Not Disturb” or “On Another Call” rather than “Number Busy”. • On 9500 Series, 9600 Series and J100 Series, if a line appearance is programmed on a button on phone A and that line is in use on phone B, then phone A displays the name of the current user of the line along with the line number. • If a line appearance on a phone is in use elsewhere in the system and another extension unsuccessfully attempts to seize that line, the phone displays “In Use:<name>” where <name> is the name of the user currently using the line. This configuration parameter sets the system wide default. Individual users can be configured for this feature using the setting **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Settings** > **Advertize Callee State To Internal Callers**
Internal Ring on Transfer	Default = Off. When enabled, the transfer enquiry calls ring with internal ring tone even if the call that is being transferred is an external call. If the user transferring the call completes the call when the call is ringing, the ring tone played to the target changes to the ring tone appropriate for the call being transferred. This feature is supported on phone series: 1400, 9500, 1600, 9600, and analog phones. This feature is not supported on SIP and H.323 DECT phones.

Related links

Telephony on page 272

Park and Page

Navigation: **System Settings** > **System** > **Telephony** > **Park and Page**

The Park and Page tab allows for simple configuration of the of the short code and the programmable button for the park and page function.

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

Field	Description
Central Park Range	Default = Blank. Range = nX to nnnnnnnXX The park slot ID range definition, where n is a digit sequence from 1 to 9999999 and X represents a park slot value from 0 to 99. The Central Park Range cannot exceed 9 characters total length. Examples: • 1X defines range 10-19 • 3XX defines range 300-399 • 9876543XX defines range 987654300-987654399
Page Target Group List	Default = Blank. The list of paging group targets that are presented on supported phones if the Page action is requested after the Call Park. On some phones, only the first three groups can be presented as Page options (via the Softkeys on the phone). On phones that support scrolling lists, a larger list of possible Page targets can be presented.

Related links

Telephony on page 272

Tones and Music

Navigation: **System Settings** > **System** > **Telephony** > **Tones and Music**

Additional configuration information

- For additional information on configuring hold music, see Music On Hold on page 536.
- For additional information on ring tones, see Ring Tones on page 535.

Configuration settings

Used to configure the various tones and music on hold sources used by the system.

Related links

Telephony on page 272

Ring Tones

Navigation: **System Settings** > **System** > **Telephony** > **Ring Tones**

Additional configuration information

For additional ring tone configuration information, see Ring Tones. on page 535

Configuration settings

Used to configure distinct ring tones for groups and incoming call routes. Ring Tone configuration is only supported on 1400 series and 9500 series phones.

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

Field	Description
Available Ring Tones	In this table, the **Number**, **Name**, and **Source** values are system supplied. The **Name** value is used to create a ring tone plan.
Ring Tone Plan	Use this table to specify available ring tones. Ring tones in this table can be applied to hunt groups and incoming call routes and by short codes. • **Number**: System supplied. The **Number** can be used in a short code by adding r(x) to the **Telephone Number** field, where x = 1 to 8 and specifies which ring tone plan to use. • **Name**: A descriptive name for where this ring tone is used. For example, the name of a hunt group. Each name in the table must be unique. Once configured in this table, ring tone names can be selected from the **Ring Tone Override** field at: - **Call Management** > **Group** > **Add/Edit Group** > **Group** - **System Settings** > **Incoming Call Route** > **Add/Edit Incoming Call Route** **Ring Tone Override** is supported on 1400 and 9500 series phones. • **Ring Tone**: The list of ring tone names from the **Available Ring Tones** table.

Related links

Telephony on page 272

SM

Navigation: **System Settings** > **System** > **Telephony** > **SM**

Used to configure settings that apply to both SM lines.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Short Form Dialing Length	Default = 0. Range = 0 to 14. This number specifies the short-form dialing length for all Centralized users and Groups. Configuration of this field allows IP Office to treat the last N digits (where N is the number entered in this field) of each Centralized user's extension number as an alias to that user's extension number. For example, if a Centralized user's extension number is 5381111 and the Short Form Dialing Length is 4, the system will match calls to 1111 with this extension. When 1111 is dialed by another user on the system, entered from the autoattendant, or comes from the ICR, then in sunny-day that call will be sent to Session Manager with the number converted to 5381111 and in rainy-day it will target the extension 5381111 locally.

Table continues…

Field	Description
Branch Prefix	Default = Blank. Maximum range = 15 digits. This number is used to identify the IP Office system within the Avaya Aura® network. The branch prefix of each IP Office system must be unique and must not overlap. For example 85, 861 and 862 are okay, but 86 and 861 overlap. On calls routed via an SM Line, the branch prefix is added to the caller's extension number. You have the option to leave the Branch Prefix field blank. If you do not configure the branch prefix, the IP Officeuser extensions must be defined with the full enterprise number.
Local Number Length	Default = Blank (Off). Range = Blank or 3 to 9 in deployments with IP Office users and blank or 3 to 15 in deployments with only centralized users. This field sets the default length for extension numbers for extensions, users, and hunt groups added to the IP Office configuration. Entry of an extension number of a different length will cause an error warning by Manager. The number of digits entered in the **Branch Prefix** field plus the value entered in the **Local Number Length** field must not exceed 15 digits. You have the option to leave the **Local Number Length** field blank.
Proactive Monitoring	Default = 60 seconds. Range = 60 seconds to 100000 seconds. The Enterprise Branch system sends regular SIP OPTIONS messages to the SM line in order to check the status of line. This setting controls the frequency of the messages when the SM line is currently in service. Centralized SIP phones use their own settings.
Monitoring Retries	Default = 1. Range = 0 to 5. The number of times the Enterprise Branch system retrys sending an OPTIONS request to Session Manager before the SM Line is marked out-of-service.
Reactive Monitoring	Default 60 seconds. Range = 10 to 3600 seconds. The Enterprise Branch system sends regular SIP OPTIONS messages to the SM line in order to check the status of line. This setting controls the frequency of the messages when the SM line is currently out of service. Centralized SIP phones use their own settings.
Failback Policy	Default = Auto. This field allows the administrator to choose between an automatic or manual failback policy on the IP Office. In deployments with Centralized phones, this field must be set consistently with the Failback Policy of the phones, which is configured via the Session Manager global settings in System Manager. The options are: • **Auto**: IP Office automatically brings the SM Line to ‘In Service’ status as soon as it detects via the Reactive Monitoring that the Session Manager is reachable • **Manual**: When an SM line is in "Out of Service" state, IP Office does not bring it back to "In Service" status based on automatic detection. IP Office keeps the SM Line in "Out of Service" state until the administrator manually initiates Failback of IP Office from Session Manager.

Related links

Telephony on page 272

Call Log

Navigation: **System Settings** > **System** > **Telephony** > **Call Log**

The system can store a centralized call log for users. Each users' centralized call log can contain up to 30 call records for user calls. When this limit is reached, each new call records replaces the oldest previous record.

On Avaya phones with a fixed **Call Log** or **History** button (1400, 1600, 9500 and 9600 Series), that button can be used to display the user's centralized call log. The centralized call log is also used for M-Series and T-Series phone. The user can use the call log to make calls or to store as a personal speed dial. They can also edit the call log to remove records. The same call log is also used if the user logs into one-X Portal for IP Office.

The centralized call log moves with the user if they log on and off from different phones. This includes if they hot desk within a network.

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

Field	Description		
Default Centralized Call Log On	Default = On. When selected, each user is defaulted to have the system store a call log of their calls. This call log is accessible on the phone when the user is using a phone with a **Call Log** or **History** button. The use of centralized call logging can be enabled/disabled on a per user basis using the setting **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Log** > **Centralized Call Log**.		
Log Missed Calls Answered at Coverage	Default = Off. This setting controls how calls to a user, that are answered by a covering user should be logged in the centralized call log. This option applies for calls answered elsewhere (covered) by pickup, call coverage (call coverage buttons or coverage group), bridged appearance button, user BLF, voicemail, etc.		
	Setting	**Targeted User**	**Covering User**
	Off	Nothing	Answered Call
	On	Missed Call	Answered Call

Table continues…

Field	Description
Log Missed Hunt Group Calls	Default = Off. By default, hunt group calls are not included in any user's centralized call log unless answered by the user. If this option is selected, a separate call log is kept for each hunt group of calls that are not answered by anyone. It includes hunt group calls that go to voicemail. If missed hunt group calls are also being logged, the system stores up to 10 call records for each hunt group. When this limit is reached, new call records replace the oldest record. Within the user call log settings (**Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Log**), the list of hunt groups allows selection of which hunt groups' missed call records should be displayed as part of the user's centralized call log.

Related links

Telephony on page 272

TUI

Navigation: **System Settings** > **System** > **Telephony** > **TUI**

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

Default phone display options:

Use these settings to define the default phone display when feature menus are disabled. Note that for new users, the default phone display options are set to the system default values.

Feature menus can be disabled in one of two ways.

- Set **System Settings** > **System** > **Telephony** > **TUI** > **Features Menu** to **Off**. Set **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **TUI** > **User Setting** to **Same as System**.
- On **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **TUI**, set **User Setting** to **Custom** and set **Features Menu** to **Off**.

Related links

Telephony on page 272

Contact Center

Navigation: **System Settings** > **System** > **Contact Center**

The Contact Center tab contains the user information required by IP Office to synchronize account information with an an Avaya Contact Center Select (ACCS) system. The information is synchronized using the Contact Center Management Application (CCMA). These settings are only used for the deployment of an ACCS system.

This tab is visible on the Server Edition Primary Server and Standard Mode IP500 V2 systems.

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

Field	Description
Contact Center Application	Default = None. The options are: • Avaya Contact Center Select • Avaya IP Office Contact Center
Synchronize to this System	Default = Off. When set to On, the CCMA fields below are enabled.
CCMA Address	Default = Blank Address of the Contact Center Management Application system.
CCMA Username	Default = Blank User name on the Contact Center Management Application system.
CCMA Password	Default = Blank Password on the Contact Center Management Application system.

Related links

System on page 221

Avaya Cloud Services

Navigation: **System Settings** > **System** > **Avaya Cloud Services**

The Avaya Cloud Services tab contains configuration settings for user information synchronization with Avaya Spaces server. IP Office users created for Avaya Equinox™ must be synchronized with the Avaya Spaces server before using Avaya Equinox™ in a cloud environment. User synchronization can be done manually or automatically.

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

Field	Description
Profile Name	Default = None The profile name for the Avaya Cloud Services settings.
Enable Avaya Cloud Account	Default = Selected Enables interoperability. If disabled, synchronization stops but there is no effect on the information that is already synchronized.
Zang URL	Default = `accounts.zang.io` Do not change this value.

Table continues…

Field	Description
Enable Settings File URL Sync	Default = Disabled The options are: • **Enable for IP Office current Node**: The settings file URL synchronization is done for the IP Office system currently being used. • **Enable for all IP Office Nodes**: The settings file URL synchronization is done for all the connected IP Office nodes.
Zang Domain	Default = Blank The company domain registered and verified with Avaya Spaces.
Enable User Synchronization	Default = Not selected If enabled, the IP Office system automatically synchronizes user information with Avaya Spaces.
Avaya Spaces API Key	The API Key from Avaya Spaces. Use the Eye icon to view the key. To obtain the key, log on to the Avaya Spaces account and browse to **Zang Account** > **Manage Companies** > **Company Profile** > **API Key** > **API Key**.
Avaya Spaces Key Secret	The key secret from Avaya Spaces account. Use the Eye icon to view the key. To obtain the key secret, log on to the Avaya Spaces account and browse to **Zang Account** > **Manage Companies** > **Company Profile** > **API Key** > **View/Edit** > **Secret**.

Related links

System on page 221

IP Route

Navigation: **System Settings** > **IP Route**

Additional configuration information

This section provides the **IP Route** field descriptions.

For additional configuration information, see Configuring IP Routes on page 564.

Main content pane

The **IP Route** main content pane lists provisioned IP routes. The contents of the list depends on the filter options selected. Click the icons beside a route to edit or delete.

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

Click **Add/Edit IP Route** to open the Add IP Route window where you can provision a location. When you click **Add/Edit IP Route**, you are prompted to specify a server.

Related links

System Settings on page 194
Add IP Route on page 288

Add IP Route

Navigation: **System Settings** > **IP Route** > **Add/Edit IP Route**

Additional configuration information

For additional configuration information, see Configuring IP Routes on page 564.

For additional configuration information, see Configuring IP Routes on page 564.

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 518.

Configuration settings

These settings are used to setup static IP routes from the system. These are in addition to RIP if RIP is enabled on LAN1 and or LAN2. Up to 100 routes are supported.

For Server Edition, this type of configuration record can be saved as a template and new records created from a template.

Warning:

The process of 'on-boarding' (refer to the IP Office SSL VPN Solutions Guide) may automatically add a static route to an SSL VPN service in the system configuration when the on-boarding file is uploaded to the system. Care should be taken not to delete or amend such a route except when advised to by Avaya.

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

Field	Description
IP Address	The IP address to match for ongoing routing. Any packets meeting the IP Address and IP Mask settings are routed to the entry configured in the **Destination** field. When left blank then an IP Address of 255.255.255.255 (all) is used.
IP Mask	The subnet mask used to mask the IP Address for ongoing route matching. If blank, the mask used is 255.255.255.255 (all). A **0.0.0.0** entry in the IP Address and IP Mask fields routes all packets for which there is no other specific IP Route available. The Default Route option with Services can be used to do this if a blank IP route is not added.
Gateway IP Address	Default = Blank The address of the gateway where packets for the above address are to be sent. If this field is set to **0.0.0.0** or is left blank then all packets are just sent down to the **Destination** specified, not to a specific IP Address. This is normally only used to forward packets to another Router on the local LAN.
Destination	Allows selection of LAN1, LAN2 and any configured Service, Logical LAN or Tunnel (L2TP only).
Metric:	Default = 0 The number of "hops" this route counts as.

Table continues…

Field	Description
Proxy ARP	Default = Off This allows the system to respond on behalf of this IP address when receiving an ARP request.

Related links

IP Route on page 287

Services

Navigation: **System Settings** > **Services**

Main content pane

The **Services** main content pane lists provisioned services. The contents of the list depends on the filter options selected. Click the icons beside a service to edit or delete.

Click **Add/Edit Service**to open the Add Service page where you can provision a service. When you click **Add/Edit Service** you are prompted to specify the server where the service will be configured.

Additional configuration information

For full details on how to configure and administer SSL VPN services, refer to *Deploying Avaya IP Office™ Platform SSL VPN Services*.

Related links

System Settings on page 194
Normal, WAN, or Internet Service on page 289
SSL VPN Service on page 297

Normal, WAN, or Internet Service

Navigation: **System Settings** > **Services** > **Add/Edit Service** > **Normal / WAN / Internet**

Additional configuration information

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 518.

Configuration settings

Services are used to configure the settings required when a user or device on the LAN needs to connect to a off-switch data service such as the Internet or another network. Services can be used when making data connections via trunk or WAN interfaces.

Once a service is created, it can be used as the destination for an IP Route record. One service can also be set as the **Default Service**. That service will then be used for any data traffic received by the system for which no IP Route is specified.

The system supports the following types of service:

- **Normal Service** This type of service should be selected when for example, connecting to an ISP.
- **WAN Service** This type of service is used when creating a WAN link. A User and RAS Service will also be created with the same name. These three records are automatically linked and each open the same form. Note however, that this type of Service cannot be used if the Encrypted Password option is checked. In this case the RAS Service name must match the Account Name. Therefore either create each record manually or create an Intranet Service.
- **Intranet Service** This type of service can be selected to automatically create a User with the same name at the same time. These two records are linked and will each open the same form. The User's password is entered in the Incoming Password field at the bottom on the Service tab. An Intranet Services shares the same configuration tabs as those available to the WAN Service.

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

Field	Description
Service Name	The name of the service. It is recommended that only alphanumeric characters be used.
Account Name	The user name that is used to authenticate the connection. This is provided by the ISP or remote system.
Password	Default = Blank Enter the password that is used to authenticate the connection. This is provided by the ISP or remote system.
Telephone Number	Default = Blank If the connection is to be made via ISDN enter the telephone number to be dialed. This is provided by the ISP or remote system.
Firewall Profile	Default = Internet01 if present, otherwise <None> From the list box select the Firewall Profile that is used to allow/disallow protocols through this Service.
Encrypted Password	Default = Off When enabled the password is authenticated via CHAP (this must also be supported at the remote end). If disabled, PAP is used as the authentication method.
Default Route	Default = Off When enabled this Service is the default route for data packets unless a blank IP Route has been defined in the system IP Routes. A green arrow appears to the left of the Service in the Configuration Tree. Only one Service can be the default route. If disabled, a route must be created under IP Route.
Incoming Password	Default = Blank Shown on WAN and Intranet services. Enter the password that will be used to authenticate the connection from the remote Control Unit. (If this field has appeared because you have created a Service and User of the same name, this is the password you entered in the User's Password field).

Bandwidth

These options give the ability to make ISDN calls between sites only when there is data to be sent or sufficient data to warrant an additional call. The calls are made automatically without the users being aware of when calls begin or end. Using ISDN it is possible to establish a data call and be passing data in less that a second.

Note:

The system will check **Minimum Call Time** first, then **Idle Period**, then the **Active Idle Period**.

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

Field	Description
Minimum No of Channels	Default = 1. Range = 1 to 30. Defines the number of channels used to connect for an outgoing connection. The initial channel must be established and stable, before further calls are made.
Maximum No of Channels	Default = 1. Range = 1 to 30. Defines the maximum number of channels to can be used. This field should contain a value equal to or greater than the Minimum Channels field.
Extra BW Threshold	Default = 50%. Range = 0 to 100%. Defines the utilization threshold at which extra channels are connected. The value entered is a %. The % utilization is calculated over the total number of channels in use at any time, which may be one, two etc. For example, if **Minimum Channels** set to 1, **Maximum Channels** set to 2 and **Extra Bandwidth** set to 50 - once 50% of first channel has been used the second channel is connected.
Reduce BW Threshold	Default = 10%. Range = 0 to 100%. Defines the utilization threshold at which additional channels are disconnected. The value entered is a %. Additional calls are only dropped when the % utilization, calculated over the total number of channels in use, falls below the % value set for a time period defined by the Service-Idle Time. The last call (calls - if Minimum Calls is greater than 1) to the Service is only dropped if the % utilization falls to 0, for a time period defined by the Service-Idle Time. Only used when 2 or more channels are set above. For example, if Minimum Channels set to 1, Maximum Channels set to 2 and Reduce Bandwidth is set to 10 - once the usage of the 2 channels drops to 10% the number of channels used is 1.
Callback Telephone Number	Default = Blank The number that is given to the remote service, via BAP, which the remote Control Unit then dials to allow the bandwidth to be increased. Incoming Call routing and RAS Services must be appropriately configured.

Table continues…

Field	Description
Idle Period (secs)	Default = 10 seconds. Range = 0 to 999999 seconds. The time period, in seconds, required to expire after the line has gone idle. At this point the call is considered inactive and is completely closed. For example, the 'Idle Period' is set to X seconds. X seconds before the 'Active Idle Period' timeouts the Control Unit checks the packets being transmitted/received, if there is nothing then at the end of the 'Active Idle Period' the session is closed & the line is dropped. If there are some packets being transmitted or received then the line stays up. After the 'Active Idle Period' has timed out the system performs the same check every X seconds, until there are no packets being transferred and the session is closed and the line dropped.
Active Idle Period (secs):	Default = 180 seconds. Range = 0 to 999999 seconds. Sets the time period during which time the line has gone idle but there are still active sessions in progress (for example an FTP is in process, but not actually passing data at the moment). Only after this timeout will call be dropped. For example, you are downloading a file from your PC and for some reason the other end has stopped responding, (the remote site may have a problem etc.) the line is idle, not down, no data is being transmitted/ received but the file download session is still active. After the set time period of being in this state the line will drop and the sessions close. You may receive a remote server timeout error on your PC in the Browser/FTP client you were using.
Minimum Call Time (secs):	Default = 60 seconds. Range = 0 to 999999 seconds. Sets the minimum time that a call is held up after initial connection. This is useful if you pay a minimum call charge every time a call is made, no matter the actual length of the call. The minimum call time should be set to match that provided by the line provider.
Extra Bandwidth Mode	Default = Incoming Outgoing Defines the mode of operation used to increases bandwidth to the initial call to the remote Service. The options are: • **Outgoing Only** Bandwidth is added by making outgoing calls. • **Incoming Only** Bandwidth is added by the remote service calling back on the BACP number (assuming that BACP is successfully negotiated). • **Outgoing Incoming** Uses both methods but bandwidth is first added using outgoing calls. • **Incoming Outgoing** Uses both methods but bandwidth is first added using incoming BACP calls.

IP

The fields in this tab are used to configure network addressing for the services you are running. Depending on how your network is configured, the use of Network Address Translation (NAT) may be required.

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

Field	Description
IP Address	Default = 0.0.0.0 (address assigned by ISP) An address should only be entered here if a specific IP address and mask have been provided by the Service Provider. Note that if the address is in a different domain from the system then NAT is automatically enabled
IP Mask	Default = 0.0.0.0 (use NAT) Enter the IP Mask associated with the IP Address if an address is entered.
Primary Transfer IP Address	Default = 0.0.0.0 (No transfer) This address acts as a primary address for incoming IP traffic. All incoming IP packets without a session are translated to this address. This would normally be set to the local mail or web server address. For control units supporting a LAN1 and LAN2, the primary transfer address for each LAN can be set through the **System Settings** > **System** > **LAN1** and **System Settings** > **System** > **LAN2** tabs.
RIP Mode	Default = None Routing Information Protocol (RIP) is a method by which network routers can exchange information about device locations and routes. RIP can be used within small networks to allow dynamic route configuration as opposed to static configuration using. The options are: • **None** The LAN does not listen to or send RIP messages. • **Listen Only (Passive)** Listen to RIP-1 and RIP-2 messages in order to learn RIP routes on the network. • **RIP1** Listen to RIP-1 and RIP-2 messages and send RIP-1 responses as a sub-network broadcast. • **RIP2 Broadcast (RIP1 Compatibility)** Listen to RIP-1 and RIP-2 messages and send RIP-2 responses as a sub-network broadcast. • **RIP2 Multicast** Listen to RIP-1 and RIP-2 messages and send RIP-2 responses to the RIP-2 multicast address.
Request DNS	Default = Off. When selected, DNS information is obtained from the service provider. To use this, the DNS Server addresses set in the system configuration (System | DNS) should be blank. The PC making the DNS request should have the system set as its DNS Server. For DHCP clients the system will provide its own address as the DNS server.
Forward Multicast Messages	Default = On. By default this option is on. Multicasting allows WAN bandwidth to be maximized through the reduction of traffic that needs to be passed between sites.

Autoconnect

These settings enable you to set up automatic connections to the specified Service.

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

Field	Description
Auto Connect Interval (mins):	Default = 0 (disabled). Range = 0 to 99999 minutes. This field defines how often this Service will automatically be called ("polled"). For example setting 60 means the system will call this Service every hour in the absence of any normally generated call (this timer is reset for every call; therefore if the service is already connected, then no additional calls are made). This is ideal for SMTP Mail polling from Internet Service Providers.
Auto Connect Time Profile	Default = <None> Allows the selection of any configured Time Profiles. The selected profile controls the time period during which automatic connections to the service are made. It does NOT mean that connection to that service is barred outside of these hours. For example, if a time profile called "Working Hours" is selected, where the profile is defined to be 9:00AM to 6:00PM Monday to Friday, then automatic connection to the service will not be made unless its within the defined profile. If there is an existing connection to the service at 9:00AM, then the connection will continue. If there is no connection, then an automatic connection will be made at 9:00AM.

Quota

Quotas are associated with outgoing calls, they place a time limit on calls to a particular IP Service. This avoids excessive call charges when perhaps something changes on your network and call frequency increases unintentionally.

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

Field	Description
Quota Time (mins)	Default = 240 minutes. Range = 0 to 99999 minutes. Defines the number of minutes used in the quota. When the quota time is used up no further data can be passed to this service. This feature is useful to stop things like an internet game keeping a call to your ISP open for a long period. **Warning:** Setting a value here without selecting a Quota period below will stop all further calls after the Quota Time has expired.
Quota:	Default = Daily. Range = None, Daily, Weekly or Monthly Sets the period during which the quota is applied. For example, if the **Quota Time** is 60 minutes and the **Quota** is set to **Daily**, then the maximum total connect time during any day is 60 minutes. Any time beyond this will cause the system to close the service and prevent any further calls to this service. To disable quotas select **None** and set a **Quota Time** of zero. **Note:** The ClearQuota feature can be used to create short codes to refresh the quota time.

PPP

These settings enable you to configure Point to Point Protocol (PPP) in relation to this particular service. PPP is a protocol for communication between two computers using a Serial interface.

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

Field	Description
Chap Challenge Interval (secs)	Default = 0 (disabled). Range = 0 to 99999 seconds. The period between CHAP challenges. Blank or 0 disables repeated challenges. Some software such as Windows 95 DUN does not support repeated CHAP challenges.
Bi-Directional Chap	Default =Off.
Header Compression	Default = None selected Enables the negotiation and use of IP Header Compression. Supported modes are IPHC and VJ. IPHC should be used on WAN links.
PPP Compression Mode	Default = MPPC Enables the negotiate and use of compression. Do not use on VoIP WAN links. The options are: • **Disable** Do not use or attempt to use compression. • **StacLZS** Attempt to use STAC compression (Mode 3, sequence check mode). • **MPPC** Attempt to use MPPC compression. Useful for NT Servers.
PPP Callback Mode	Default = Disabled. The options are: • **Disable** Callback is not enabled • **LCP** (Link Control Protocol) After authentication the incoming call is dropped and an outgoing call to the number configured in the Service is made to re-establish the link. • **Callback CP** (Microsoft's Callback Control Protocol) After acceptance from both ends the incoming call is dropped and an outgoing call to the number configured in the Service is made to re-establish the link. • **Extended CBCP** (Extended Callback Control Protocol) Similar to Callback CP except the Microsoft application at the remote end prompts for a telephone number. An outgoing call is then made to that number to re-establish the link.

Table continues…

Field	Description
PPP Access Mode	Default = Digital64 Sets the protocol, line speed and connection request type used when making outgoing calls. Incoming calls are automatically handled (see RAS services). The options are: • **Digital64** Protocol set to Sync PPP, rate 64000 bps, call presented to local exchange as a "Data Call". • **Digital56** As above but rate 56000 bps. • **Voice56** As above but call is presented to local exchange as a "Voice Call". • **V120** Protocol set to Async PPP, rate V.120, call presented to local exchange as a "Data Call". This mode runs at up to 64K per channel but has a higher Protocol overhead than pure 64K operation. Used for some bulletin board systems as it allows the destination end to run at a different asynchronous speed to the calling end. • **V110** Protocol is set to Async PPP, rate V.110. This runs at 9600 bps, call is presented to local exchange as a "Data Call". It is ideal for some bulletin boards. • **Modem** Allows Asynchronous PPP to run over an auto-adapting Modem to a service provider (requires a Modem2 card in the main unit)
Data Pkt. Size	Default = 0. Range = 0 to 2048. Sets the size limit for the Maximum Transmissible Unit.
BACP	Default = Off. Enables the negotiation and use of BACP/BCP protocols. These are used to control the addition of B channels to increase bandwidth.
Incoming traffic does not keep link up	Default = On. When enabled, the link is not kept up for incoming traffic only.
Multilink/QoS	Default = Off. Enables the negotiation and use of Multilink protocol (MPPC) on links into this Service. Multilink must be enabled if there is more than one channel that is allowed to be Bundled/ Multilinked to this RAS Service.

Fallback

These settings allow you to set up a fallback for the Service. For example, you may wish to connect to your ISP during working hours and at other times take advantage of varying call charges from an alternative carrier. You could therefore set up one Service to connect during peak times and another to act as fallback during the cheaper period.

You need to create an additional Service to be used during the cheaper period and select this service from the Fallback Service list box (open the Service form and select the Fallback tab).

If the original Service is to be used during specific hours and the Fallback Service to be used outside of these hours, a Time Profile can be created. Select this Time Profile from the Time Profile list box. At the set time the original Service goes into Fallback and the Fallback Service is used.

A Service can also be put into Fallback manually using short codes, for example:

Put the service "Internet" into fallback:

- **Short Code**: *85
- **Telephone Number**: "Internet"
- **Line Group ID**: 0
- **Feature**: SetHuntGroupNightService

Take the service "Internet" out of fallback:

- **Short Code**: *86
- **Telephone Number**: "Internet"
- **Line Group ID**: 0
- **Feature**: ClearHuntGroupNightService

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

Field	Description
In Fallback	Default = Off. This option indicates whether the Service is in Fallback or not. A service can be set into fallback using this setting. Alternatively a service can be set into fallback using a time profile or short codes.
Time profile	Default = <None> (No automatic fallback) Select the time profile you wish to use for the service. The time profile should be set up for the hours that you wish this service to be operational, out of these hours the Fallback Service is used.
Fallback Service	Default = <None> Select the service that is used when this service is in fallback.

Dial In

Only available for WAN and Intranet Services. This tab is used to define a WAN connection.

To define a WAN connection, click Add and enter `WAN` if the service is being routed via a WAN port on a WAN3 expansion module.

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

Related links

Services on page 289

SSL VPN Service

Navigation: **System Settings** > **Services** > **Add/Edit Service** > **SSL VPN**

The SSL VPN service provides secure tunneling between the Avaya IP Office hardware installed at a customer site and a remote Avaya VPN Gateway (AVG). This secure tunnel allows support

personnel to offer remote management services to customers, such as fault management, monitoring, and administration.

For full details on how to configure and administer SSL VPN services, refer to *Deploying Avaya IP Office™ Platform SSL VPN Services*.

For Server Edition, this type of configuration record can be saved as a template and new records created from a template.

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

Field	Description
Service Name	Enter a name for the SSL VPN service.
Account Name	Enter the SSL VPN service account name. This account name is used for authenticating the SSL VPN service when connecting with the Avaya VPN Gateway (AVG).
Account Password	Enter the password for the SSL VPN service account.
Confirm Password	Confirm the password for the SSL VPN service account.
Server Address	Enter the address of the VPN gateway. The address can be a fully qualified domain name or an IPv4 address
Server Type	Default = AVG. This field is fixed to **AVG** (Avaya VPN Gateway).
Server Port Number	Default = 443. Select a port number.

Session

Field	Description
Session Mode	Default = Always On. This setting is greyed out and cannot be adjusted.
Preferred Data Transport Protocol	Default = UDP. This is the protocol used by the SSL VPN service for data transport. Only **TCP** is supported. If you select **UDP** as the protocol when you configure the connection, UDP displays in this field but the SSL VPN service falls back to TCP.
Heartbeat Interval	Default = 30 seconds. Range = 1 to 600 seconds. Enter the length of the interval between heartbeat messages, in seconds. The default value is 30 seconds.
Heartbeat Retries	Default = 4. Range = 1 to 10. Enter the number of unacknowledged heartbeat messages that IP Office sends to AVG before determining that AVG is not responsive. When this number of consecutive heartbeat messages is reached and AVG has not acknowledged them, IP Office ends the connection.
Keepalive Interval	Default = 10 seconds. Range = 0 (Disabled) to 600 seconds. Not used for **TCP** connections. Keepalive messages are sent over the UDP data transport channel to prevent sessions in network routers from timing out.

Table continues…

Field	Description
Reconnection Interval on Failure	Default = 60 seconds. Range = 1 to 600 seconds. The interval the system waits attempting to re-establish a connection with the AVG. The interval begins when the SSL VPN tunnel is in-service and makes an unsuccessful attempt to connect with the AVG, or when the connection with the AVG is lost. The default is 60 seconds.

NAPT

The Network Address Port Translation (NAPT) rules are part of SSL VPN configuration. NAPT rules allow a support service provider to remotely access LAN devices located on a private IP Office network. You can configure each SSL VPN service instance with a unique set of NAPT rules. You can configure up to 64 rules.

Field	Description		
Application	Default = Blank Defines the communication application used to connect to the LAN device through the SSL VPN tunnel. When you select an application, the **Protocol** and **Port Number** fields are filled with the default values. The drop-down **Application** selector options and the associated default values are:		
	Application	**Protocol**	**External and Internal Port Number**
	Custom	TCP	0
	VMPro	TCP	50791
	OneXPortal	TCP	8080
	SSH	TCP	22
	TELNET	TCP	23
	RDP	TCP	3389
	WebControl	TCP	7070
Protocol	Default = TCP The protocol used by the application. The options are **TCP** and **UDP**.		
External Port Number	Default = the default port number for the application. Range = 0 to 65535 Defines the port number used by the application to connect from the external network to the LAN device in the customer private network.		
Internal IP address	Default = Blank. The IP address of the LAN device in the customer network.		
Internal Port Number	Default = the default port number for the application. Range = 0 to 65535 Defines the port number used by the application to connect to the LAN device in the customer private network.		

Fallback

Field	Description
In Fallback	Default = Off. This setting is used to indicate whether the SSL VPN service is in use or not. • To configure the service without establishing an SSL VPN connection, or to disable an SSL VPN connection, select this option. • To enable the service and establish an SSL VPN connection, de-select this option. • The **Set Hunt Group Night Service** and **Clear Hunt Group Night Service** short code and button features can be used to switch an SSL VPN service off or on respectively. The service is indicated by setting the service name as the telephone number or action data. Do not use quotation marks.

Related links

Services on page 289

Alternate Route Selection

Navigation: **System Settings** > **Alternate Route Selection**

Main content pane

The **Alternate Route Selection** main content pane lists provisioned routes. The contents of the list depends on the filter options selected. Click the icons beside an route to edit or delete.

Click **Add/Edit Alternate Route** to open the Create Alternate Route page where you can provision a location. When you click **Add/Edit Alternate Route**, you are prompted to specify a server.

Related links

System Settings on page 194
Add Alternate Route on page 300

Add Alternate Route

Navigation: **System Settings** > **Alternate Route Selection** > **Add/Edit Alternate Route**

Additional configuration information

See Configuring ARS on page 552.

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 518.

Configuration settings

Each ARS form contains short codes which are used to match the result of the short code that triggered use of the ARS form, ie. the Telephone Number resulting from the short code is used rather than the original number dialed by the user.

For Server Edition, this type of configuration record can be saved as a template and new records created from a template.

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

Field	Description
ARS Route ID	The default value is automatically assigned. Range = 0 to 99999. For most deployments, do not edit this field. For those conditions where it is necessary to edit this field, the value must be unique within ARS and within the line Outbound Group IDs.
Route Name	Default = Blank. Range = Up to 15 characters. The name is used for reference and is displayed in other areas when selecting which ARS to use.
Dial Delay Time	Default = System. Range = 1 to 30 seconds. This settings defines how long ARS should wait for further dialing digits before assuming that dialing is complete and looking for a short code match against the ARS form short codes. When set to **System**, the system setting **System Settings** > **System** > **Telephony** > **Dial Delay Time** is used.

Table continues…

Field	Description
Secondary Dial Tone	Defaults = Off. When on, this setting instructs the system to play secondary dial tone to the user. The tone used is set by the field below. The tone used is set as either **System Tone** (normal dial tone) or **Network Tone** (secondary dial tone). Both tone types are generated by the system in accordance with the system specific locale setting. Note that in some locales normal dial tone and secondary dial tone are the same. When **Secondary Dial Tone** is selected, the ARS form will return tone until it receives digits with which it can begin short code matching. Those digits can be the result of user dialing or digits passed by the short code which invoked the ARS form. For example with the following system short codes: In this example, the 9 is stripped from the dialed number and is not part of the telephone number passed to the ARS form. So in this case secondary dial tone is given until the user dials another digit or dialing times out. • **Code**: 9N • **Telephone Number**: N • **Line Group ID**: 50 Main In this example, the dialed 9 is included in the telephone number passed to the ARS form. This will inhibit the use of secondary dial tone even if secondary dial tone is selected on the ARS form. • **Code**: 9N • **Telephone Number**: 9N • **Line Group ID**: 50 Main
Check User Call Barring	Default = Off If enabled, the dialing user's **Outgoing Call Bar** setting and any user short codes set to the function **Barred** are checked to see whether they are appropriate and should be used to bar the call.
Description	Default = Blank. Maximum 31 characters. Use this field to enter a description of this configuration.
In Service:	Default = On This field is used to indicate whether the ARS form is in or out of service. When out of service, calls are rerouted to the ARS form selected in the **Out of Service Route** field. Short codes can be used to take an ARS form in and out of service. This is done using the short code features Disable ARS Form and Enable ARS Form and entering the ARS Route ID as the short code **Telephone Number** value.
Out of Service Route	Default = None. This is the alternate ARS form used to route calls when this ARS form is not in service.

Table continues…

Field	Description
Time Profile	Default = None. Use of a ARS form can be controlled by an associate time profile. Outside the hours defined within the time profile, calls are rerouted to an alternate ARS form specified in the Out of Hours Route drop-down. Note that the Time Profile field cannot be set until an Out of Hours Route is selected.
Out of Hours Route	Default = None. This is the alternate ARS form used to route calls outside the hours defined within the Time Profile selected above.
Short Codes	Short codes within the ARS form are matched against the "Telephone Number" output by the short code that routed the call to ARS. The system then looks for another match using the short codes with the ARS form. Only short codes using the following features are supported within ARS: **Dial**, **Dial Emergency**, **Dial Speech**, **Dial 56K**, **Dial64K**, **Dial3K1**, **DialVideo**, **DialV110**, **DialV120** and **Busy**. Multiple short codes with the same **Code** field can be entered so long as they have differing **Telephone Number** and or **Line Group ID** settings. In this case when a match occurs the system will use the first match that points to a route which is available.
Alternate Route Priority	Default = 3. Range = 1 (low) to 5 (high). If the routes specified by this form are not available and an **Alternate Route** has been specified, that route will be used if the users priority is equal to or higher than the value set here. User priority is set through the **Call Management** > **Users** > **Add/Edit Users** > **User** form and by default is **5**. If the users priority is lower than this value, the **Alternate Route Wait Time** is applied. This field is grayed out and not used if an ARS form has not been selected in the **Alternate Route** field. If the caller's dialing matches a short code set to the **Barred** function, the call remains at that short code and is not escalated in any way.
Alternate Route Wait Time	Default = 30 seconds. Range = Off, 5 to 60 seconds. If the routes specified by this form are not available and an **Alternate Route** has been specified, users with insufficient priority to use the alternate route immediately must wait for the period defined by this value. During the wait the user hears camp on tone. If during that period a route becomes available it is used. This field is grayed out and not used if an ARS form has not been selected in the Alternate Route field.
Alternate Route	Default = None. This field is used when the route or routes specified by the short codes are not available. The routes it specifies are checked in addition to those in this ARS form and the first route to become available is used.

Cause Codes and ARS

ARS routing to digital trunks can be affected by signalling from the trunk.

The following cause codes cause ARS to no longer target the line group (unless it is specified by an alternate ARS route). The response to cause codes received from the line is as follows.

Code	Cause Code
1	Unallocated Number.
2	No route to specific transit network/(5ESS) Calling party off hold.
3	No route to destination./(5ESS) Calling party dropped while on hold.
4	Send special information tone/(NI-2) Vacant Code.
5	Misdialed trunk prefix.
8	Preemption/(NI-2) Prefix 0 dialed in error.
9	Preemption, cct reserved/ (NI-2) Prefix 1 dialed in error.
10	(NI-2) Prefix 1 not dialed.
11	(NI-2) Excessive digits received call proceeding.
22	Number Changed.
28	Invalid Format Number.
29	Facility Rejected.
50	Requested Facility Not Subscribed.
52	Outgoing calls barred.
57	Bearer Capability Not Authorized.
63	Service or Option Unavailable.
65	Bearer Capability Not Implemented.
66	Channel Type Not Implemented.
69	Requested Facility Not Implemented.
70	Only Restricted Digital Information Bearer Capability Is Available.
79	Service Or Option Not Implemented.
88	Incompatible.
91	Invalid Transit Network Selection.
95	Invalid Message.
96	Missing Mandatory IE.
97	Message Type Nonexistent Or Not Implemented.
98	Message Not Implemented.
99	Parameter Not Implemented.
100	Invalid IE Contents.
101	Msg Not Compatible.
111	Protocol Error.
127	Interworking Unspecified.

Stop ARS The following cause codes stop ARS targeting completely.

Code	Cause Code
17	Busy.
21	Call Rejected.
27	Destination Out of Order.

No Affect All other cause codes do not affect ARS operation.

Related links

Alternate Route Selection on page 300

Account Code

Navigation: **System Settings** > **Account Code**

Additional configuration information

This section provides the **Account Code** field descriptions.

For additional configuration information, see Configuring Account Codes on page 596.

Main content pane

The **Account Code** main content pane lists provisioned account codes. The contents of the list depends on the filter options selected. Click the icons beside a record to edit or delete.

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

Click **Add/Edit Account Code** to open the Create Account Code window where you can provision an account code. When you click **Add/Edit Account Code**, you are prompted to specify if the account code will be a common object or specific to a server.

Related links

System Settings on page 194
Add Account Code on page 305

Add Account Code

Navigation: **System Settings** > **Account Code** > **Add/Edit Account Code**

Account codes are commonly used to control cost allocation and out-going call restriction. The account code used on a call is included in the call information output by the system's call log. Incoming calls can also trigger account codes automatically by matching the Caller ID stored with the account code.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Once a call has been completed using an account code, the account code information is removed from the user's call information. This means that re-dial functions will not re-enter the account code. The maximum recommended number of accounts codes is 1000.

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

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Descriptions
Account Code	Enter the account code required. It can also include wildcards; **?** matches a single digit and ***** matches any digits.
Caller ID	A caller ID can be entered and used to automatically assign an account code to calls made to or received from caller ID.

Voice Recording

These settings are used to activate the automatic recording of external calls when the account code is entered at the start of the call.

Call recording requires Voicemail Pro to be installed and running. Call recording also requires available conference resources similar to a 3-way conference.

Note the following:

- Calls to and from IP devices, including those using Direct media, can be recorded.
- Calls parked or held pause recording until the unparked or taken off hold (does not apply to SIP terminals).
- Recording is stopped if:
  - User recording stops if the call is transferred to another user.
  - User account code recording stops if the call is transferred to another user.
  - Hunt group recording stops if the call is transferred to another user who is not a member of the hunt group.
  - Incoming call route recording continues for the duration of the call on the system.

The destination mailbox for the recording can be specified.

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

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Description
Record Outbound	Default = None Select whether automatic recording of outgoing calls is enabled. The Auto Record Calls option sets whether just external calls or external and internal calls are included. The options are: • **None**: Do not automatically record calls. • **On**: Record the call if possible. If not possible to record, allow the call to continue. • **Mandatory**: Record the call if possible. If not possible to record, block the call and return busy tone. • **Percentages of calls**: Record a selected percentages of the calls.
Record Time Profile	Default = <None> (Any time) Used to select a time profile during which automatic call recording of outgoing calls is applied. If no profile is selected, automatic recording of outgoing calls is active at all times.
Recording (Auto)	Default = Mailbox Sets the destination for automatically triggered recordings. The options are: • **Mailbox** This option sets the destination for the recording to be a selected user or hunt group mailbox. The adjacent drop down list is used to select the mailbox. • **Voice Recording Library**: This options set the destination for the recording to be a VRL folder on the voicemail server. The ContactStore application polls that folder and collects waiting recordings which it then places in its own archive. Recording is still done by the Voicemail Pro. • **Voice Recording Library Authenticated**: This option is similar to Voice Recording Library above but instructs the voicemail server to create an authenticated recording. If the file contents are changed, the file is invalidated though it can still be played. This option is not currently supported with Linux based systems.

Related links

Account Code on page 305

Lines

Navigation: **System Settings** > **Line**

Main content pane

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

Click **Add/Edit Trunk Line** to select a line type to add and to specify the system where the line will be added.

Related links

System Settings on page 194

Add Trunk Line on page 308
Configuring IP Office using the Dashboard on page 38
Configuration dashboard on page 37

Add Trunk Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line**

The line settings shown in the system configuration will change according to the types of trunk cards installed in the control unit or added using external expansion modules.

Warning:

Changing Trunk Cards Changing the trunk card installed in an control unit will result in line settings for both the previous trunk card and the currently installed trunk card. In order to change the trunk card type in a particular card slot, the configuration must be defaulted. This does not apply if replacing an existing card with one of a higher capacity or fitting a trunk card into a previously unused slot.

Trunk Incoming Call Routing

Each trunk type can be categorized as either an external trunk or internal trunk. The trunk type affects how the system routes calls received on that trunk and the routing of calls to the trunk.

	External Trunks	Internal Trunks
Trunk Types	**Analog trunks** **T1 Robbed Bit** **E1R2** **ISDN BRI** (excluding So) **ISDN PRI T1** **ISDN PRI E1** **SIP**	**QSIG** (T1, E1 or H.323) **BRI So** **H.323** **SCN** **SES** **IP Office Line**
Incoming Calls Routed by	All incoming calls are routed by comparison of call details for matches within the system Incoming Call Routes. Line short codes are not used.	Incoming calls are routed by looking for a match to the incoming digits in the following order: • Extension number. • Trunk short codes (excluding ? short code). • System short codes (excluding ? short code). • Trunk ? short code. • System ? short code.

Line Groups

Each system trunk (or in some cases individual trunk channels) can be configured with an **Incoming Group ID** and an **Outgoing Group ID**. These group IDs are used as follows:

- Incoming Call Routes For incoming calls on external trunks, the Incoming Group ID of the trunk is one of the factors used to match the call to one of the configured incoming call routes.
- Short Codes - Routing Outgoing Calls For dialing which matches a short code set to a **Dial** feature, the short codes **Line Group ID** can indicate either an ARS form or to use a trunk from set to the same **Outgoing Group ID**. If the call is routed to an ARS form, the short codes in the ARS form will specify the trunks to use by matching **Outgoing Group ID**.

Removing Unused Trunks

In cases where a trunk card is installed but the trunk is not physically connected, it is important to ensure that the trunk is disabled in the configuration. This can be done on most trunks using by setting the line's **Admin** setting to **Out of Service**.

This is especially important with analog trunks. Failure to do this may cause the system to attempt to present outgoing calls to that trunk. Similarly, where the number of channels subscribed is less than those supportable by the trunk type, the unsubscribed channels should be disabled.

Clock Quality

Calls between systems using digital trunks (for example E1, E1R2, T1 PRI and BRI) require an common clock signal. The system will try to obtain this clock signal from an exchange through one of its digital trunks. This is done by setting the Clock Quality setting of that Line to Network. If there are multiple trunks to public exchanges, another trunk can be set as Fallback should the primary clock signal fail. Other trunks should be set as Unsuitable.

Related links

Lines on page 307
SIP Line on page 309
H.323 Line on page 343
IP Office Line on page 350
SIP DECT Line on page 360
IP DECT on page 362
SM Line on page 368
Analog Line on page 377
BRI Line on page 386
PRI Trunks on page 391

SIP Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line**

IP Office supports SIP voice calls through the addition of SIP lines to the system configuration. This approach allows users with non-SIP phones to make and receive SIP calls.

Deleting a SIP line requires a “merge with service disruption”. When the configuration file is sent to the system, the SIP trunk is restarted and all calls on the line are dropped.

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 518.

Related links

Add Trunk Line on page 308
SIP Line on page 310
SIP Line I Transport on page 314
Call Details on page 319
SIP Line VoIP on page 332
T.38 Fax on page 336
SIP Line Credentials on page 337
SIP Line Advanced on page 338
SIP Line Engineering on page 343

SIP Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Line**

Configuration Settings

These settings are mergeable with the exception of the **Line Number** setting. Changing the **Line Number** setting requires a “merge with service disruption”. When the configuration file is sent to the system, the SIP trunk is restarted and all calls on the line are dropped.

Offline editing is not required.

Field	Description
Line Number	Default = Auto-filled. Range = 1 to 249 *(IP500 V2)*/349 *(Server Edition)*. Enter the line number that you wish. Note that this must be unique. On IP500 V2 systems, line numbers 1 to 16 are reserved for internal hardware.

Table continues…

Field	Description
ITSP Domain Name	Default = Blank. This field is used to specify the default host part of the SIP URI in the From, To, and R-URI fields for outgoing calls. For example, in the SIP URI `name@example.com`, the host part of the URI is `example.com`. When empty, the default host is provided by the **SIP Line** > **SIP Transport** > **ITSP Proxy Address** field value. If multiple addresses are defined in the **ITSP Proxy Address** field, then this field must be defined. For the user making the call, the user part of the From SIP URI is determined by the settings of the SIP URI channel record being used to route the call (see **SIP Line** > **SIP URI** > **Local URI**). This will use one of the following: • a specific name entered in Local URI field of the channel record. • or specify using the primary or secondary authentication name set for the line below. • or specify using the SIP Name set for the user making the call (**Call Management** > **Users** > **Add/Edit Users** > **SIP** > **SIP Name**). For the destination of the call, the user part of the To and R-URI fields are determined by dial short codes of the form 9N/N"@example.com" where N is the user part of the SIP URI and "@example.com" is optional and can be used to override the host part of the To and R-URI.
Local Domain Name	Default = Blank. An IP address or SIP domain name as required by the service provider. When configured, the **Local Domain Name** value is used in • the **From** and **Contact** headers • the **PAI header**, when the setting **SIP Line** > **SIP Advanced** > **Use Domain for PAI** is checked • the **Diversion** header If both the **ITSP Domain Name** and the **Local Domain Name** are configured, then **Local Domain** takes precedence. **Local Domain Name** is not used in the **Remote Party ID** header.
URI	Default = SIP. When SIP or SIPS is selected in the drop-down box, the SIP URI format is used (for example, name@example.com). When **Tel** is selected in the drop-down box, the Tel URI format is used (for example, +1-425-555-4567). This affects the From field of outgoing calls. The To field for outgoing calls will always use the format specified by the short codes used for outgoing call routing. Recommendation: When SIP Secured URI is required, the URI Type should be set to SIPS. SIPS can be used only when Layer 4 Protocol is set to TLS.

Table continues…

Field	Description
Location	Default = Cloud. Specify a location to associate the line with a physical location. Associating a line with a location: • Allows emergency services to identify the source of an emergency call. • Allows you to configure call admission control settings for the location. The drop down list contains all locations that have been defined in the **System Settings** > **Locations** form.
Prefix	Default = Blank. This prefix is removed from the called number on outgoing calls if present.
National Prefix	Default = 0. This prefix is added to calls identified as not being international.
International Prefix	Default = 00. This prefix is added to calls identified as not being national.
Country Code	Default = Blank. Set to match the local country code of the system location.
Name Priority	Default = System Default. For SIP trunks, the caller name displayed on an extension can either be that supplied by the trunk or one obtained by checking for a number match in the extension user's personal directory and the system directory. This setting determines which method is used by the line. The options are: • **System Default**: Use the system setting **System Settings** > **System** > **Telephony** > **Default Name Priority**. • **Favor Trunk**: Display the name provided by the trunk. For example, the trunk may be configured to provide the calling number or the name of the caller. The system should display the caller information as it is provided by the trunk. If the trunk does not provide a name, the system uses the **Favor Directory** method. • **Favor Directory**: Search for a number match in the extension user's personal directory and then in the system directory. The first match is used and overrides the name provided by the SIP line. If no match is found, the name provided by the line, if any, is used.
Description	Default = Blank. Maximum 31 characters. Use this field to enter a description of this configuration.

Table continues…

Field	Description
Network Type	Default = Public. This option is available if **System Settings** > **System** > **Telephony** > **Restrict Network Interconnect** is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
In Service	Default = On. When this field is not selected, the SIP trunk is unregistered and not available to incoming and outgoing calls.
Check OOS	Default = On. If enabled, the system will regularly check if the trunk is in service using the methods listed below. Checking that SIP trunks are in service ensures that outgoing call routing is not delayed waiting for response on a SIP trunk that is not currently usable. For UDP and TCP trunks, OPTIONS message are regularly sent. If no reply to an OPTIONS message is received the trunk is taken out of service. For trunks using DNS, if the IP address is not resolved or the DNS resolution has expired, the trunk is taken out of service.
Session Timers	
Refresh Method	Default = Auto. The options are: • **Auto** • **Reinvite** • **Update** When **Auto** is selected, if UPDATE is in the Allow: header from the far SIP endpoint, then it is used. Otherwise INVITE is used.
Timer (seconds)	Default = On Demand. Range = 90 to 64800 This field specifies the session expiry time. At the half way point of the expiry time, a session refresh message is sent. When set to **On Demand**, IP Office will not send a session refresh message but will respond to them.

Table continues…

Field	Description
Redirect and Transfer Redirection and blind transfer are configured separately. By default, they are disabled. A supervised transfer occurs when a consultation call is made and the REFER contains a Replaces: header indicating the CallID of another call leg which the REFERing agent has already initiated with the REFER target. **Note:** Do not change these settings unless directed to by the SIP service provider.	
Incoming Supervised REFER	Default = Auto. Determines if IP Office will accept a REFER being sent by the far end. The options are: • **Always**: Always accepted. • **Auto**: If the far end does not advertise REFER support in the Allow: header of the OPTIONS responses, then IP Office will reject a REFER from that endpoint. • **Never**: Never accepted.
Outgoing Supervised REFER	Default = Auto. Determines if IP Office will attempt to use the REFER mechanism to transfer a party to a call leg which IP Office has already initiated so that it can include the CallID in a Replaces: header. The options are: • **Always**: Always use REFER. • **Auto**: Use the Allow: header of the OPTIONS response to determine if the endpoint supports REFER. • **Never**: Never use REFER.
Send 302 Moved Temporarily	Default = Off. A SIP response code used for redirecting an unanswered incoming call. It is a response to the INVITE, and cannot be used after the 200 OK has been sent as a response to the INVITE.
Outgoing Blind REFER	Default = Off. When enabled, a user, voicemail system or IVR can transfer a call by sending a REFER to an endpoint that has not set up a second call. In this case, there is no Replaces: header because there is no CallID to replace the current one. This directs the far end to perform the transfer by initiating the new call and release the current call with IP Office.

Related links

SIP Line on page 309

SIP Line I Transport

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Transport**

Behavior during Service unavailable

A proxy server is considered Active once the system has received a response to an INVITE, REGISTER or OPTIONS.

In the case of the proxy server responding with 503 - Service Unavailable, it should be considered Active - In Maintenance. In this case, the following should occur:

If the response 503 - Service Unavailable was in response to an INVITE request:

- If calls are tied to registrations (**Calls Route via Registrar** enabled) and there are other proxies available, the tied registrations should issue an Un-REGISTER and try to REGISTER with a different proxy. The call should fail with cause = Temporary Fail.
- If calls are not tied, the INVITE should be immediately tried to a different proxy.

If the response 503 - Service Unavailable was in response to a REGISTER request:

- If there are other proxies available, this registration only should issue an Un-REGISTER and try to REGISTER with a different proxy.
- If **Explicit DNS Server(s)** are configured, a DNS request should be sent out to see whether the proxy server has disappeared from those being offered.

An Active-InMaintenance proxy server should not be used for a new transactions (INVITE or REGISTER) until:

- There is a change in DNS responses indicating the proxy has become active.
- The configuration does not leave any better option available. In this case, there should be a throttle so that no more than 5 failures (without successes) in 1 minute should be allowed.
- A configuration merge has occurred where the ITSP Proxy Address has been changed.
- 10 minutes has expired.

Behavior during Not Responding

A proxy server that is not-responding (UDP) is indicated when 3 requests are sent and no replies are received. This would normally occur during a single INVITE transaction.

Consideration should be given whether this is caused by a local network fault or is caused by the Proxy being out of service. Since it is likely to be local, no action should be taken unless traffic is received from an alternative proxy while this proxy is actually not responding. The state should be "Possibly non responding".

If explicit DNS servers are configured, a DNS request should be sent out to see whether this Proxy server has disappeared from those being offered.

If possible, an alternative proxy should be stimulated simultaneously with stimulating the suspect server.

The server should be considered non-responding if it is persistently non-responding while other proxies are responding or if it is non-responding and has disappeared from the DNS advertisement.

While in the "possibly not responding" state, it would be better to send an INVITE to an alternative proxy while simultaneously sending any appropriate message to this proxy. This will help to resolve whether it is really not responding rather than there being local network problems. However, there is no requirement to blacklist the proxy.

Once in the "definitely not responding" state:

- If there are other proxies available: this registration only issues an Un-REGISTER, and try to REGISTER with a different proxy. Calls do not automatically clear.
- If a SIP message is received from it, the state should immediately go"Active".
- This proxy should be blacklisted unless there are no better options available. While blacklisted, only one transaction per 10 minutes is allowed.
- Even if not blacklisted, there should be a throttle so that no more than 5 failures (without successes) in 1 minute should be allowed.

Configuration settings

The **ITSP Proxy Address** and **Calls Route via Registrar** settings are mergeable. Changing the remaining settings requires a “merge with service disruption”. When the configuration file is sent to the system, the SIP trunk is restarted and all calls on the line are dropped.

Offline editing is not required.

Field	Description
ITSP Proxy Address	Default = Blank This is the SIP Proxy address used for outgoing SIP calls. The address can be specified in the following ways: • If left blank, the ITSP Domain Name is used and is resolved by DNS resolution in the same way as if a DNS address had been specified as below. • An IP address. • A list of up to 4 IP addresses, with each address separated by a comma or space. - The addresses can include an indication of the relative call weighting of each address compared to the others. This is done by adding a **w N** suffix to the address where **N** is the weighting value. For example, in the list 213.74.81.102w3 213.74.81.100w2, the weighting values assigns 1.5 times the weight of calls to the first address. The default weight if not specified is 1. A weight of 0 can be used to disable an address. Weight is only applied to outgoing calls. If there is more than one proxy defined, and no weight indication, then calls are only sent to the first in the list until there is a failure at which point the next proxy is used. - If the **Calls Route via Registrar** setting below is enabled, the weighting is applied to registrations rather than calls. • A DNS address, for example sbc.example.com. - The DNS response may return multiple proxy addresses (RFC 3263). If that is the case, the system will resolve the address to use based on priority, TTL and weighting information included with each address. - A load balancing suffix can be added to specify that multiple proxy results should be returned if possible, for example sbc.example.com(N). where **N** is the required number of addresses from 1 to 4. This field is mergeable. However, no more than 4 IP Addresses should be in use at any time. So, if the combined new and old address settings exceed 4, the new addresses are only phased into use as transactions in progress on the previous addresses are completed.
Network Configuration	

Table continues…

Field	Description
Layer 4 Protocol	Default = UDP. The options are: • **TCP** • **UDP** • **TLS** • **Auto** TLS connections support the following ciphers: • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA
Use Network Topology Info	Default = None. This field associates the SIP line with the LAN interface **System Settings** > **System** > **LAN1** > **Network Topology** settings. It also applies the **System Settings** > **System** > **LAN1** > **VoIP** > **DiffServ Settings** to the outgoing traffic on the SIP line. If **None** is selected, STUN lookup is not applied and routing is determined by the system's routing tables. If no STUN server address is set for the interface, then the **System | LAN | Network Topology | Binding Refresh TimeSystem Settings** > **System** > **LAN1** > **Network Topology** > **Binding Refresh Time** is ignored by SIP Lines when calculating the periodic OPTIONS timing unless the **Firewall/NAT Type** is set to **Open Internet**.
Send Port	When Network Configuration is set to TLS, the default setting is 5061. When Network Configuration is set to TCP or UDP, the default setting is 5060.
Listen Port	When Network Configuration is set to TLS, the default setting is 5061. When Network Configuration is set to TCP or UDP, the default setting is 5060.
Explicit DNS Server(s)	Default = 0.0.0.0 (Off) If specific DNS servers should be used for SIP trunk operation rather than the general DNS server specified or obtained for the system, the server addresses can be specified here. If exported or imported as part of a trunk template.
Calls Route via Registrar	Default = On If selected, all calls are routed via the same proxy as used for registration. If multiple ITSP proxy addresses have been specified, there is no load balancing of registrations.
Separate Registrar	Default = Blank This field allows the SIP registrar address to be specified if it is different from that of the SIP proxy. The address can be specified as an IP address or DNS name.

Related links

SIP Line on page 309

Call Details

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **Call Details**

SIP URI

Having set up the SIP trunk to the SIP ITSP, the SIP URI's registered with that ITSP are entered on this tab. A SIP URI (Uniform Resource Identifier) is similar to an internet email address and represents the source or destination for SIP connection. The URI consists of two parts, the user part (name) and the host part (example.com).

SIP URI records are used to describe content of SIP headers when working with various ITSPs, since they use these SIP headers for various purposes and match them to IP Office interpretation of these headers. For incoming calls, headers in the SIP message must match the headers described in the appropriate URI. For outgoing calls, IP Office internal displays and calling or called numbers are mapped to appropriate headers in a way provider expects them to be formatted.

If the **Auto** setting is used in the SIP trunk's **Local URI**, **Contact** and **Display** fields, that SIP trunk will accept any incoming SIP call. The incoming call routing is still performed by the system incoming call routes based on matching the values received with the call or the URI's incoming group setting. On outgoing calls, **Auto** passes the calling and called party numbers from IP Office call unchanged to the SIP provider. The **Auto** setting has replaced the wildcard * used in previous releases.

For outgoing calls using this SIP URI, all valid short code CLI manipulations are used (transforming calling party number to ISDN will be ignored). For a full list of valid CLI manipulations, see “Telephone Number Field Characters” in the chapter “Short Code Overview”. For example, character ‘i’ is not supported since it sets calling party number plan to isdn and number type to national.

For the system, each SIP URI acts as a set of trunk channels. Outgoing calls can then be routed to the required URI by short codes that match that URI's **Outgoing Group** setting. Incoming calls can be routed by incoming call routes that match the URI's **Incoming Group** setting.

Note that the system supports only up to 150 URI records on a SIP line.

SIP Line Appearances

Using this feature, Line appearances can be configured on phones that support Line appearances. Several Line appearances can be associated with one SIP Line, specified by an ITSP. The buttons can be used to make or receive calls. ITSPs specify how many calls can be made or received using a particular SIP number.

If a SIP number can be used to make “n” number of calls, the system allocates “n” system wide unique line appearances for that number. All phones that wish to use the Line Appearance to make or receive calls must have a line appearance button configured to point to that Line ID. A SIP number can be accessed through the Line Appearance to make calls, answer calls, or conference with other users already on the call. Lamps on the button indicate whether the number is in use.

In case a sip number can be used to make or receive three calls, system can be configured to associate that number with three Line Appearance IDs. For simplicity purposes, Line Appearance IDs should be consecutive (for example 700, 701, 702…). The direction of call allocation can also be configured. The preferred way of configuring for outgoing calls and incoming calls are reverse

of each other to avoid confusion. For example, if the outgoing calls are allocated from 700->702, the incoming calls are allocated from 702->700.

SIP line appearances are supported on all phones that support line appearances. They are not supported over SCN or in resiliency.

Related links

SIP Line on page 309
SIP URI on page 320
SIP Line Appearances on page 327

SIP URI

Name	Description
URI	This field is for information only and cannot be edited. It shows the IP address of the system LAN interface with which the SIP trunk is associated.
Incoming Group	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.
Outgoing Group	Default = Previous external line + 1, Range 0 to 99999. Short codes that specify a number to dial can also specify the line group to be used. The system will then seize a line from those with the matching Outgoing Group ID. In a Server Edition network, the **Outgoing Group ID** used must be unique within the network. The same ID cannot be used in the configuration of any lines on another server system in the network. For non-Server Edition deployments, the same ID can be used for multiple lines. **Reserved Group ID Numbers:** • **90000 - 99999** Reserved for system use (not enforced). • **99999 and 99998** In a Server Edition network, reserved for the IP Office lines to the Primary Server and Secondary Server respectively. • **99901 to 99930** In a Server Edition network, reserved for the IP Office lines from the Primary Server to each expansion system in the network. • **0** In a Server Edition network, the ID 0 cannot be used. • **98888** For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.
Max Sessions	Default =10 This field sets the maximum number of simultaneous calls that can use the URI before the system returns busy to any further calls. For capacity information, see *Deploying Avaya IP Office™ Platform Server Edition*.
Credentials	Default = 0:<None> This field is used to select from a list of the account credentials configured on the line's **SIP Credentials** tab.

Table continues…

Name	Description
Local URI:	This field sets the 'From' field for outgoing SIP calls using this URI. • **Display**: This field sets the Name value for outgoing SIP calls using this URI. • **Content**: This field sets the Content of SIP headers for outgoing SIP calls using this URI. The values you type in the Content field are also reflected in the Display field. • **Outgoing Calls**: Default = Caller. You can select any one of the following options: - Caller - Explicit - None • **Forwarding/Twinning**: Default = Caller. This column sets the source used for the system's SIP URIs with incoming calls that it then redirects as outgoing calls. For example, calls it forwards or twins for users. You can select any one of the following options: - Caller: Use the name and number of the user or device forwarding the call. - Explicit: Use the values manually typed in the **Display** and **Content** columns. - Original Caller: Use the name and number details of the original caller who is now being forwarded. Note that use of this value form some headers such as P-Asserted-ID and P-Preferred-ID may not be supported if the line provider requires the caller information to be present in that header for billing purposes. • **Incoming Calls**: Default = Called. This column sets the source for the value used to match incoming calls from the line provider. You can select any one of the following options: - Called: Use the automatically determined settings appropriate to the call destination. - Explicit:Use the values manually typed in the **Display** and **Content** columns as intended destination. - None: Do not send the header.

Table continues…

Name	Description
Contact	This field sets the From field for outgoing SIP calls using this URI. • **Display**: This configurable field sets the Name value for outgoing SIP calls using this URI. • **Content**: This configurable field sets the Content of SIP headers for outgoing SIP calls using this URI. The values you type in the Content field are also reflected in the Display field. • **Outgoing Calls**: Default = Caller. You can select any one of the following options: - Caller - Explicit - None • **Forwarding/Twinning**: Default = Caller. This field can be used to set an originator number for forwarded and twinned calls. You can select any one of the following options: - Caller - Explicit - Original Caller • **Incoming Calls**: Default = Called. You can select any one of the following options: - Called - Explicit - None

Table continues…

Name	Description
P. Asserted ID	Default = Disabled When selected, identity information is provided in the P Asserted Identity header of SIP messages. You can enable P-Asserted-Identity (PAI) headers to assert the identity of users in outgoing SIP requests or response messages. • **Display**: This configurable field sets the Name value for outgoing SIP calls using this URI. • **Content**: This configurable field sets the Content of SIP headers for outgoing SIP calls using this URI. The values you type in the Content field are also reflected in the Display field. • **Outgoing Calls**: Default = Caller. You can select any one of the following options: - Caller - Explicit - None • **Forwarding/Twinning**: Default = Original Caller. This field can be used to set an originator number for forwarded and twinned calls. You can select any one of the following options: - Caller - Explicit - Original Caller • **Incoming Calls**: Default = Called. You can select any one of the following options: - Called - Explicit - None

Table continues…

Name	Description
P Preferred ID:	Default = Disabled When selected, identity information is provided in the P Preferred Identity header of SIP messages. • **Display**: This configurable field sets the Name field for outgoing SIP calls using this URI. • **Content**: This configurable field sets the Content of SIP headers for outgoing SIP calls using this URI. The values you type in the Content field are also reflected in the Display field. • **Outgoing Calls**: Default = Caller. You can select any one of the following options: - Called - Explicit - None • **Forwarding/Twinning**: Default = Original Caller This field can be used to set an originator number for forwarded and twinned calls. You can select any one of the following options: - Caller - Explicit - None - Original Caller • **Incoming Calls**: Default = Called. You can select any one of the following options: - Called - Explicit - None

Table continues…

Name	Description
Diversion Header	Default = Disabled When selected, information from the Diversion Header is provided in the SIP messages. • **Display**: This configurable field sets the Name field for outgoing SIP calls using this URI. • **Content**: This configurable field sets the Content of SIP headers for outgoing SIP calls using this URI. The values you type in the Content field are also reflected in the Display field. • **Outgoing Calls**: Default = Caller. You can select any one of the following options: - Caller - Explicit - None • **Forwarding/Twinning**: Default = Caller. This field can be used to set an originator number for forwarded and twinned calls. You can select any one of the following options: - Caller - Explicit - None - Original Caller • **Incoming Calls**: Default = None.

Table continues…

Name	Description
Remote Party ID	Default = Disabled When selected, it sets up the Remote Party ID header. the Diversion header for outgoing SIP calls using this URI. • **Display**: This configurable field sets the Name value for outgoing SIP calls using this URI. • **Content**: This configurable field sets the Content of SIP headers for outgoing SIP calls using this URI. The values you type in the Content field are also reflected in the Display field. • **Outgoing Calls**: Default = Caller. You can select any one of the following options: - Caller - Explicit - None • **Forwarding/Twinning**: Default = Original Caller. This field can be used to set an originator number for forwarded and twinned calls. You can select any one of the following options: - Caller - Explicit - None - Original Caller • **Incoming Calls**: Default = Called. You can select any one of the following options: - Called - Explicit - None

Display and Content fields are configurable for each SIP header separately. The value can either be entered manually or one of the following options can be selected:

- **Auto**: Use the number that IP Office is using to make the call as the From field. The number will be aligned with IP Office internal numbering schema.
- **Use Internal Data**: Use the value **Call Management** > **Users** > **Add/Edit Users** > **SIP** > **Display Name (Alias)** for the user making the call.

  The system can also use

  - **Call Management** > **Group** > **Add/Edit Group** > **SIP** > **Display Name (Alias)** for a group
  - **System Settings** > **System** > **Voicemail** > **Display Name (Alias)** for voicemail

If you have selected a Credential value other than None, the following options become available in the drop-down list for you to select:

- Credentials User Name: Use the value **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Credentials** > **User Name** for the user making the call.

- Credentials Authentication Name: Use the value **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Credentials** > **Authentication Name**.
- Credentials Contact: Use the value **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Credentials** > **Contact**.

Related links

Call Details on page 319

SIP Line Appearances

Name	Description
SIP Line Appearances	Default = Disabled When enabled, the content of the pane is displayed at the bottom half of the page. You can use the Add, Edit, and Delete options to configure SIP Line Appearances parameters. If you disable the SIP Line Appearances check box and save the configuration, all the configured values are lost.
Incoming Group	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.
Outgoing Group	Default = Previous external line + 1, Range 0 to 99999. Short codes that specify a number to dial can also specify the line group to be used. The system will then seize a line from those with the matching Outgoing Group ID. In a Server Edition network, the **Outgoing Group ID** used must be unique within the network. The same ID cannot be used in the configuration of any lines on another server system in the network. For non-Server Edition deployments, the same ID can be used for multiple lines. **Reserved Group ID Numbers:** • **90000 - 99999** Reserved for system use (not enforced). • **99999 and 99998** In a Server Edition network, reserved for the IP Office lines to the Primary Server and Secondary Server respectively. • **99901 to 99930** In a Server Edition network, reserved for the IP Office lines from the Primary Server to each expansion system in the network. • **0** In a Server Edition network, the ID 0 cannot be used. • **98888** For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.
Credentials	Default = 0:<None> This field is used to select from a list of the account credentials configured on the line's **SIP Credentials** tab.

Table continues…

Name	Description
Max Sessions	Default =10 This field sets the maximum number of simultaneous calls that can use the URI before the system returns busy to any further calls. For capacity information, see *Deploying Avaya IP Office™ Platform Server Edition*.
Incoming Sessions	Default = 3 The number of Incoming call sessions. The range varies from 0 to Max Sessions. If you change the Max Sessions, the number of Incoming sessions are automatically updated to reflect the change.
Outgoing Sessions	Default = 3 The number of Outgoing call sessions. The range varies from 0 to Max Sessions. If you change the Max Sessions, the number of Outgoing sessions are automatically updated to reflect the change.
Line Appearance ID	Default = 701 The Line Appearance ID is a representation of the SIP trunk line on the IP Office system. The indicator corresponding to the Line Appearance indicates the activities on the line.
Incoming ID	The ID on which the Incoming call activities are indicated. The range of the IDs are from maximum to minimum and changes when the Max Sessions values are updated.
Outgoing ID	The ID on which the Outgoing call activities are indicated. This is a read-only field. The range of the IDs are from minimum to maximum and changes when the Max Sessions values are updated.
Local URI	This field sets the 'From' field for outgoing SIP calls using this SIP Line. • **Display**: This configurable field sets the Name value for outgoing SIP calls using this SIP Line. • **Content**: This field sets the Content of SIP headers for outgoing SIP calls using this SIP Line. The values you type in the Content field are also reflected in the Display field. • **Outgoing Calls**: Default = Explicit. • **Incoming Calls**: Default = Explicit.

Table continues…

Name	Description
Contact	This field sets the From field for outgoing SIP calls using this SIP Line. • **Display**: This configurable field sets the Name value for outgoing SIP calls using this SIP Line. • **Content**: This field sets the Content of SIP headers for outgoing SIP calls using this SIP Line. The values you type in the Content field are also reflected in the Display field. • **Outgoing Calls**: Default = Explicit. You can select any one of the following options: - Explicit - None • **Incoming Calls**: Default = Explicit. You can select any one of the following options: - Explicit - None
P Asserted ID	Default = Disabled When selected, identity information is provided in the P Asserted Identity header of SIP messages. You can enable P-Asserted-Identity (PAI) headers to assert the identity of users in outgoing SIP requests or response messages. **Note:** You can enter the wildcard character "*". Entering this value populates the SIP PAI header with the caller information available to IP Office. • **Display**: This configurable field sets the Name value for outgoing SIP calls using this SIP Line. • **Content**: This field sets the Content of SIP headers for outgoing SIP calls using this SIP Line. The values you type in the Content field are also reflected in the Display field. • **Outgoing Calls**: Default = Explicit. You can select any one of the following options: - Explicit - None • **Incoming Calls**: Default = Explicit. You can select any one of the following options: - Explicit - None

Table continues…

Name	Description
P Preferred ID	Default = Disabled When selected, identity information is provided in the P Preferred Identity header of SIP messages. • **Display**: This configurable field sets the Name value for outgoing SIP calls using this SIP Line. • **Content**: This field sets the Content of SIP headers for outgoing SIP calls using this SIP Line. The values you type in the Content field are also reflected in the Display field. • **Outgoing Calls**: Default = Explicit. You can select any one of the following options: - Explicit - None • **Incoming Calls**: Default = Explicit. You can select any one of the following options: - Explicit - None
Diversion Header	Default = Disabled When selected, information from the Diversion Header is provided in the SIP messages. • **Display**: This configurable field sets the Name value for outgoing SIP calls using this SIP Line. • **Content**: This field sets the Content of SIP headers for outgoing SIP calls using this SIP Line. The values you type in the Content field are also reflected in the Display field. • **Outgoing Calls**: Default = Explicit. You can select any one of the following options: - Explicit - None • **Incoming Calls**: Default = None.

Table continues…

Name	Description
Remote Party ID	Default = Disabled When selected, it sets up the Remote Party ID header. the Diversion header for outgoing SIP calls using this URI. . • **Display**: This configurable field sets the Name value for outgoing SIP calls using this SIP Line. • **Content**: This field sets the Content of SIP headers for outgoing SIP calls using this SIP Line. The values you type in the Content field are also reflected in the Display field. • **Outgoing Calls**: Default = Explicit. You can select any one of the following options: - Explicit - None • **Incoming Calls**: Default = Explicit. You can select any one of the following options: - Explicit - None

Display and Content fields are configurable for each SIP header separately. The value can either be entered manually or one of the following options can be selected:

- **Auto**: Use the number that IP Office is using to make the call as the From field. The number will be aligned with IP Office internal numbering schema.
- **Use Internal Data**: Use the value **Call Management** > **Users** > **Add/Edit Users** > **SIP** > **Display Name (Alias)** for the user making the call.

  The system can also use

  - **Call Management** > **Group** > **Add/Edit Group** > **SIP** > **Display Name (Alias)** for a group
  - **System Settings** > **System** > **Voicemail** > **Display Name (Alias)** for voicemail

If you have selected a Credential value other than None, the following options become available in the drop-down list for you to select:

- Credentials User Name: Use the value **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Credentials** > **User Name** for the user making the call.
- Credentials Authentication Name: Use the value **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Credentials** > **Authentication Name**.
- Credentials Contact: Use the value **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Credentials** > **Contact**.

Related links

Call Details on page 319

SIP Line VoIP

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP VoIP**

This form is used to configure the VoIP settings applied to calls on the SIP trunk.

Configuration Settings

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

Field	Description
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. The available codecs in default preference order are: • **G.711 A-Law** • **G.711 U-LAW** • **G.729** • **G.723.1** Note that the default order for G.711 codecs varies to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition, it is supported on Primary Server, Secondary Server and Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo. The codecs available in this form are set through the codec list on **System Settings** > **System** > **VoIP**. Within a network of systems, it is strongly recommended that all the systems and the lines connecting those systems use the same codecs. The options are: • **System Default** This is the default setting. When selected, the codec list below matches the codecs set in the system wide list. • **Custom** This option allows specific configuration of the codec preferences to be different from the system list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.

Table continues…

Field	Description
Fax Transport Support	Default = Off. This option is only available if **Re-Invite Supported** is selected. IP500 V2 systems can terminate T38 fax calls. IP Office Linux systems can route the calls between trunks/terminals with compatible fax types. If the media is routed by IP Office between trunks/terminals with incompatible fax types or if fax is terminated by IP Office, IP Office will detect fax tones and renegotiate the call as needed. This setting must be configured based on what is supported by the SIP ATA. The options are: • **None** Select this option if fax is not supported by the line provider. • **G.711** G.711 is used for the sending and receiving of faxes. • **T38** T38 is used for the sending and receiving of faxes. • **T38 Fallback** When you enable this option, T38 is used for sending and receiving faxes on a SIP line. If the called destination does not support T38, the system will send a re-invite to change the transport method to G.711.
DTMF Support	Default = RFC2833. This setting is used to select the method by which DTMF key presses are signalled to the remote end. The options are: • **In Band**: Send DTMF digits as part of the audio path. • **RFC2833**: Send DTMF digits using a separate audio stream from the voice path. Note that use of RFC2833 is negotiated with the remote end of the call. If not agreed or not supported, the line reverts to using in band signalling. • **Info**: Send the DTMF digits in SIP INFO packets.
Media Security	Default = Disabled. These setting control whether SRTP is used for this line and the settings used for the SRTP. The options are: • **Same as System**: Matches the system setting at **System Settings** > **System** > **VoIP Security**. • **Disabled**: Media security is not required. All media sessions (audio, video, and data) will be enforced to use RTP only. • **Preferred**: Media security is preferred. Attempt to use secure media first and if unsuccessful, fall back to non-secure media. • **Enforced**: Media security is required. All media sessions (audio, video, and data) will be enforced to use SRTP only. **Warning:** Selecting **Enforced** on a line or extension that does not support media security will result in media setup failures.

Table continues…

Field	Description
Advanced Media Security Options	Not displayed if **Media Security** is set to **Disabled**. The options are: • **Same as System**: Use the same settings as the system setting configured on **System Settings** > **System** > **VoIP Security**. • **Encryptions**: Default = RTP This setting allows selection of which parts of a media session should be protected using encryption. The default is to encrypt just the RTP stream (the speech). • **Authentication**: Default = RTP and RTCP This setting allows selection of which parts of the media session should be protected using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Currently not adjustable. • **Crypto Suites**: Default = SRTP_AES_CM_128_SHA1_80. There is also the option to select SRTP_AES_CM_128_SHA1_32.
VoIP Silence Suppression	Default = Off When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunks between networked systems, the same setting should be set at both ends.
Local Hold Music	Default = Off. When enabled, if the far end puts the call on HOLD, the system plays music received from far end (SIP Line) to the other end. RTCP reports are sent towards SIP Line. When disabled, the system plays local music to the other endpoint and no RTCP packets are sent to SIP trunk.
Re-Invite Supported	Default = Off. When enabled, **Re-Invite** can be used during a session to change the characteristics of the session. For example when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk. Requires the ITSP to also support **Re-Invite**. This setting must be enabled for video support.
Codec Lockdown	Default = Off. Supports RFC 3264 Section 10.2 when **RE-Invite Supported** is enabled. In response to a SIP offer with a list of codecs supported, some SIP user agents supply a SDP answer that also lists multiple codecs. This means that the user agent may switch to any of those codecs during the session without further negotiation. The system does not support multiple concurrent codecs for a session, so loss of speech path will occur if the codec is changed during the session. If codec lockdown is enabled, when the system receives an SDP answer with more than one codec from the list of offered codecs, it sends an extra re-INVITE using just a single codec from the list and resubmits a new SDP offer with just the single chosen codec.

Table continues…

Field	Description
Allow Direct Media Path	Default = On This settings controls whether IP calls must be routed via the system or can be routed alternatively if possible within the network structure. • If enabled, IP calls can take routes other than through the system, removing the need for system resources such as voice compression channels. Both ends of the calls must support Direct Media and have compatible VoIP settings such as matching codec, etc. If otherwise, the call will remain routed via the system. Enabling this option may cause some vendors problems with changing the media path mid call. • If disabled, the call is routed via the system. In that case, RTP relay support may still allow calls between devices using the same audio codec to not require a voice compression channel.
PRACK/100rel Supported	Default = Off. When selected, supports Provisional Reliable Acknowledgement (PRACK) on SIP trunks. Enable this parameter when you want to ensure that provisional responses, such as announcement messages, have been delivered. Provisional responses provide information on the progress of the request that is in process. For example, while a cell phone call is being connected, there may be a delay while the cell phone is located; an announcement such as “please wait while we attempt to reach the subscriber” provides provisional information to the caller while the request is in process. PRACK, which is defined in RFC 3262, provides a mechanism to ensure the delivery of these provisional responses.
Force direct media with phones	Default = On The setting is only available when the trunk's **Re-invite Supported** and **Allow Direct Media Path** settings are enabled and its DTMF Support option is set to **RFC2833/ RFC4733**. It also requires the H.323 IP extension involved in the call to also have **Allow Direct Media Path** enabled. This feature is only supported with Avaya H.323 IP telephones. For calls where the Avaya H.323 IP extension using the trunk is doing so as a direct media call, this feature allows digits pressed on the extension to be detected and the call changed to an indirect media call so that RFC2833 DTMF can be sent. The call remains as an indirect media call for 15 seconds after the last digit before reverting back to being a direct media call.
G.711 Fax ECAN	Default = Off This setting is only available on IP500 V2 systems when **Fax Transport Support** is set to **G.711** or **T.38 Fallback**. When IP Office detects a fax call, the IP Office negotiates to G.711 (if not already in G.711) and reconfigures the connection with echo cancellation (ECAN) based on the 'G.711 Fax ECAN field. This can be used to avoid an ECAN mismatch with the SIP trunk service provider. Also for fax calls, the connection’s NLP is disabled, a fixed jitter buffer is set and silence suppression is disabled.

Related links

SIP Line on page 309

T.38 Fax

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP T38 Fax**

The settings are available only on IP500 V2 since it can terminate T38 fax. On the **VoIP** settings for the line type, **Fax Transport Support** must be set to **T38** or **T38 Fallback**.

These settings are mergeable.

Field	Description
Use Default Values	Default = On. If selected, all the fields are set to their default values and greyed out.
T38 Fax Version	Default = 3. During fax relay, the two gateways will negotiate to use the highest version which they both support. The options are: • **0** • **1** • **2** • **3**
Transport	Default = UDPTL (fixed). Only **UDPTL** is supported. **TCP** and **RTP** transport are not supported. For **UDPTL**, redundancy error correction is supported. Forward Error Correction (FEC) is not supported.
Redundancy Redundancy sends additional fax packets in order to increase the reliability. However increased redundancy increases the bandwidth required for the fax transport.	
Low Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for low speed V.21 T.30 fax transmissions.
High Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for V.17, V.27 and V.28 fax transmissions.
TCF Method	Default = Trans TCF. TCF = Training Check Frame.
Max Bit Rate (bps)	Default = 14400. Lower rates can be selected if the current rate is not supported by the fax equipment or is found to not be reliable.
EFlag Start Timer (msecs)	Default = 2600.
EFlag Stop Timer (msecs)	Default = 2300.

Table continues…

Field	Description
Tx Network Timeout (secs)	Default = 150.
Scan Line Fix-up	Default = On.
TFOP Enhancement	Default = On.
Disable T30 ECM	Default = Off. When selected, disabled the T.30 Error Correction Mode used for fax transmission.
Disable EFlags For First DIS	Default = Off.
Disable T30 MR Compression	Default = Off.
NSF Override	Default = Off. If selected, the NSF (Non-Standard Facility) information sent by the T38 device can be overridden using the values in the fields below. **Country Code**: Default = 0. **Vendor Code**: Default = 0.

Related links

SIP Line on page 309

SIP Line Credentials

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Credentials**

Used to enter the ITSP username and password for the SIP account with the ITSP. If you have several SIP accounts going to the same ITSP IP address or domain name, you can enter up to 30 sets of ITSP account names and passwords on this tab.

Use the **Add**, **Remove**, and **Edit** buttons to manage the set of credentials for the SIP trunk accounts. The settings for each account are listed below.

Configuration Settings

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

Field	Descriptions
Index	This number is assigned automatically and cannot be edited. If the **From** field on the SIP URI being used for the call is set to **Use Authentication Name** , the registration field of the SIP URI will indicate the index number of the SIP credentials to use for calls by that SIP URI.
User Name	This name must be unique and is used to identify the trunk. The name can include the domain if necessary.

Table continues…

Field	Descriptions
Authentication Name	Default = Blank. This field can be blank but must be completed if a **Password** is also specified. This value is provided by the SIP ITSP. Depending on the settings on the Local URI tab associated with the SIP call, it may also be used as the user part of the SIP URI. The name can include the domain if necessary.
Contact	Default = Blank. This field is used to enter a contact and can include the domain if necessary.
Password	Default = Blank. This value is provided by the SIP ITSP. If a password is specified, the matching **Authentication Name** must also be set.
Expiry	Default = 60 minutes. This setting defines how often registration with the SIP ITSP is required following any previous registration.
Registration Required	Default = On. If selected, the fields above above are used for registration when making calls. If exported or imported as part of a trunk template.

Related links

SIP Line on page 309

SIP Line Advanced

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Advanced**

Additional configuration information

For additional information regarding the **Media Connection Preservation** setting, see Media Connection Preservation on page 551.

Configuration settings

These settings are mergable, with the exception of the **Media Connection Preservation** setting. Changing the **Media Connection Preservation** setting requires a “merge with service disruption”. When the configuration file is sent to the system, the SIP trunk is restarted and all calls on the line are dropped.

Offline editing is not required.

Field	Description
Addressing	

Table continues…

Field	Description
Association Method	Default = By Source IP Address. This setting sets the method by which a SIP line is associated with an incoming SIP request. The match criteria used for each line can be varied. The search for a line match for an incoming request is done against each line in turn using each lines Association Method. The order of line matching uses the configured **Line Number** settings until a match occurs. If no match occurs the request is ignored. This method allows multiple SIP lines with the same address settings. This may be necessary for scenarios where it may be required to support multiple SIP lines to the same ITSP. For example when the same ITSP supports different call plans on separate lines or where all outgoing SIP lines are routed from the system via an additional on-site system. The options are: • **By Source IP Address**: This option uses the source IP address and port of the incoming request for association. The match is against the configured remote end of the SIP line, using either an IP address/port or the resolution of a fully qualified domain name. • **"From" header hostpart against ITSP domain**: This option uses the host part of the From header in the incoming SIP request for association. The match is against the **ITSP Domain Name** above. • **R-URI hostpart against ITSP domain**: This option uses the host part of the Request-URI header in the incoming SIP request for association. The match is against the **ITSP Domain Name** above. • **"To" header hostpart against ITSP domain**: This option uses the host part of the To header in the incoming SIP request for association. The match is against the **ITSP Domain Name** above. • **"From" header hostpart against DNS-resolved ITSP domain**: This option uses the host part of the FROM header in the incoming SIP request for association. The match is found by comparing the FROM header against a list of IP addresses resulting from resolution of the **ITSP Domain Name** above or, if set, the **SIP Line** > **SIP Transport** > **ITSP Proxy Address** setting. • **"Via" header hostpart against DNS-resolved ITSP domain**: This option uses the host part of the VIA header in the incoming SIP request for association. The match is found by comparing the VIA header against a list of IP addresses resulting from resolution of the **ITSP Domain Name** above or, if set, the **SIP Line** > **SIP Transport** > **ITSP Proxy Address** setting. • **"From" header hostpart against ITSP proxy**: This option uses the host part of the “From” header in the incoming SIP request for association. The match is against the **SIP Line** > **SIP Transport** > **ITSP Proxy Address** setting. • **"To" header hostpart against ITSP proxy**: This option uses the host part of the From header in the incoming SIP request for association. The match is against the **SIP Line** > **SIP Transport** > **ITSP Proxy Address** setting.

Table continues…

Field	Description
	• **R-URI hostpart against ITSP proxy**: This option uses the host part of the Request-URI in the incoming SIP request for association. The match is against the **SIP Line** > **SIP Transport** > **ITSP Proxy Address** setting.
Call Routing Method	Default = Request URI. This field allows selection of which incoming SIP information should be used for incoming number matching by the system's incoming call routes. The options are to match either the **Request URI** or the **To Header** element provided with the incoming call.
Use P-Called-Party	Default = Off. When enabled, IP Office reads the `P-Called-Party ID` header if present in the SIP message and routes the incoming SIP calls based on it. The feature can be enabled on public SIP trunk interfaces. The configuration should be present in SIP Trunks templates. If not present, will be treated as disabled. If the feature is enabled and the header is not present in the SIP message, IP Office uses the header configured in the Call Routing method for Incoming Call Route.
Suppress DNS SRV Lookups	Default = Off. Controls whether to send SRV queries for this endpoint, or just NAPTR and A record queries.
Identity	
Use Phone Context	Default = Off. When set to On, signals SIP enabled PBXs that the call routing identifier is a telephone number.
Add user=phone	Default = Off. This setting is available when **Use Phone Context** is set to On. This setting adds the SIP parameter **user** with value **phone** to the From and To SIP headers in outgoing calls.
Use + for International	Default = Off. When set to On, outgoing international calls use E.164/International format with a '+' followed by the country code and then the directory number.
Use PAI for Privacy	Default = Off. When set to On, if the caller ID is withheld, the SIP message From: header is made anonymous, and the caller's identity, for admission control, billing, and emergency services, is inserted into the P-Asserted-Identity header. This mechanism should only be used in a trusted network and must be stripped out of the SIP message before it is forwarded outside the trusted domain.
Use Domain for PAI	Default = Off. When set to Off, the DNS resolved IP address of the ITSP Proxy is used for the host part in the P-Asserted-Identity header. When set to On, the the Domain for PAI is used.

Table continues…

Field	Description
Caller ID FROM Header	Default = Off. Incoming calls can include caller ID information in both the From field and in the PAI fields. When this option is selected, the caller ID information in the From field is used rather than that in the PAI fields.
Send From In Clear	Default = Off. When selected, the user ID of the caller is included in the From field. This applies even if the caller has selected to be or is configured to be anonymous, though their anonymous state is honored in other fields used to display the caller identity.
Cache Auth Credentials	Default = On. When set to On, allows the credentials challenge and response from a registration transaction to be automatically inserted into later SIP messages without waiting for a subsequent challenge.
Add UUI header	Default — Off. When set to On, the User-to-User Information (UUI) is passed in SIP headers to applications.
Add UUI header to redirected calls	Default — Off. When set to On, the UUI is passed in SIP headers for calls that are redirected, for example, forwarded calls, twinned calls. This field can be modified only if the **Add UUI header** is set to On.
User-Agent and Server Headers	Default = Blank (Use system type and software level). The value set in this field is used as the User-Agent and Server value included in SIP request headers made by this line. If the field is blank, the type of IP Office system and its software level used. Setting a unique value can be useful in call diagnostics when the system has multiple SIP trunks.
Send Location Info	Default = Never. The options are: • **Never**: Do not send location information. • **Emergency Calls**: When set to **Emergency Calls**, the location defined at **System Settings** > **Locations** > **Add/Edit Location** is sent as part of the INVITE message when emergency calls are made.
Media	
Allow Empty INVITE	Default = Off. When set to On, allows 3pcc devices to initiate calls to IP Office by sending an INVITE without SDP.
Send Empty re-INVITE	Default = Off. This option is only available if **SIP Line** > **SIP VoIP** > **Reinvite Supported** is selected. If set to On, when connecting a call between two endpoints, IP Office sends an INVITE without SDP in order to solicit the full media capabilities of both parties.

Table continues…

Field	Description
Allow To Tag Change	Default = Off. When set to On, allows the IP Office to change media parameters when connecting a call to a different party than that which was advertised in the media parameters of provisional responses, such as 183 Session Progress.
P-Early-Media Support	Default = None. The options are: • **None**: IP Office will not advertise support of this SIP header and will always take incoming early media into account regardless of presence of this header • **Receive**: IP Office will advertise support of this SIP header and will discard incoming early media unless this header is present in the sip message. • **All**: IP Office will advertise support of this sip header, will discard incoming early media unless this header is present in the sip message and will include this sip header when providing early media.
Send SilenceSupp=off	Default = Off. Used for the G711 codec. When checked, the silence suppression off attribute is sent in SDP on this trunk.
Force Early Direct Media	Default = Off. When set to On, allows the direct connection of early media streams to IP endpoints rather than anchoring it at the IP Office.
Media Connection Preservation	Default = Disabled. When enabled, allows established calls to continue despite brief network failures. Call handling features are no longer available when a call is in a preserved state. Preservation on public SIP trunks is not supported until tested with a specific service provider.
Indicate HOLD	Default = Off. When enabled, the system sends a HOLD INVITE to the SIP trunk endpoint.
Call Control	
Call Initiation Timeout (s)	Default = 4 seconds. Range = 1 to 99 seconds. Sets how long the system should wait for a response to its attempt to initiate a call before following the alternate routes set in an ARS form.
Call Queuing Timeout (m)	Default = 5 minutes. For incoming calls, how many minutes to wait before dropping a call that has been queued waiting for a free VCM resource, or has remained in the unanswered state. For outgoing calls, how many minutes to wait for the call to be answered after receiving a provisional response.

Table continues…

Field	Description
Service Busy Response	Default = 486 - Busy Here (503 - Service Unavailable for the France2 locale). For calls that result in a busy response from IP Office, this setting determines the response code. The options are: • **486 - Busy Here** • **503 - Service Unavailable**
on No User Responding Send	Default = 408-Request Timeout. Specifies the cause to be used when releasing incoming calls from SIP trunks, when the cause of releasing is that user did not respond. The options are 408-Request Timeout or 480 Temporarily Unavailable.
Action on CAC Location Limit	Default = Allow Voicemail When set to **Allow Voicemail**, the call is allowed to go to a user's voicemail when the user's location call limit has been reached. When set to **Reject Call**, the call is rejected with the failure response code configured in the **Service Busy Response** field.
Suppress Q.850 Reason Header	Default = Off. When SIP calls are released by sending BYE and CANCEL, a release reason header is added to the message. When set to On, the Q.850 reason header is not included.
Emulate NOTIFY for REFER	Default = Off. Use for SIP providers that do not send NOTIFY messages. When set to On, after IP Office issues a REFER, and the provider responds with 202 ACCEPTED, IP Office will assume the transfer is complete and issue a BYE.
No REFER if using Diversion	Default = Off. When enabled, REFER is not sent on the trunk if the forwarding was done with 'Send Caller ID = Diversion Header'. Applies to Forwards and Twinning.

Related links

SIP Line on page 309

SIP Line Engineering

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Engineering**

This page is used to enter values that apply special features to the SIP line. These are entered using the **Add**, **Edit** and **Remove** buttons.

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

Related links

SIP Line on page 309

H.323 Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **H323 Line**

These lines are added manually. They allow voice calls to be routed over data links within the system. They are therefore dependent on the IP data routing between the system and the destination having being configured and tested.

Calls received on IP, S0 and QSIG trunks do not use incoming call routes. Routing for these is based on incoming number received as if dialed on-switch. Line short codes on those trunks can be used to modify the incoming digits.

Network Assessments

Not all data connections are suitable for voice traffic. A network assessment is required for internal network connections. For external network connections a service level agreement is required from the service provider. Avaya cannot control or be held accountable for the suitability of a data connection for carrying voice traffic.

QSIG trunks trunks are not supported on IP500 V2 systems without IP500 Voice Networking licenses.

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 518.

Related links

Add Trunk Line on page 308
H.323 Line VoIP on page 344
H.323 Line Short Codes on page 346
H.323 Line VoIP Settings on page 347

H.323 Line VoIP

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **H323 Line** > **VoIP Line**

Configuration Settings

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

Field	Description
Line Number	Default = Auto-filled. Range = 1 to 249 *(IP500 V2)*/349 *(Server Edition)*. Enter the line number that you wish. Note that this must be unique. On IP500 V2 systems, line numbers 1 to 16 are reserved for internal hardware.
Telephone Number	Used to remember the telephone number of this line. For information only.
Network Type	Default = Public. This option is available if **System Settings** > **System** > **Telephony** > **Restrict Network Interconnect** is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.

Table continues…

Field	Description
Prefix	Default = Blank. The prefix is used in the following ways: • **For incoming calls** The ISDN messaging tags indicates the call type (National, International or Unknown). If the call type is unknown, then the number in the Prefix field is added to the ICLID. • **For outgoing calls** The prefix is not stripped, therefore any prefixes not suitable for external line presentation should be stripped using short codes.
National Prefix	Default = 0 This indicates the digits to be prefixed to a incoming national call. When a number is presented from ISDN as a "national number" this prefix is added. For example 1923000000 is converted to 01923000000.
International Prefix	Default = 00 This indicates the digits to be prefixed to an incoming international call. When a number is presented from ISDN as an "international number" this prefix is added. For example 441923000000 is converted to 00441923000000.
Location	Default = Cloud. Specify a location to associate the extension with a physical location. Associating an extension with a location: • Allows emergency services to identify the source of an emergency call. • Allows you to configure call admission control settings for the location. The drop down list contains all locations that have been defined on **System Settings** > **Locations**.
Description	Default = Blank. Maximum 31 characters. Use this field to enter a description of this configuration.
Send original calling party for forwarded and twinning calls	Default = Off. Use the original calling party ID when forwarding calls or routing twinned calls.

Table continues…

Field	Description
Outgoing Group ID	Default = 1. Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID. In a Server Edition network, the **Outgoing Group ID** used on a system must also be unique within the network. The same ID cannot be used in the configuration of any lines on another server system in the network. For Standard Edition deployments, the same ID can be used for multiple lines. **Reserved Group ID Numbers:** • **90000 - 99999** Reserved for system use (not enforced). • **99999 and 99998** In a Server Edition network, reserved for the IP Office lines to the Primary Server and Secondary Server respectively. • **99901 to 99930** In a Server Edition network, reserved for the IP Office lines from the Primary Server to each expansion system in the network. • **0** In a Server Edition network, the ID 0 cannot be used. • **98888** For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.
Number of Channels	Default = 20, Range 1 to 250. Defines the number of operational channels that are available on this line.
Outgoing Channels	Default = 20, Range 0 to 250. This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as Number of Channels field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls.
TEI	Default = 0. Range = 0 to 127. The Terminal Equipment Identifier. Used to identify each Control Unit connected to a particular ISDN line. For Point to Point lines this is typically (always) 0. It can also be 0 on a Point to Multi-Point line, however if multiple devices are actually sharing a Point to Multi-Point line it should be set to 127 which will result in the exchange deciding on the TEI's to be used by this Control Unit.

Related links

H.323 Line on page 343

H.323 Line Short Codes

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **H323 Line** > **Short Codes**

For some types of line, Line short codes can be applied to any digits received with incoming calls.

The line Short Code tab is shown for the following trunk types which are treated as internal or private trunks: **QSIG** (T1, E1, H.323), **BRI S0**, **H.323**, **SCN**, **IP Office**. Incoming calls on those types of trunk are not routed using **Incoming Call Route** settings. Instead the digits received with incoming calls are checked for a match as follows:

Extension number (including remote numbers in a multi-site network).

- Line short codes (excluding ? short code).
- System short codes (excluding ? short code).
- Line ? short code.
- System ? short code.

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

These settings can be edited online.

Related links

H.323 Line on page 343

H.323 Line VoIP Settings

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **H323 Line** > **VoIP Settings**

This form is used to configure the VoIP setting applied to calls on the H.323 line.

Configuration Settings

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

Field	Description
Gateway IP Address	Default = Blank Enter the IP address of the gateway device at the remote end.
Port	Default = 1720 The H.323 line is identified by the IP Address:Port value. Specifying a unique port value for this IP address allows multiple lines to use the same IP address.

Table continues…

Field	Description
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. The available codecs in default preference order are: • **G.711 A-Law** • **G.711 U-LAW** • **G.729** • **G.723.1** Note that the default order for G.711 codecs varies to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition, it is supported on Primary Server, Secondary Server and Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo. The codecs available in this form are set through the codec list on **System Settings** > **System** > **VoIP**. Within a network of systems, it is strongly recommended that all the systems and the lines connecting those systems use the same codecs. The options are: • **System Default** This is the default setting. When selected, the codec list below matches the codecs set in the system wide list. • **Custom** This option allows specific configuration of the codec preferences to be different from the system list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.
Supplementary Services	Default = H450. Selects the supplementary service signaling method for use across the H.323 trunk. The remote end of the trunk must support the same option. The options are: • **None**: No supplementary services are supported. • **H450**: Use for H.323 lines connected to another PBX or device that uses H450. • **QSIG**: Use for H.323 lines connected to another PBX or device that uses QSIG.
Call Initiation Timeout	Default = 4 seconds. Range = 1 to 99 seconds. This option sets how long the system should wait for a response to its attempt to initiate a call before following the alternate routes set in an ARS form.

Table continues…

Field	Description
VoIP Silence Suppression	Default = Off. When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.
Enable FastStart for non-Avaya IP Phones	Default = Off A fast connection procedure. Reduces the number of messages that need to be exchanged before an audio channel is created.
Fax Transport Support	Default = Off This option is only supported on trunks with their **Supplementary Services** set to **IP Office SCN** or **IP Office Small Community Network - Fallback**. Fax relay is supported across H.323 multi-site network lines with **Fax Transport Support** selected. This will use 2 VCM channels in each of the systems. Fax relay is only supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 and or IP500 Combo cards. Fax relay is not supported on Server Edition Linux servers.
Local Tones	Default = Off When selected, the tones are generated by the local system to which the phone is registered. This option should not be used with lines being used for a multi-site network.
DTMF Support	Default = Out of Band DTMF tones can be sent to the remote end either as DTMF tones within the calls audio path (**In Band**) or a separate signals (**Out of Band**). Out of Band is recommended for compression modes such as G.729 and G.723 compression modes where DTMF in the voice stream could become distorted.
Allow Direct Media Path	Default = On This settings controls whether IP calls must be routed via the system or can be routed alternatively if possible within the network structure. • If enabled, IP calls can take routes other than through the system, removing the need for system resources such as voice compression channels. Both ends of the calls must support Direct Media and have compatible VoIP settings such as matching codec, etc. If otherwise, the call will remain routed via the system. Enabling this option may cause some vendors problems with changing the media path mid call. • If disabled, the call is routed via the system. In that case, RTP relay support may still allow calls between devices using the same audio codec to not require a voice compression channel.

Table continues…

Field	Description
Progress Ends Overlap Send	Default = Off. Some telephony equipment, primarily AT&T switches, over IP trunks send a H.323 Progress rather than H.323 Proceeding message to signal that they have recognized the digits sent in overlap state. By default the system expects an H.323 Proceeding message. This option is not available by default. If required, the value **ProgressEndsOverlapSend** must be entered into the Source Numbers tab of the NoUser user.
Default Name From Display IE	Default = Off. When set, the Display IE is used as the default source for the name.

Related links

H.323 Line on page 343

IP Office Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP Office Line**

This line type is used to connect two IP Office systems.

In previous releases, connecting two IP Office systems was achieved using H.323 Lines configured with **Supplementary Services** set to **IP Office SCN**. In the current release, the IP Office line type is used to connect IP Office systems. Separating out the IP Office line type from the H.323 line type allows for the logical grouping of features and functions available when connecting two IP Office systems, including IP Office systems connected through the cloud.

Note:

Setting an IP Office line with **Transport Type** = **Proprietary** and **Networking Level** = **SCN** will interwork with a previous release system configured with an H.323 SCN line.

Related links

Add Trunk Line on page 308
IP Office Line on page 350
IP Office Line Short Codes on page 355
IP Office Line VoIP Settings on page 355
T38 Fax on page 358

IP Office Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP Office Line** > **Line**

Additional configuration information

For information on the **SCN Resiliency Options**, see Server Edition Resiliency on page 653.

Configuration Settings

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

Field	Description
Line Number	Default = Auto-filled. Range = 1 to 249 *(IP500 V2)*/349 *(Server Edition)*. Enter the line number that you wish. Note that this must be unique. On IP500 V2 systems, line numbers 1 to 16 are reserved for internal hardware.
Transport Type	Default = Proprietary. The options are • **Proprietary**: The default connection type when connecting two IP Office systems. • **WebSocket Client / Websocket Server**: A WebSocket connection is an HTTP / HTTPS initiated TCP pipe through which Call signalling and Network Signaling is tunneled. This transport type is used to connect IP Office systems through the cloud. Selecting one of the WebSocket options enables the **Security** field and the **Password** fields.
Networking Level	Default = SCN. The options are • **None**: No supplementary services are supported. • **SCN**: This option is used to link IP Office system within a multi-site network. The systems within a multi-site network automatically exchange information about users and extensions, allowing remote users to be called without any additional configuration on the local system.
Security	Default = Unsecured. The Security field is available when **Transport Type** is set to **WebSocket Client** or **WebSocket Server**. The options are • **Unsecured** : The connection uses HTTP/TCP. • **Medium**: The connection uses HTTPS/TLS. • **High**: The connection uses HTTPS/TLS. The server certificate store must contain the client identity certificate.
Network Type	Default = Public. This option is available if **System Settings** > **System** > **Telephony** > **Restrict Network Interconnect** is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Include location specific information	Default = Off. Enabled when **Network Type** is set to **Private**. Set to **On** if the PBX on the other end of the trunk is toll compliant.

Table continues…

Field	Description
Telephone Number	Default = Blank. Used to remember the telephone number of this line. For information only.
Prefix	Default = Blank. The prefix is used in the following ways: • **For incoming calls** The ISDN messaging tags indicates the call type (National, International or Unknown). If the call type is unknown, then the number in the Prefix field is added to the ICLID. • **For outgoing calls** The prefix is not stripped, therefore any prefixes not suitable for external line presentation should be stripped using short codes.
Outgoing Group ID	Default = 1. Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID. In a Server Edition network, the **Outgoing Group ID** used on a system must also be unique within the network. The same ID cannot be used in the configuration of any lines on another server system in the network. For Standard Edition deployments, the same ID can be used for multiple lines. **Reserved Group ID Numbers:** • **90000 - 99999** Reserved for system use (not enforced). • **99999 and 99998** In a Server Edition network, reserved for the IP Office lines to the Primary Server and Secondary Server respectively. • **99901 to 99930** In a Server Edition network, reserved for the IP Office lines from the Primary Server to each expansion system in the network. • **0** In a Server Edition network, the ID 0 cannot be used. • **98888** For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.
Number of Channels	Default = 20. Range 1 to 250; 1 to 500 for Select systems. Defines the number of operational channels that are available on this line.
Outgoing Channels	Default = 20, Range 0 to 250; 0 to 500 for Select systems. This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as Number of Channels field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls.
Gateway	
Address	Default = Blank. Enter the IP address of the gateway device at the remote end. This address must not be shared by any other IP line (H.323, SIP, SES or IP DECT).

Table continues…

Field	Description
Location	Default = Cloud. Specify a location to associate the extension with a physical location. Associating an extension with a location: • Allows emergency services to identify the source of an emergency call. • Allows you to configure call admission control settings for the location. The drop down list contains all locations that have been defined on **System Settings** > **Locations**.
Password **Confirm Password**	Default = Blank. The **Password** field is enabled when **Transport Type** is set to **WebSocket Server** or **WebSocket Client**. WebSockets are bi-directional HTTP or HTTPS communication pipes initiated from a client to a server. They permit clients behind local a firewall to traverse the internet to a server by using well known ports and protocols. A matching password must be set at each end of the line.
Port	When **Transport Type** is set to **Proprietary**, the default port is 1720 and cannot be changed. When **Transport Type** is set to **WebSocket Client**, the default port is 80. The **Port** field is not available when **Transport Type** is set to **WebSocket Server**. The HTTP and HTTPS receive ports are defined at the system level in the security settings **System Details** tab.
SCN Resiliency Options These options are only available when the **Networking Level** option is set to **SCN**. The intention of this feature is to attempt to maintain a minimal level of operation while problems with the local system are resolved.	
Supports Resiliency	Default = Off. These fields are available when **Networking Level** is set to **SCN**. When selected, all the available options are defaulted to **On**. When resiliency support is enabled on an IP Office Line in systems having IP extensions and the resilient systems do not have the corresponding H.323 or SIP registrars enabled, the IP Office system displays the error message - `System is configured to support resiliency. Registration of IP extensions in failover requires the corresponding registrar to be enabled.`

Table continues…

Field	Description
Backs up my IP Phones	Default = Off. When selected, the local system shares information about the registered phones and users on those phones with the backup system. If the local system is no longer visible to the phones, the phones will reregister with the backup system. When phones have registered with the backup system, they show an **R** on their display. Note that while IP Office line settings are mergeable, changed to this setting require the IP phones to be restarted in order to become aware of the change in their failover destination. If the setting **System Settings** > **System** > **Telephony** > **Phone Failback** is set to **Automatic**, and the phone's primary server has been up for more than 10 minutes, the backup system causes idle phones to perform a failback recovery to the original system. If using resilience backup to support Avaya IP phones, **Auto-create Extn** and **Auto-create User** should not be left enabled after initial configuration or any subsequent addition of new extensions and users. Leaving auto-create options enabled on a system that is a failover target may cause duplicate extension/user records on the multi-site network under multiple failure scenarios.
Backs up my Hunt Groups	Default = Off. This option is available only on the IP Office Line connecting the Server Edition Primary server to the Server Edition Secondary server. When selected, any hunt groups the local system is advertising to the network are advertised from the backup system when fallback is required. The trigger for this occurring is phones registered with the local system registering with the backup system, ie. **Backs up my IP Phones** above must also be enabled. When used, the only hunt group members that will be available are as follows: • If the group was a distributed hunt group, those members who were remote members on other systems are still visible within the network. • Any local members who have hot desked to another system still visible within the network. When the local system becomes visible to the backup system again, the groups will return to be advertised from the local system.
Backs up my Voicemail	Default = Off. This option can be used if the local system is hosting the Voicemail Pro server being used by the network. If selected, when the local system is no longer visible to the voicemail server, the backup system acts as host for the voicemail server. In a Server Edition network, this option is only available on the H.323 trunk from the Primary Server to the Secondary Server. It is assumed to be on and is automatically set by the Resilience Administration tool. The option requires the backup system to have licenses for the Voicemail Pro features that are required to operate during any fallback period.

Table continues…

Field	Description
Backs up my IP DECT Phones	Default = Off. This option is used for Avaya IP DECT phones registered with the system. When selected, it will share information about the registered phones and users on those phones with the backup system. If the local system is no longer visible to the phones, the phones will reregister with the backup system. The users who were currently on those phones will appear on the backup system as if they had hot desked. Note that when the local system is restored to the network, the phones will not automatically re-register with it. A phone reset via either a phone power cycle or using the System Status Application is required. When phones have registered with the backup system, they will show an **R** on their display. **Note:** Only one IP Office Line can have this configuration parameter set to On.
Backs up my one-X Portal	Default = Off. This option is available on Server Edition Select deployments and only on the IP Office Line connecting the Server Edition Primary server to the Server Edition Secondary server. When set to On, this setting enables one-X Portal resiliency and turns on the backup one-X Portal on the Server Edition Secondary server.
Description	Default = Blank. Maximum 31 characters. Use this field to enter a description of this configuration.

Related links

IP Office Line on page 350

IP Office Line Short Codes

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP Office Line** > **Short Codes**

Incoming calls on IP Office Lines are not routed using Incoming Call Route settings.

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

These settings can only be edited offline. Changes to these settings require a reboot of the system. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Related links

IP Office Line on page 350

IP Office Line VoIP Settings

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP Office Line** > **VoIP Settings**

Configuration Settings

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

Field	Description
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. The available codecs in default preference order are: • **G.711 A-Law** • **G.711 U-LAW** • **G.729** • **G.723.1** Note that the default order for G.711 codecs varies to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition, it is supported on Primary Server, Secondary Server and Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo. The codecs available in this form are set through the codec list on **System Settings** > **System** > **VoIP**. Within a network of systems, it is strongly recommended that all the systems and the lines connecting those systems use the same codecs. The options are: • **System Default** This is the default setting. When selected, the codec list below matches the codecs set in the system wide list. • **Custom** This option allows specific configuration of the codec preferences to be different from the system list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.

Table continues…

Field	Description
Fax Transport Support	Default = None. IP500 V2 systems can terminate T38 fax calls. IP Office Linux systems can route the calls between trunks/terminals with compatible fax types. If the media is routed by IP Office between trunks/terminals with incompatible fax types or if fax is terminated by IP Office, IP Office will detect fax tones and renegotiate the call as needed. The options are: • **None** Select this option if fax is not supported by the line provider. • **Fax Relay** On IP Office Lines, fax relay is supported across multi-site network lines with **Fax Transport Support** selected. This will use 2 VCM channels in each of the systems. Fax relay is only supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 and or IP500 Combo cards. Not supported on Server Edition. • **G.711** G.711 is used for the sending and receiving of faxes. • **T38** T38 is used for the sending and receiving of faxes. • **T38 Fallback** When you enable this option, T38 is used for sending and receiving faxes. If the called destination does not support T38, the system will renegotiate to change the transport method to G.711.
Call Initiation Timeouts	Default = 4. Range = 1 to 99 seconds. This option sets how long the system should wait for a response to its attempt to initiate a call before following the alternate routes set in an ARS form.
Media Security	Default = Same as System. Secure RTP (SRTP) can be used between IP Offices to add additional security. These settings control whether SRTP is used for this line and the settings used for the SRTP. The options are: • **Same as System**: Matches the system setting at **System Settings** > **System** > **VoIP Security**. • **Disabled**: Media security is not required. All media sessions (audio, video, and data) will be enforced to use RTP only. • **Preferred**: Media security is preferred. Attempt to use secure media first and if unsuccessful, fall back to non-secure media. • **Enforced**: Media security is required. All media sessions (audio, video, and data) will be enforced to use SRTP only. **Warning:** Selecting **Enforced** on a line or extension that does not support media security will result in media setup failures.

Table continues…

Field	Description
Advanced Media Security Options	Not displayed if **Media Security** is set to **Disabled**. The options are: • **Same as System**: Use the same settings as the system setting configured on **System Settings** > **System** > **VoIP Security**. • **Encryptions**: Default = RTP This setting allows selection of which parts of a media session should be protected using encryption. The default is to encrypt just the RTP stream (the speech). • **Authentication**: Default = RTP and RTCP This setting allows selection of which parts of the media session should be protected using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Currently not adjustable. • **Crypto Suites**: Default = SRTP_AES_CM_128_SHA1_80. There is also the option to select SRTP_AES_CM_128_SHA1_32.
VoIP Silence Suppression	Default = Off When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.
Out Of Band DTMF	Default = On. Out of Band DTMF is set to on and cannot be changed.
Allow Direct Media Path	Default = On This settings controls whether IP calls must be routed via the system or can be routed alternatively if possible within the network structure. • If enabled, IP calls can take routes other than through the system, removing the need for system resources such as voice compression channels. Both ends of the calls must support Direct Media and have compatible VoIP settings such as matching codec, etc. If otherwise, the call will remain routed via the system. Enabling this option may cause some vendors problems with changing the media path mid call. • If disabled, the call is routed via the system. In that case, RTP relay support may still allow calls between devices using the same audio codec to not require a voice compression channel.

Related links

IP Office Line on page 350

T38 Fax

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP Office Line** > **T38 Fax**

The settings are available only on IP500 V2 since it can terminate T38 fax. On the **VoIP** settings for the line type, **Fax Transport Support** must be set to **T38** or **T38 Fallback**.

These settings are mergeable.

Field	Description
Use Default Values	Default = On. If selected, all the fields are set to their default values and greyed out.
T38 Fax Version	Default = 3. During fax relay, the two gateways will negotiate to use the highest version which they both support. The options are: • **0** • **1** • **2** • **3**
Transport	Default = UDPTL (fixed). Only **UDPTL** is supported. **TCP** and **RTP** transport are not supported. For **UDPTL**, redundancy error correction is supported. Forward Error Correction (FEC) is not supported.
Redundancy Redundancy sends additional fax packets in order to increase the reliability. However increased redundancy increases the bandwidth required for the fax transport.	
Low Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for low speed V.21 T.30 fax transmissions.
High Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for V.17, V.27 and V.28 fax transmissions.
TCF Method	Default = Trans TCF. TCF = Training Check Frame.
Max Bit Rate (bps)	Default = 14400. Lower rates can be selected if the current rate is not supported by the fax equipment or is found to not be reliable.
EFlag Start Timer (msecs)	Default = 2600.
EFlag Stop Timer (msecs)	Default = 2300.
Tx Network Timeout (secs)	Default = 150.
Scan Line Fix-up	Default = On.
TFOP Enhancement	Default = On.
Disable T30 ECM	Default = Off. When selected, disabled the T.30 Error Correction Mode used for fax transmission.

Table continues…

Field	Description
Disable EFlags For First DIS	Default = Off.
Disable T30 MR Compression	Default = Off.
NSF Override	Default = Off. If selected, the NSF (Non-Standard Facility) information sent by the T38 device can be overridden using the values in the fields below. **Country Code**: Default = 0. **Vendor Code**: Default = 0.

Related links

IP Office Line on page 350

SIP DECT Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP DECT Line**

A SIP DECT line can be manually added. SIP DECT lines are used to manage D100 Base Station operation.

Related links

Add Trunk Line on page 308
SIP DECT Base on page 360
SIP DECT VoIP on page 361

SIP DECT Base

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP DECT Line** > **SIP DECT Base**

Currently, IP Office supports four D100 Base Stations.

These settings are not mergeable. Changes to these settings requires a reboot of the system.

Field	Description
Line Number	Default = Blank. A unique line number associated with the SIP DECT Base Station. **Associated Extensions** are other extensions that can log into the base station.
Base Name	Default = Blank. Maximum 16 characters. A name assigned to the base station. Each base station provisioned on the IP Office must have a unique name. The field cannot be blank. The format is an alphanumeric string with no special characters.
Base MAC Address	Default = Blank. The MAC Address of the base station. If only one base station is provisioned, the field can remain at the default value. If multiple base stations are provisioned, the MAC address for each base station must be entered.

Table continues…

Field	Description
Configure Base IP	
Configure Base IP	Default = Off. Set to **On** to configure IP address attributes for the base station. When enabled, the Configure Base IP settings are displayed.
DHCP Client	Default = On. When enabled, specifies that the base station operates as a DHCP client. When enabled, not other IP address attributes can be configured.
IP Address	Default = Blank. The IP address of the base station. The IP address must be on the same subnet as one of the LAN interfaces.
IP Mask	Default = Blank. IP address mask.
IP Gateway	Default = Blank. The default gateway address
Provisioning Server	Default = IP Office interface address. The server address from where the Base Station configuration files can be retrieved.
Description	Default = Blank. Maximum 31 characters. Use this field to enter a description of this configuration.

Related links

SIP DECT Line on page 360

SIP DECT VoIP

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP DECT Line** > **VoIP**

This form is used to configure the VoIP setting applied to calls on the SIP DECT line.

These settings are not mergeable. Changes to these settings requires a reboot of the system.

Field	Description
IP Address	Default = Blank. The IP address of the SIP DECT extension.
Codec Selection	Default = Custom This field defines the codec or codecs offered during call setup. The codecs available to be used are set through **System Settings** > **System** > **VoIP**. The Custom option allows specific configuration of the codec preferences to be different from the system **Default Selection** list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs. The D100 Base Station supports only G711 codecs.

Table continues…

Field	Description
TDM | IP Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the system TDM interface to the IP connection. This field is not shown on Linux based platforms.
IP | TDM Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the IP connection to the system TDM interface. This field is not shown on Linux based platforms.
DTMF Support	Default =RFC2833 The D100 Base Station supports only RFC2833.
VoIP Silence Suppression	Default = Off When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.
Local Hold Music	Default = Off
Allow Direct Media Path	Default = On This settings controls whether IP calls must be routed via the system or can be routed alternately if possible within the network structure. • If enabled, IP calls can take routes other than through the system. This removes the need for a voice compression channel. Both ends of the calls must support Direct Media and be using the same protocol (H.323 or SIP). Enabling this option may cause some vendors problems with changing the media path mid call. • If disabled or not supported at on one end of the call, the call is routed via the system. RTP relay support allows calls between devices using the same audio codec to not require a voice compression channel.
RE-Invite Supported	Default = Off. When enabled, Re-Invite can be used during a session to change the characteristics of the session. For example when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk. Requires the ITSP to also support **Re-Invite**.

Related links

SIP DECT Line on page 360

IP DECT

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP DECT Line**

This type of line can be manually added. They are used to route voice calls over an IP data connection to an Avaya IP DECT system. Only one IP DECT line can be added to a system. Refer to the IP DECT R4 Installation manual for full details.

Currently, only one IP DECT line is supported on a system.

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 518.

Related links

Add Trunk Line on page 308
IP DECT Line on page 363
Gateway on page 363
VoIP on page 366

IP DECT Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP DECT Line** > **Line**

When creating an IP DECT line, these settings are mergeable. You can also remove an IP DECT line without rebooting. Changing an IP DECT line that has been imported into the configuration is not mergeable.

Field	Description
Line Number	This number is allocated by the system and is not adjustable.
Associated Extensions	Lists all the DECT extensions associated with the IP DECT line.
Description	Default = Blank. Maximum 31 characters. Use this field to enter a description of this configuration.

Related links

IP DECT on page 362

Gateway

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP DECT Line** > **Gateway**

This form is used to configure aspects of information exchange between the IP Office and IP DECT systems.

When creating an IP DECT line, these settings are mergeable. You can also remove an IP DECT line without rebooting. Changing an IP DECT line that has been imported into the configuration is not mergeable.

Field	Description
Auto-Create Extension	Default = Off. If enabled, subscription of a handset with the DECT system causes the auto-creation of a matching numbered extension within the system configuration if one does not already exist. This setting is not supported on systems configured to use WebLM server licensing. For security, auto-create is automatically disabled after 24 hours.

Table continues…

Field	Description
Auto-Create User	Default = Off. This option is only usable if **Auto-Create Extension** is also enabled. If enabled, subscription of a handset with the DECT system causes the auto-creation of a matching user within the system configuration if one does not already exist. For security, any auto-create settings set to On are automatically set to Off after 24 hours.
Enable DHCP Support	Default = Off This option is not supported for use with Avaya IP DECT R4. The IP DECT base stations require DHCP and TFTP support. Enable this option if the system is being used to provide that support, using IP addresses from its DHCP range (LAN1 or LAN2) and its TFTP server setting. If not enabled, alternate DHCP and TFTP options must be provided during the IP DECT installation. • If it is desired to use the system for DHCP support of the ADMM and IP DECT base stations only, the system address range should be set to match that number of addresses. Those addresses are then taken during the system restart and will not be available for other DHCP responses following the restart. • For larger IP DECT installations, the use of a non-embedded TFTP software option other than Manager is recommended.
Boot File	Default = ADMM_RFP_1_0_0.tftp. Range = Up to 31 characters. The name and path of the ADMM software file. The path is relative to the TFTP server root directory.
ADMM MAC Address	Default = 00:00:00:00:00:00 This field must be used to indicate the MAC address of the IP DECT base station that should load the ADMM software file and then act as the IP DECT system's ADMM. The address is entered in hexadecimal format using comma, dash, colon or period separators.
VLAN ID	Default = Blank. Range = 0 to 4095. If VLAN is being used by the IP DECT network, this field sets the VLAN address assigned to the base stations by the system if Enable DHCP Support is selected. • The system itself does not apply or use VLAN marking. It is assumed that the addition of VLAN marking and routing of VLAN traffic is performed by other switches within the customer network. • An ID of zero is not recommended for normal VLAN operation. • When blank, no VLAN option is sent to the IP DECT base station.
Base Station Address List	Default = Empty This box is used to list the MAC addresses of the IP DECT base stations, other than the base station being used as the ADMM and entered in the ADMM MAC Address field. Right-click on the list to select Add or Delete. or use the Insert and Delete keys. The addresses are entered in hexadecimal format using comma, dash, colon or period separators.

Table continues…

Field	Description
Enable Provisioning This option can be used with DECT R4 systems. It allows the setting of several values in the system configuration that previously needed to be set separately in the master base stations configuration. For full details refer to the DECT R4 Installation manual. The use of provisioning requires the system security settings to include an **IPDECT Group**.	
SARI/PARK	Default = 0 Enter the PARK (Portable Access Rights Key) license key of the DECT R4 system. DECT handset users enter this key when subscribing to the DECT system.
Subscriptions	Default = Disabled Select the method of subscription supported for handsets subscribing to the DECT R4 system. The options are: • **Disabled**:Disables subscription of handsets. • **Auto-Create**: Allow anonymous subscription of handsets. Once subscribed, the handset is assigned a temporary extension number. That extension number can be confirmed by dialing ***#**. A new extension number can be specified by dialing <Extension Number>*<Login Code>**#**. The **Auto-Create Extension** and **Auto-Create User** settings above should also be enabled. While configured to this mode, Manager will not allow the manual addition of new IP DECT extensions. • **Preconfigured**: Allow subscription only against existing IP DECT extensions records in the system configuration. The handset IPEI number is used to match the subscribing handset to a system extension.
Authentication Code	Default = Blank. Set an authentication code that DECT handset users should enter when subscribing to the DECT system.
Enable Resiliency Default = Off. Enables resiliency on the IP DECT Line. To configure resiliency, you must also configure an IP Office Line with **Backs up my IP Dect Phones** set to **On**.	
Status Enquiry Period	Default = 30 seconds. The period between successive verifications on the H.323 channel. The smaller the interval, the faster the IP DECT system recognizes that IP Office is down.
Prioritize Primary	Default = Off. Only available when **Enable Provisioning** is set to **On**. Set to **On** for automatic fail-over recovery. When on, the IP DECT system switches automatically from the backup IP Office to the "primary" IP Office. Note that the IP DECT system does not switch back automatically from the backup IP Office to the primary. The IP DECT system must be manually switched using Web Manager.

Table continues…

Field	Description
Supervision Timeout	Default = 120 seconds. Only available when **Enable Provisioning** is set to **On**. The period of time the IP DECT system will wait between attempts to switch from the backup IP Office to its "primary" IP Office.

Related links

IP DECT on page 362

VoIP

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **IP DECT Line** > **VoIP**

Used to configure the VoIP setting applied to calls on the IP DECT line.

When creating an IP DECT line, these settings are mergeable. You can also remove an IP DECT line without rebooting. Changing an IP DECT line that has been imported into the configuration is not mergeable.

Field	Description
Gateway IP Address	Default = Blank. Enter the IP address of the gateway device at the remote end. This address must not be shared by any other IP line (H.323, SIP, SES or IP DECT).
Standby IP Address	Default = Blank. IP Address of the Standby Master IP Base Station or the second Mirror Base Station. When the primary Mirror Base Station or Master Base Station is offline the second Mirror or the Standby Master will take over and the system will use this IP address.

Table continues…

Field	Description
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. The available codecs in default preference order are: • **G.711 A-Law** • **G.711 U-LAW** • **G.729** • **G.723.1** Note that the default order for G.711 codecs varies to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition, it is supported on Primary Server, Secondary Server and Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo. The codecs available in this form are set through the codec list on **System Settings** > **System** > **VoIP**. Within a network of systems, it is strongly recommended that all the systems and the lines connecting those systems use the same codecs. The options are: • **System Default** This is the default setting. When selected, the codec list below matches the codecs set in the system wide list. • **Custom** This option allows specific configuration of the codec preferences to be different from the system list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.
TDM | IP Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the system TDM interface to the IP connection. This field is not shown on Linux based platforms.
IP | TDM Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the IP connection to the system TDM interface. This field is not shown on Linux based platforms.
VoIP Silence Suppression	Default = Off. When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.

Table continues…

Field	Description
Allow Direct Media Path	Default = On This settings controls whether IP calls must be routed via the system or can be routed alternatively if possible within the network structure. • If enabled, IP calls can take routes other than through the system, removing the need for system resources such as voice compression channels. Both ends of the calls must support Direct Media and have compatible VoIP settings such as matching codec, etc. If otherwise, the call will remain routed via the system. Enabling this option may cause some vendors problems with changing the media path mid call. • If disabled, the call is routed via the system. In that case, RTP relay support may still allow calls between devices using the same audio codec to not require a voice compression channel.

Related links

IP DECT on page 362

SM Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SM Line**

This type of line is used to create a SIP connection between an IP Office and an Avaya Aura® Session Manager. The other end of the SIP connection must be configured on the Session Manager as a SIP Entity Link.

An SM Line can only be added to IP Office system Standard Mode or Server Edition configurations. It is typically used in IP Office Standard mode in Enterprise Branch deployments connected to the Avaya Aura® network. For more details about IP Office Enterprise Branch deployments refer to *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

An SM Line can also be used in IP Office Server Edition to connect to an Avaya Aura® Session Manager. Through the SM Line, IP Office Server Edition supports interoperability with Avaya Aura® Session Manager. It also supports interoperability, via the Avaya Aura® Session Manager, with Avaya Aura® Communication Manager systems and with CS 1000 systems. Note that IP Office Server Edition is not used as an enterprise branch product and does not support some of the IP Office enterprise branch functionality, such as management by Avaya Aura® System Manager, WebLM licensing, Centralized Users or voicemail over the SM Line.

If the Avaya Aura® network has multiple Avaya Aura® Session Managers to provide redundancy, two SM lines can be added, one configured for each Avaya Aura® Session Manager.

Related links

Add Trunk Line on page 308
SM Line Session Manager on page 369
SM Line VoIP on page 371
SM Line T38 Fax on page 376

SM Line Session Manager

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SM Line** > **Session Manager**

Additional configuration information

For additional information regarding the **Media Connection Preservation** setting, see Media Connection Preservation on page 551.

Configuration settings

These settings cannot be edited online. Changes to these settings require a reboot of the system.

Changing the **In Service** setting to **Disabled** (out of service) requires a system reboot. However, changing the **In Service** setting to **Enabled** is mergeable. Configuration changes made while the line is out of service are also mergeable.

Field	Description
Line Number	Default = Auto-filled. Range = 1 to 249 *(IP500 V2)*/349 *(Server Edition)*. Enter the line number that you wish. Note that this must be unique. On IP500 V2 systems, line numbers 1 to 16 are reserved for internal hardware. • **Session Manager line prioritization**: Up to two Session Manager lines can be configured. The two Session Manager lines are prioritized based on the line number. The lower line number is considered the primary Session Manager line. For example, if the first Session Manager line is configured as line number 17 and the second Session Manager line is configured as line 18, then line number 17 is considered the primary Session Manager line. If you want to designate the second Session Manager line (line 18 in this example) as the primary Session Manager line, you must change one or both of the line numbers so that the second Session Manager line is configured with a lower number than the current primary line. • **Session Manager line redundancy**: Based on the priority of the Session Manager lines designated by the line number, the active line to which the IP Office> sends all calls will always be the highest priority Session Manager line in service. That is, if the primary Session Manager line is in service, it will be the active line for sending calls. If the connection to the primary Session Manager line is lost, causing the IP Office to switch to the secondary Session Manager line, then when the primary line comes back up later, the IP Office reverts back to the primary Session Manager line.
In Service	Default = Enabled This option can be used to administratively disable the SM Line. It does not reflect the dynamic state of the line. If an SM Line is administratively disabled it is not equivalent to being in the dynamic out of service state.
SM Domain Name	This should match a SIP domain defined in the Session Manager system's SIP Domains table. Unless there are reasons to do otherwise, all the Enterprise Branch systems in the Avaya Aura® network can share the same domain.
SM Address	Enter the IP address of the Session Manager the line should use in the Avaya Aura network. The same Session Manager should be used for the matching **Entity Link** record in the Avaya Aura® configuration.

Table continues…

Field	Description
Outgoing Group ID	Default = 98888 This value is not changeable. However note the value as it is used in Enterprise Branch short codes used to route calls to the Session Manager.
Prefix	Default = Blank This prefix will be added to any source number received with incoming calls.
Max Calls	Default = 10 Sets the number of simultaneous calls allowed between the Enterprise Branch and Session Manager using this connection. Each call will use one of the available licenses that are shared by all SIP trunks configured in the system.
Network Type	Default = Public. This option is available if **System Settings** > **System** > **Telephony** > **Restrict Network Interconnect** is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Include location specific information	Default = Off. Enabled when **Network Type** is set to **Private**. Set to **On** if the PBX on the other end of the trunk is toll compliant.
URI Type	Default = SIP. When **SIP** or **SIPS** is selected in the drop-down box, the SIP URI format is used (for example, name@example.com). This affects the **From** field of outgoing calls. The **To** field for outgoing calls will always use the format specified by the short codes used for outgoing call routing. Recommendation: When SIP Secured URI is required, the URI Type should be set to **SIPS**. **SIPS** can be used only when Layer 4 Protocol is set to TLS.
Media Connection Preservation	Default = Enabled. When enabled, attempts to maintain established calls despite brief network failures. Call handling features are no longer available when a call is in a preserved state. When enabled, Media Connection Preservation applies to Avaya H.323 phones that support connection preservation.

Table continues…

Field	Description
Location	Default = Cloud. Specify a location to associate the extension with a physical location. Associating an extension with a location: • Allows emergency services to identify the source of an emergency call. • Allows you to configure call admission control settings for the location. The drop down list contains all locations that have been defined in the **Location** form.
Network Configuration TLS connections support the following ciphers: • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA	
Layer 4 Protocol	Default = TCP.
Send Port	When Network Configuration is set to TLS, the default setting is 5061. When Network Configuration is set to TCP, the default setting is 5060.
Listen Port	When Network Configuration is set to TLS, the default setting is 5061. When Network Configuration is set to TCP, the default setting is 5060.
Session Timer	Default = 1200. Range = 90 to 64800 This field specifies the session expiry time. At the half way point of the expiry time, a session refresh message is sent. Setting the field to **On Demand** disables the session timer. Communication Manager supports SIP session refresh via UPDATE in Communicaton Manger release 6.2 SP1 and later. If using an earlier release of Communication Manager, then the **Session Timer** parameter must be set to **On Demand**.
Description	Default = Blank. Maximum 31 characters. Use this field to enter a description of this configuration.

Related links

SM Line on page 368

SM Line VoIP

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SM Line** > **VoIP**

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

Field	Description
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. The available codecs in default preference order are: • **G.711 A-Law** • **G.711 U-LAW** • **G.729** • **G.723.1** Note that the default order for G.711 codecs varies to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition, it is supported on Primary Server, Secondary Server and Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo. The codecs available in this form are set through the codec list on **System Settings** > **System** > **VoIP**. Within a network of systems, it is strongly recommended that all the systems and the lines connecting those systems use the same codecs. The options are: • **System Default** This is the default setting. When selected, the codec list below matches the codecs set in the system wide list. • **Custom** This option allows specific configuration of the codec preferences to be different from the system list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.

Table continues…

Field	Description
Fax Transport Support	Default = None. This option is only available if **Re-Invite Supported** is selected. When enabled, the system performs fax tone detection on calls routed via the line and, if fax tone is detected, renegotiates the call codec as configured below. The SIP line provider must support the selected fax method and Re-Invite. The system must have available VCM resources using an IP500 VCM, IP500 VCM V2 or IP500 Combo base card. For systems in a network, fax relay is supported for fax calls between the systems. The options are: • **None** Select this option if fax is not supported by the line provider. • **G.711** G.711 is used for the sending and receiving of faxes. • **T38** T38 is used for the sending and receiving of faxes. This option is not supported by Linux based systems. • **T38 Fallback** When you enable this option, T38 is used for sending and receiving faxes on a SIP line. If the called destination does not support T38, the system will send a re-invite to change the transport method to G.711. This option is not supported on Linux based systems.
Call Initiation Timeout	Default = 4 seconds. Range = 1 to 99 seconds. This option sets how long the system should wait for a response to its attempt to initiate a call before following the alternate routes set in an ARS form.
DTMF Support	Default = RFC2833. This setting is used to select the method by which DTMF key presses are signalled to the remote end. The options are: • **In Band** • **RFC2833** • **Info**

Table continues…

Field	Description
Media Security	Default = Same as System. These setting control whether SRTP is used for this line and the settings used for the SRTP. The options are: • **Same as System**: Matches the system setting at **System Settings** > **System** > **VoIP Security**. • **Disabled**: Media security is not required. All media sessions (audio, video, and data) will be enforced to use RTP only. • **Preferred**: Media security is preferred. Attempt to use secure media first and if unsuccessful, fall back to non-secure media. • **Enforced**: Media security is required. All media sessions (audio, video, and data) will be enforced to use SRTP only. **Warning:** Selecting **Enforced** on a line or extension that does not support media security will result in media setup failures.
Advanced Media Security Options	Not displayed if **Media Security** is set to **Disabled**. The options are: • **Same as System**: Use the same settings as the system setting configured on **System Settings** > **System** > **VoIP Security**. • **Encryptions**: Default = RTP This setting allows selection of which parts of a media session should be protected using encryption. The default is to encrypt just the RTP stream (the speech). • **Authentication**: Default = RTP and RTCP This setting allows selection of which parts of the media session should be protected using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Currently not adjustable. • **Crypto Suites**: Default = SRTP_AES_CM_128_SHA1_80. There is also the option to select SRTP_AES_CM_128_SHA1_32.
VoIP Silence Suppression	Default = Off. When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.

Table continues…

Field	Description
Allow Direct Media Path	Default = On This settings controls whether IP calls must be routed via the system or can be routed alternatively if possible within the network structure. • If enabled, IP calls can take routes other than through the system, removing the need for system resources such as voice compression channels. Both ends of the calls must support Direct Media and have compatible VoIP settings such as matching codec, etc. If otherwise, the call will remain routed via the system. Enabling this option may cause some vendors problems with changing the media path mid call. • If disabled, the call is routed via the system. In that case, RTP relay support may still allow calls between devices using the same audio codec to not require a voice compression channel.
Re-Invite Supported	Default = On. When enabled, Re-Invite can be used during a session to change the characteristics of the session. For example when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk. Requires the ITSP to also support **Re-Invite**.
Codec Lockdown	Default = Off. Supports RFC 3264 Section 10.2 when **RE-Invite Supported** is enabled. In response to a SIP offer with a list of codecs supported, some SIP user agents supply a SDP answer that also lists multiple codecs. This means that the user agent may switch to any of those codecs during the session without further negotiation. The system does not support multiple concurrent codecs for a session, so loss of speech path will occur if the codec is changed during the session. If codec lockdown is enabled, when the system receives an SDP answer with more than one codec from the list of offered codecs, it sends an extra re-INVITE using just a single codec from the list and resubmits a new SDP offer with just the single chosen codec.
Force direct media with phones	Default = On The setting is only available when the trunk's **Re-invite Supported** and **Allow Direct Media Path** settings are enabled and its DTMF Support option is set to **RFC2833/RFC4733**. It also requires the H.323 IP extension involved in the call to also have **Allow Direct Media Path** enabled. This feature is only supported with Avaya H.323 IP telephones. For calls where the Avaya H.323 IP extension using the trunk is doing so as a direct media call, this feature allows digits pressed on the extension to be detected and the call changed to an indirect media call so that RFC2833 DTMF can be sent. The call remains as an indirect media call for 15 seconds after the last digit before reverting back to being a direct media call.

Table continues…

Field	Description
G.711 Fax ECAN	Default = Off This setting is only available on IP500 V2 systems when **Fax Transport Support** is set to **G.711** or **T.38 Fallback**. When IP Office detects a fax call, the IP Office negotiates to G.711 (if not already in G.711) and reconfigures the connection with echo cancellation (ECAN) based on the 'G.711 Fax ECAN field. This can be used to avoid an ECAN mismatch with the SIP trunk service provider. Also for fax calls, the connection's NLP is disabled, a fixed jitter buffer is set and silence suppression is disabled.

Related links

SM Line on page 368

SM Line T38 Fax

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **SM Line** > **SM Line T38 Fax**

The settings are available only on IP500 V2 since it can terminate T38 fax. On the **VoIP** settings for the line type, **Fax Transport Support** must be set to **T38** or **T38 Fallback**.

These settings are mergeable.

Field	Description
Use Default Values	Default = On. If selected, all the fields are set to their default values and greyed out.
T38 Fax Version	Default = 3. During fax relay, the two gateways will negotiate to use the highest version which they both support. The options are: • **0** • **1** • **2** • **3**
Transport	Default = UDPTL (fixed). Only **UDPTL** is supported. **TCP** and **RTP** transport are not supported. For **UDPTL**, redundancy error correction is supported. Forward Error Correction (FEC) is not supported.
Redundancy Redundancy sends additional fax packets in order to increase the reliability. However increased redundancy increases the bandwidth required for the fax transport.	
Low Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for low speed V.21 T.30 fax transmissions.

Table continues…

Field	Description
High Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for V.17, V.27 and V.28 fax transmissions.
TCF Method	Default = Trans TCF. TCF = Training Check Frame.
Max Bit Rate (bps)	Default = 14400. Lower rates can be selected if the current rate is not supported by the fax equipment or is found to not be reliable.
EFlag Start Timer (msecs)	Default = 2600.
EFlag Stop Timer (msecs)	Default = 2300.
Tx Network Timeout (secs)	Default = 150.
Scan Line Fix-up	Default = On.
TFOP Enhancement	Default = On.
Disable T30 ECM	Default = Off. When selected, disabled the T.30 Error Correction Mode used for fax transmission.
Disable EFlags For First DIS	Default = Off.
Disable T30 MR Compression	Default = Off.
NSF Override	Default = Off. If selected, the NSF (Non-Standard Facility) information sent by the T38 device can be overridden using the values in the fields below. **Country Code**: Default = 0. **Vendor Code**: Default = 0.

Related links

SM Line on page 368

Analog Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **Analog Line**

Analog trunks can be provided within the systems in the following ways. In all cases the physical ports are labeled as Analog. For full details of installation refer to the IP Office Installation manual.

Using ICLID: The system can route incoming calls using the ICLID received with the call. However ICLID is not sent instantaneously. On analog trunks set to Loop Start ICLID, there will be a short delay while the system waits for any ICLID digits before it can determine where to present the call.

Line Status: Analog line do not indicate call status other than whether the line is free or in use. Some system features, for example retrieving unanswered forwards and making twinned calls make use of the call status indicated by digital lines. This is not possible with analog lines. Once an analog line has been seized, the system has to assume that the call is connected and treats it as having been answered.

Dialing Complete: The majority of North-American telephony services use en-bloc dialing. Therefore the use of a ; is recommended at the end of all dialing short codes that use an N. This is also recommended for all dialing where secondary dial tone short codes are being used.

Ground Start: This type of analog trunk is only supported through the Analog Trunk external expansion module.

Related links

Add Trunk Line on page 308
Line Settings on page 378
Line Options on page 380

Line Settings

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **Analog Line** > **Line Settings**

Configuration Settings

These settings are mergeable with the exception of the **Network Type** setting. Changes to this setting will require a reboot of the system.

Field	Description
Line Number	This parameter is not configurable, it is allocated by the system.
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Network Type	Default = Public. This option is available if **System Settings** > **System** > **Telephony** > **Restrict Network Interconnect** is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Telephone Number	Used to remember the external telephone number of this line to assist with loop-back testing. For information only.

Table continues…

Field	Description
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.
Outgoing Group ID	Default = 1. Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID. In a Server Edition network, the **Outgoing Group ID** used on a system must also be unique within the network. The same ID cannot be used in the configuration of any lines on another server system in the network. For Standard Edition deployments, the same ID can be used for multiple lines. **Reserved Group ID Numbers:** • **90000 - 99999** Reserved for system use (not enforced). • **99999 and 99998** In a Server Edition network, reserved for the IP Office lines to the Primary Server and Secondary Server respectively. • **99901 to 99930** In a Server Edition network, reserved for the IP Office lines from the Primary Server to each expansion system in the network. • **0** In a Server Edition network, the ID 0 cannot be used. • **98888** For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.
Outgoing Channels	Default = 1 (not changeable)
Voice Channels	Default = 1 (not changeable)
Prefix	Default = Blank Enter the number to prefix to all incoming numbers for callback. This is useful if all users must dial a prefix to access an outside line. The prefix is automatically placed in front of all incoming numbers so that users can dial the number back. For outgoing calls: The system does not strip the prefix, therefore any prefixes not suitable for external line presentation should be stripped using short codes.
Line Appearance ID	Default = Auto-assigned. Range = 2 to 9 digits. Allows a number to be assigned to the line to identify it. On phones that support call appearance buttons, a Line Appearance button with the same number will show the status of the line and can be used to answer calls on the line. The line appearance ID must be unique and not match any extension number.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.

Related links

Analog Line on page 377

Line Options

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **Analog Line** > **Analog Options**

Covers analog line specific settings. The system wide setting **System Settings** > **System** > **Telephony** > **Tones and Music** > **CLI Type** is used for to set the incoming CLI detection method for all analogue trunks.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Channel	Set by the system. Shown for information only.
Trunk Type	Default = Loop Start Sets the analog line type. The options are: • **Ground Start**: Ground Start is only supported on trunks provided by the Analog Trunk 16 expansion module. It requires that the module and the control unit are grounded. Refer to the IP Office installation manual. • **Loop Start** • **Loop Start ICLID**: As the system can use ICLID to route incoming calls, on analog Loop Start ICLID trunks there is a few seconds delay while ICLID is received before the call routing can be determined.
Signaling Type	Default = DTMF Dialing Sets the signaling method used on the line. The options are: • **DTMF Dialing** • **Pulse Dialing**
Direction	Default = Both Directions Sets the allowed direction of operation of the line. The options are: • **Incoming** • **Outgoing** • **Both Directions**
Flash Pulse Width	Default = 0. Range = 0 to 2550ms. Set the time interval for the flash pulse width.
Await Dial Tone	Default = 0. Range = 0 to 25500ms. Sets how long the system should wait before dialing out.

Table continues…

Field	Description
Echo Cancellation	Default = 16ms. The echo cancellation should only be adjusted as high as required to remove echo problems. Setting it to a higher value than necessary can cause other distortions. Not used with external expansion module trunks. The options are (milliseconds): • **Off** • **8** • **16** • **32** • **64** • **128**
Echo Reduction	Default = On. (ATM4Uv2 card only) Used when impedance matching is not required but echo reduction is.
Mains Hum Filter	Default = Off. If mains hum interference on the lines is detected or suspected, this settings can be used to attempt to remove that interference. Useable with ATM16 trunks and IP500 ATM4U trunks. The options are: • **Off** • **50Hz** • **60Hz**
Impedance	Set the impedance used for the line. This field is only available for system locales where the default value can be changed. The value used for **Default** is set by the setting **System Settings** > **System** > **System** > **Locale**. For information, see *Avaya IP Office™ Platform Locale Settings*. The following values are used for **Automatic Impedance Matching**: 600+2150nF, 600, 900+2150nF, 900, 220+820||115nF, 370+620||310nF, 270+750||150nF, 320+1050||230nF, 350+1000||210nF, 800+100||210nF.
Quiet Line	This field is only available for certain system locales (see above). The setting may be required to compensate for signal loss on long lines.
Digits to break dial tone	Default = 2. Range = Up to 3 digits. During automatic impedance testing (see below), once the system has seized a line, it dials this digit or digits to the line. In some cases it may be necessary to use a different digit or digits. For example, if analog trunk go via another PBX system or Centrex, it will be necessary to use the external trunk dialing prefix of the remote system plus another digit, for example 92.

Table continues…

Field	Description
Automatic	Default = Yes. (ATM4Uv2 card only) When set to **Yes**, the **Default** value is used. The value used for **Default** is set by the system **Locale**. When set to **No**, the **Impedance** value can be manually selected from the list of possible values: 600 900 270+(750R || 150nF) and 275R + (780R || 150nF) 220+(820R || 120nF) and 220R+ (82R || 115nF) 370+(620R || 310nF) 320+(1050R || 230nF) 370+(820R || 110nF) 275+(780R || 115nF) 120+(820R || 110nF) 350+(1000R || 210nF) 200+(680R || 100nF) 600+2.16µF 900+1µF 900+2.16µF 600+1µF Global Impedance

Table continues…

Field	Description
Automatic Balance Impedance Match	These controls can be used to test the impedance of a line and to then display the best match resulting from the test. Testing should be performed with the line connected but the system otherwise idle. To start testing click **Start**. The system will then send a series of signals to the line and monitor the response, repeating this at each possible impedance setting. Testing can be stopped at any time by clicking **Stop**. When testing is complete, Manager will display the best match and ask whether that match should be used for the line. If **Yes** is selected, Manager will also ask whether the match should be applied to all other analog lines provided by the same analog trunk card or module. Note that on the Analog Trunk Module (ATM16), there are four control devices, each supporting four channels. The impedance is set by the control device for all four channels under its control. Consequently, the impedance match tool only functions on lines 1, 5, 9, and 13. Before testing, ensure that the following system settings are correctly set: • **System Settings** > **System** > **System** > **Locale** • **System Settings** > **System** > **Telephony** > **Companding Law** If either needs to be changed, make the required change and save the setting to the system before proceeding with impedance matching. Due to hardware differences, the impedance matching result will vary slightly depending on which type of trunk card or expansion module is being used. **Automatic Balance Impedance Matching**, **Quiet Line** and **Digits to break dial tone** are available for the Bahrain, Egypt, French Canadian, India, Kuwait, Morocco, Oman, Pakistan, Qatar, Saudi Arabia, South Africa, Turkey, United Arab Emirates, United States and Customize locales.
Allow Analog Trunk to Trunk Connect	Default = Not selected (Off). When not enabled, users cannot transfer or forward external calls back off-switch using an analog trunk if the call was originally made or received on another analog trunk. This prevents transfers to trunks that do not support disconnect clear. If the setting **System Settings** > **System** > **Telephony** > **Unsupervised Analog Trunk Disconnect Handling** is enabled, this setting is greyed out and trunk to trunk connections to any analog trunks are not allowed.
BCC	Default = Not selected [Brazil locale only] A collect call is a call at the receiver's expense and by his permission. If supported by the line provider, BCC (Block Collect Call) can be used to bar collect calls.

Table continues…

Field	Description
Secondary Dial Tone	Default = Off Configures the use of secondary dial tone on analog lines. This is a different mechanism from secondary dial tone using short codes. This method is used mainly within the Russian locale. When selected, the options are: • **Await time:** Default = 3000ms. Range = 0 to 25500ms. Used when secondary dial tone (above) is selected. Sets the delay. • **After n Digits**: Default = 1. Range = 0 to 10. Sets where in the dialing string, the delay for secondary dial tone, should occur. • **Matching Digit**: Default =8. Range = 0 to 9. The digit which, when first matched in the dialing string, will cause secondary dial tone delay.
Long CLI Line	Default = Off The CLI signal on some analog lines can become degraded and is not then correctly detected. If you are sure that CLI is being provided but not detected, selecting this option may resolve the problem.
Modem Enabled	Default = Off The first analog trunk in a control unit can be set to modem operation (V32 with V42 error correction). This allows the trunk to answer incoming modem calls and be used for system maintenance. When on, the trunk can only be used for analog modem calls. The default system short code *9000* can be used to toggle this setting. For the IP500 ATM4U-V2 Trunk Card Modem, it is not required to switch the card's modem port on/off. The trunk card's V32 modem function can be accessed simply by routing a modem call to the RAS service's extension number. The modem call does not have to use the first analog trunk, instead the port remains available for voice calls.
MWI Standard	Default = None. This setting is only displayed for ATM4U-V2 cards. When **System Settings** > **System** > **Voicemail** is set to **Analogue MWI**, change this setting to **Bellcore FSKBellcore FSK**.
Pulse Dialing	These settings are used for pulse dialing. • **Mark**: Default = 40ms. Range = 0 to 255. Interval when DTMF signal is kept active during transmission of DTMF signals. • **Space**: Default = 60ms. Range = 0 to 255. Interval of silence between DTMF signal transmissions. • **Inter-Digit Pause**: Default = 500ms. Range = 0 to 2550ms. Sets the pause between digits transmitted to the line.

Table continues…

Field	Description
Ring Detection	These settings are used for ring detection. • **Ring Persistency**: Default = Set according to system locale. Range = 0 to 2550ms. The minimum duration of signal required to be recognized. • **Ring Off Maximum**: Default = Set according to system locale. Range = 0 to 25500ms. The time required before signaling is regarded as ended.
Disconnect Clear	Disconnect clear (also known as 'Line Break' or 'Reliable Disconnect') is a method used to signal from the line provider that the call has cleared. The system also uses 'Tone Disconnect', which clears an analog call after 6 seconds of continuous tone, configured through the Busy Tone Detection (**System | Telephony | Tones & Music**) settings. • **Enable:** Default = On Enables the use of disconnect clear. • **Units**: Default = 500ms. Range = 0 to 2550ms. This time must be less than the actual disconnect time period used by the line provider by at least 150ms. If the setting **System Settings** > **System** > **Telephony** > **Unsupervised Analog Trunk Disconnect Handling** is enabled, this setting is greyed out and disconnect clear disabled.
DTMF	These settings are used for DTMF dialing. • **On**: Default = 80ms. Range = 0 to 255ms. The width of the on pulses generated during DTMF dialing. • **Off**: Default = 80ms. Range = 0 to 255ms. The width of the off pulses generated during DTMF dialing.
BCC Flash Pulse Width	[Brazil locale only] Default = 100 (1000ms). Range = 0 to 255. Sets the BCC (Block collect call) flash pulse width.
Gains	These settings are used to adjust the perceived volume on all calls. • **A | D**: Default = 0dB. Range =-10.0dB to +6.0dB in 0.5dB steps. Sets the analog to digital gain applied to the signal received from the trunk by the system. To conform with the Receive Objective Loudness Rating at distances greater than 2.7km from the central office, on analog trunks a receive gain of 1.5dB must be set. • **D | A**: Default = 0dB. Range =-10.0dB to +6.0dB in 0.5dB steps. Sets the digital to analog gain applied to the signal from the system to the trunk. • **Voice Recording**: Default = Low Used to adjust the volume level of calls recorded by voicemail. The ptions are: - **Low** - **Medium** - **High**

Related links

Analog Line on page 377

BRI Line

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **BRI Line**

BRI trunks are provided by the installation of a BRI trunk card into the control unit. The cards are available in different variants with either 2 or 4 physical ports. Each port supports 2 B-channels for calls. For full details of installation refer to the IP Office Installation manual.

Point-to-Point or Multipoint

BRI lines can be used in either Point-to-Point or Point-to-Multipoint mode. Point-to-Point lines are used when only one device terminates a line in a customer's office. Point-to-Multipoint lines are used when more than one device may be used on the line at the customer's premises. There are major benefits in using Point-to-Point lines:-

- The exchange knows when the line/terminal equipment is down/dead, thus it will not offer calls down that line. If the lines are Point-to-Multipoint, calls are always offered down the line and fail if there is no response from the terminal equipment. So if you have two Point-to-Multipoint lines and one is faulty 50% of incoming calls fail.
- You get a green LED on the Control Unit when the line is connected. With Point-to-Multipoint lines some exchanges will drop layer 1/2 signals when the line is idle for a period.
- The timing clock is locked to the exchange. If layer 1/2 signals disappear on a line then the Control Unit will switch to another line, however this may result in some audible click when the switchover occurs.

The system's default Terminal Equipment Identifier (TEI) will normally allow it to work on Point-to-Point or Point-to-Multipoint lines. However if you intend to connect multiple devices simultaneously to an BRI line, then the TEI should be set to 127. With a TEI of 127, the control unit will ask the exchange to allocate a TEI for operation.

Note:

When connected to some manufactures equipment, which provides an S0 interface (BRI), a defaulted Control Unit will not bring up the ISDN line. Configuring the Control Unit to a TEI of 127 for that line will usually resolve this.

Related links

Add Trunk Line on page 308
Line Settings on page 386
Channels on page 391

Line Settings

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **BRI Line** > **Line Settings**

The following settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

- **Line Sub Type**
- **Network Type**
- **TEI**
- **Add 'Not-end-to-end ISDN' Information Element**

- **Progress Replacement**
- **Clock Quality**
- **Force Number Plan to ISDN**
- **Number of Channels**

The remaining settings can be edited online.

Field	Description
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Line Number	This parameter is not configurable; it is allocated by the system.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.
Line Sub Type	Default = **NTT** for Japan/**ETSI** for other locales. Select to match the particular line type provided by the line provider. IP500 BRI daughter cards can be configured for **S-Bus** (So) operation for connection to ISDN terminal devices. Note that this requires the addition of terminating resistors at both the system and remote ends, and the use of a suitable cross-over cable. For full details refer to the Deploying Avaya IP Office Platform IP500 V2 manual.
Network Type	Default = Public. This option is available if **System Settings** > **System** > **Telephony** > **Restrict Network Interconnect** is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Telephone Number	Used to remember the external telephone number of this line to assist with loop-back testing. For information only.
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.

Table continues…

Field	Description
Outgoing Group ID	Default = 1. Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID. In a Server Edition network, the **Outgoing Group ID** used on a system must also be unique within the network. The same ID cannot be used in the configuration of any lines on another server system in the network. For Standard Edition deployments, the same ID can be used for multiple lines. **Reserved Group ID Numbers:** • **90000 - 99999** Reserved for system use (not enforced). • **99999 and 99998** In a Server Edition network, reserved for the IP Office lines to the Primary Server and Secondary Server respectively. • **99901 to 99930** In a Server Edition network, reserved for the IP Office lines from the Primary Server to each expansion system in the network. • **0** In a Server Edition network, the ID 0 cannot be used. • **98888** For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.
Prefix	Default = Blank. The prefix is used in the following ways: • **For incoming calls**: The ISDN messaging tags indicates the call type (National, International or Unknown). If the call type is unknown, then the number in the Prefix field is added to the ICLID. • **For outgoing calls**: The prefix is not stripped, therefore any prefixes not suitable for external line presentation should be stripped using short codes.
National Prefix	Default = 0 This indicates the digits to be prefixed to a incoming national call. When a number is presented from ISDN as a "national number" this prefix is added. For example 1923000000 is converted to 01923000000.
International Prefix	Default = 00 This indicates the digits to be prefixed to an incoming international call. When a number is presented from ISDN as an "international number" this prefix is added. For example 441923000000 is converted to 00441923000000.
TEI	Default = 0 The Terminal Equipment Identifier. Used to identify each device connected to a particular ISDN line. For Point-to-Point lines this is 0. It can also be 0 on a Point to Multipoint line, however if multiple devices are sharing a Point-to-Multipoint line it should be set to 127 which results in the exchange allocating the TEI's to be used.
Number of Channels	Default = 2. Range = 0 to 2. Defines the number of operational channels that are available on this line.

Table continues…

Field	Description
Outgoing Channels	Default = 2. Range = 0 to 2. This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as Number of Channels field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls.
Voice Channels	Default = 2. Range = 0 to 2. The number of channels available for voice use.
Data Channels	Default = 2. Range = 0 to 2. The number of channels available for data use. If left blank, the value is 0.
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available. • Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source. • In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.
Add 'Not-end-to-end ISDN' Information Element	Default = Never*. Sets whether the optional 'Not end-to-end ISDN' information element should be added to outgoing calls on the line. The options are **Never**, **Always** or **POTS** (only if the call was originated by an analog extension). *The default is **Never** except for the following locales; for Italy the default is **POTS**, for New Zealand the default is **Always**.

Table continues…

Field	Description
Progress Replacement	Default = None. Progress messages are defined in the Q.931 ISDN connection control signaling protocol. Generally, If a progress message is sent, the caller does not get connected and so typically does not accrue call costs. Not all ISDN lines support Q.931 Progress messages. Use this setting to configure alternative signaling to the ISDN line for internally generated Progress messages. The options are: • **Alerting**: Map to Q.931 Alerting. The call is not connected. The caller does not hear the message and typically does not accrue call costs. • **Connect**: Map to Q.931 Connect. The caller hears the message and typically will accrue call costs.
Supports Partial Rerouting	Default = Off. Partial rerouting (PR) is an ISDN feature. It is supported on external (non-network and QSIG) ISDN exchange calls. When an external call is transferred to another external number, the transfer is performed by the ISDN exchange and the channels to the system are freed. Use of this service may need to be requested from the line provider and may incur a charge.
Force Number Plan to ISDN	Default = Off. This option is only configurable when **Support Partial Rerouting** is also enabled. When selected, the plan/type parameter for Partial Rerouting is changed from **Unknown/Unknown** to **ISDN/Unknown**.
Send Redirecting Number	Default = Off. This option can be used on ISDN trunks where the redirecting service is supported by the trunk provider. Where supported, on twinned calls the caller ID of the original call is passed through to the twinning destination. This option is only used for twinned calls.
Support Call Tracing	Default = Off. The system supports the triggering of malicious caller ID (MCID) tracing at the ISDN exchange. Use of this feature requires liaison with the ISDN service provider and the appropriate legal authorities to whom the call trace will be passed. The user will also need to be enabled for call tracing and be provider with either a short code or programmable button to activate MCID call trace. Refer to Malicious Call Tracing in the Telephone Features section for full details.
Active CCBS Support	Default = Off. Call completion to a busy subscriber (CCBS). It allows automatic callback to be used on outgoing ISDN calls when the destination is busy. This feature can only be used on point-to-point trunks. Use of this service may need to be requested from the line provider and may incur a charge.
Passive CCBS	Default = Off.

Table continues…

Field	Description
Cost Per Charging Unit	The information is provided in the form of charge units. This setting is used to enter the call cost per charging unit set by the line provider. The values are 1/10,000th of a currency unit. For example if the call cost per unit is £1.07, a value of 10700 should be set on the line. Refer to Advice of Charge.
Send original calling party for forwarded and twinning calls	Default = Off. Use the original calling party ID when forwarding calls or routing twinned calls. This setting applies to BRI lines with subtype ETSI.
Originator number for forwarded and twinning calls	Default = blank. The number used as the calling party ID when forwarding calls or routing twinned calls. This field is grayed out when the **Send original calling party for forwarded and twinning calls** setting is enabled. This setting applies to BRI lines with subtype ETSI.

Related links

BRI Line on page 386

Channels

Navigation: **System Settings** > **Line** > **Add/Edit Trunk Line** > **BRI Line** > **Channels**

This tab allows settings for individual channels within the trunk to be adjusted. To edit a channel either double-click on it or click the channel and then select **Edit**.

To edit multiple channels at the same time, select the required channels using Ctrl or Shift and then click **Edit**. When editing multiple channels, fields that must be unique such as **Line Appearance ID** are not shown.

These settings can be edited online.

Field	Description
Line Appearance ID	Default = Auto-assigned. Range = 2 to 9 digits. Used for configuring Line Appearances with button programming. The line appearance ID must be unique and not match any extension number. Line appearance is not supported for trunks set to QSIG operation and is not recommended for trunks be used for DID.

Related links

BRI Line on page 386

PRI Trunks

PRI trunks are provided by the installation of a PRI trunk card into the control unit. avThe IP500 PRI-U trunk card can be configured (see below) to one of those line types. The cards are also available with either 1 or 2 physical ports. The number of B-channels supported by each physical port depends on the line type of the card.

- **E1**: 30 B-channels and 1 D-channel per port.
- **T1**: 24 B-channels per port.

- **US PRI**: 23 B-channels and 1 D-channel per port.
- **E1-R2**: 30 B-channels and 1 D-channel per port.

IP500 PRI-U Trunk Card Line Type

The IP500 PRI-U card can be configured to support either E1, T1 or E1-R2 PRI line types. To select the line type required, right-click on the line in the group or navigation pane and select **Change Universal PRI Card Line Type**.

The control unit supports 8 B-channels on each IP500 PRI-U card fitted. Additional B-channels up to the full capacity of IP500 PRI-U ports installed require licenses added to the configuration. D-channels are not affected by licensing.

For ETSI and QSIG trunks, license instances are consumed by the number of calls in progress on B-channels.

For T1, E1R2 and ETSI CHI trunks, licenses instances are consumed by the channels set as in service.

Related links

Add Trunk Line on page 308
E1 Line on page 392
E1 R2 Line on page 401
T1 Line on page 406
T1 PRI Line on page 412

E1 Line

Related links

PRI Trunks on page 391
E1 PRI Line on page 392
E1 Short Codes on page 398
E1 PRI Channels on page 399

E1 PRI Line

Navigation: **System Settings** > **Line** > **E1 PRI Line**

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Line Number	This parameter is not configurable; it is allocated by the system.

Table continues…

Field	Description
Line Sub Type	Select to match the particular line type provided by the line provider. The options are: • **ETSI** • **ETSI CHI** • **QSIG A** • **QSIG B** **ETSI CHI** is used to send the channel allocation ID (CHI) in the call setup signalling. This is a request to use a particular B-channel rather than use any B-channel allocated by the central office exchange. QSIG trunks trunks are not supported on IP500 V2 systems without IP500 Voice Networking licenses.
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Network Type	Default = Public. This option is available if **System Settings** > **System** > **Telephony** > **Restrict Network Interconnect** is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Telephone Number	Used to remember the external telephone number of this line to assist with loop-back testing. For information only.
Channel Allocation	Default = 30|1. For lines set to **ETSI CHI**, this option allows the system to select the default order in which channels should be used for outgoing calls. Typically this is set as the opposite of the default order in which the central office exchange uses channels for incoming calls. For lines set to the **Line Sub Type** of **ETSI CHI**, the **Incoming Group ID** is set as part of the individual channel settings.
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.

Table continues…

Field	Description
Outgoing Group ID	Default = 1. Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID. In a Server Edition network, the **Outgoing Group ID** used on a system must also be unique within the network. The same ID cannot be used in the configuration of any lines on another server system in the network. For Standard Edition deployments, the same ID can be used for multiple lines. **Reserved Group ID Numbers:** • **90000 - 99999** Reserved for system use (not enforced). • **99999 and 99998** In a Server Edition network, reserved for the IP Office lines to the Primary Server and Secondary Server respectively. • **99901 to 99930** In a Server Edition network, reserved for the IP Office lines from the Primary Server to each expansion system in the network. • **0** In a Server Edition network, the ID 0 cannot be used. • **98888** For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.
Prefix	Default = Blank. The prefix is used in the following ways: • **For incoming calls** The ISDN messaging tags indicates the call type (National, International or Unknown). If the call type is unknown, then the number in the Prefix field is added to the ICLID. • **For outgoing calls** The prefix is not stripped, therefore any prefixes not suitable for external line presentation should be stripped using short codes.
National Prefix	Default = 0 This indicates the digits to be prefixed to a incoming national call. When a number is presented from ISDN as a "national number" this prefix is added. For example 1923000000 is converted to 01923000000.
International Prefix	Default = 00 This indicates the digits to be prefixed to an incoming international call. When a number is presented from ISDN as an "international number" this prefix is added. For example 441923000000 is converted to 00441923000000.
TEI	Default = 0 The Terminal Equipment Identifier. Used to identify each Control Unit connected to a particular ISDN line. For Point to Point lines this is typically (always) 0. It can also be 0 on a Point to Multi-Point line, however if multiple devices are sharing a Point to Multi-Point line it should be set to 127 which results in the exchange deciding on the TEI's to be used.
Number of Channels	Defines the number of operational channels that are available on this line. Up to 30 for E1 PRI, 23 for T1 PRI.

Table continues…

Field	Description
Outgoing Channels	This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as **Number of Channels** field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls. Only available when the **Line Sub Type** is set to **ETSI**.
Voice Channels	The number of channels available for voice use. Only available when the **Line Sub Type** is set to **ETSI**.
Data Channels	The number of channels available for data use. Only available when the **Line Sub Type** is set to **ETSI**.
CRC Checking	Default = On Switches CRC on or off.
Line Signalling	Default = CPE This option is not used for lines where the **Line SubType** is set to **QSIG**. Select either **CPE** (customer premises equipment) or **CO** (central office). The **CO** feature is intended to be used primarily as a testing aid. It allows PRI lines to be tested in a back-to-back configuration, using crossover cables. The CO feature operates on this line type by modifying the way in which incoming calls are disconnected for system configuration in Brazil and Argentina. In these locales, the CO setting uses Forced-Release instead of Clear-Back to disconnect incoming calls. The Brazilian Double-Seizure mechanism, used to police Collect calls, is also disabled in CO mode.
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available. • Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source. • In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.

Table continues…

Field	Description
Add 'Not-end-to-end ISDN' Information Element	Default = Never Sets whether the optional 'Not end-to-end ISDN' information element should be added to outgoing calls on the line. The options are: • **Never** • **Always** • **POTS**(only if the call was originated by an analog extension). The default is **Never** except for the following locales; for Italy the default is **POTS**, for New Zealand the default is **Always**.
Progress Replacement	Default = None. Progress messages are defined in the Q.931 ISDN connection control signaling protocol. Generally, If a progress message is sent, the caller does not get connected and so typically does not accrue call costs. Not all ISDN lines support Q.931 Progress messages. Use this setting to configure alternative signaling to the ISDN line for internally generated Progress messages. The options are: • **Alerting**: Map to Q.931 Alerting. The call is not connected. The caller does not hear the message and typically does not accrue call costs. • **Connect**: Map to Q.931 Connect. The caller hears the message and typically will accrue call costs.
Supports Partial Rerouting	Default = Off. Partial rerouting (PR) is an ISDN feature. It is supported on external (non-network and QSIG) ISDN exchange calls. When an external call is transferred to another external number, the transfer is performed by the ISDN exchange and the channels to the system are freed. Use of this service may need to be requested from the line provider and may incur a charge.
Force Number Plan to ISDN	Default = Off. This option is only configurable when **Support Partial Rerouting** is also enabled. When selected, the plan/type parameter for Partial Rerouting is changed from **Unknown/Unknown** to **ISDN/Unknown**.
Send Redirecting Number	Default = Off. This option can be used on ISDN trunks where the redirecting service is supported by the trunk provider. Where supported, on twinned calls the caller ID of the original call is passed through to the twinning destination. This option is only used for twinned calls.

Table continues…

Field	Description
Support Call Tracing	Default = Off. The system supports the triggering of malicious caller ID (MCID) tracing at the ISDN exchange. Use of this feature requires liaison with the ISDN service provider and the appropriate legal authorities to whom the call trace will be passed. The user will also need to be enabled for call tracing and be provider with either a short code or programmable button to activate MCID call trace. Refer to Malicious Call Tracing in the Telephone Features section for full details.
Active CCBS Support	Default = Off. Call completion to a busy subscriber (CCBS). It allows automatic callback to be used on outgoing ISDN calls when the destination is busy. This feature can only be used on point-to-point trunks. Use of this service may need to be requested from the line provider and may incur a charge.
Passive CCBS	Default = Off.
Cost Per Charging Unit	Advice of charge (AOC) information can be display on T3/T3IP phones and output in SMDR. The information is provided in the form of charge units. This setting is used to enter the call cost per charging unit set by the line provider. The values are 1/10,000th of a currency unit. For example if the call cost per unit is £1.07, a value of 10700 should be set on the line. Refer to Advice of Charge.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.
Send original calling party for forwarded and twinning calls	Default = Off. Use the original calling party ID when forwarding calls or routing twinned calls. This setting applies to the following ISDN lines: • PRI24 with subtypes: - PRI - QSIGA - QSIGB - ETSI - ETSI CHI • PRI30 with subtypes - QSIGA - QSIGB - ETSI - ETSI CHI

Table continues…

Field	Description
Originator number for forwarded and twinning calls	Default = blank. The number used as the calling party ID when forwarding calls or routing twinned calls. This field is grayed out when the **Send original calling party for forwarded and twinning calls** setting is enabled. This setting applies to the following ISDN lines: • PRI24 with subtypes: - PRI - QSIGA - QSIGB - ETSI - ETSI CHI • PRI30 with subtypes - QSIGA - QSIGB - ETSI - ETSI CHI

The following fields are shown for a US T1 trunk card set to ETSI or QSIG operation. These cards have the same settings E1 PRI trunk cards set to ETSI or QSIG but only support 23 channels.

These settings are not mergeable. Changing these settings requires a system reboot.

Field	Description
CSU Operation	Check this field to enable the T1 line to respond to loop-back requests from the line.
Haul Length	Default = 0-115 feet Sets the line length to a specific distance.
Channel Unit	Default = Foreign Exchange This field should be set to match the channel signaling equipment provided by the Central Office. The options are Foreign Exchange, Special Access or Normal.

Related links

E1 Line on page 392

E1 Short Codes

Navigation: **System Settings** > **Line** > **E1 Short Codes**

For some types of line, Line short codes can be applied to any digits received with incoming calls.

The line Short Code tab is shown for the following trunk types which are treated as internal or private trunks: **QSIG** (T1, E1, H.323), **BRI S0**, **H.323**, **SCN**, **IP Office**. Incoming calls on those types of trunk are not routed using **Incoming Call Route** settings. Instead the digits received with incoming calls are checked for a match as follows:

Extension number (including remote numbers in a multi-site network).

- Line short codes (excluding ? short code).
- System short codes (excluding ? short code).
- Line ? short code.
- System ? short code.

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

These settings can be edited online.

Related links

E1 Line on page 392

E1 PRI Channels

Navigation: **System Settings** > **Line** > **E1 PRI Channels**

This tab allows settings for individual channels within the trunk to be adjusted. To edit a channel either double-click on it or click the channel and then select **Edit**.

To edit multiple channels at the same time, select the required channels using Ctrl or Shift and then click **Edit**. When editing multiple channels, fields that must be unique such as **Line Appearance ID** are not shown.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Line Appearance ID	Default = Auto-assigned. Range = 2 to 9 digits. Used for configuring Line Appearances with button programming. The line appearance ID must be unique and not match any extension number. Line appearance is not supported for trunks set to QSIG operation and is not recommended for trunks be used for DID. If the trunk **Line Sub Type** is set to **ETSI CHI**, outgoing line appearance calls must use the corresponding channel.

The following additional fields are shown for lines where the **Line Sub Type** is set to **ETSI CHI**.

Field	Description
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.

Table continues…

Field	Description
Outgoing Group ID	Default = 1. Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID. In a Server Edition network, the **Outgoing Group ID** used on a system must also be unique within the network. The same ID cannot be used in the configuration of any lines on another server system in the network. For Standard Edition deployments, the same ID can be used for multiple lines. **Reserved Group ID Numbers:** • **90000 - 99999** Reserved for system use (not enforced). • **99999 and 99998** In a Server Edition network, reserved for the IP Office lines to the Primary Server and Secondary Server respectively. • **99901 to 99930** In a Server Edition network, reserved for the IP Office lines from the Primary Server to each expansion system in the network. • **0** In a Server Edition network, the ID 0 cannot be used. • **98888** For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.
Direction	Default = Bothways The direction of calls on the channel. The options are: • **Incoming** • **Outgoing** • **Bothways**
Bearer	Default = Any The type of traffic carried by the channel. The options are: • **Voice** • **Data** • **Any**
Admin	Default = Out of Service. This field can be used to indicate whether the channel is in use or not. On trunks where only a limited number of channels have been requested from the trunk provider (known as sub-equipped trunks), those channels not provided should be set as **Out of Service**. For channels that are available but are temporarily not being used select **Maintenance**.
Tx Gain	Default = 0dB. Range = -10dBb to +5dB. The transmit gain in dB.
Rx Gain	Default = 0dB. Range = -10dBb to +5dB. The receive gain in dB.

Related links

E1 Line on page 392

E1 R2 Line

Related links

PRI Trunks on page 391
E1-R2 Options on page 401
E1-R2 Channels on page 402
E1–R2 MFC Group on page 404
E1-R2 Advanced on page 405

E1-R2 Options

Navigation: **System Settings** > **Line** > **E1–R2 Options**

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Network Type	Default = Public. This option is available if **System Settings** > **System** > **Telephony** > **Restrict Network Interconnect** is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Line Number	Allocated by the system.

Table continues…

Field	Description
Line SubType	Default = E1-R2 The options are: • **E1-R2** • **ETSI** • **QSIGA** • **QSIGB** QSIG trunks trunks are not supported on IP500 V2 systems without IP500 Voice Networking licenses.
Channel Allocation	Default = 30 | 1 The order, **30 | 1** or **1 | 30**, in which channels are used.
Country (Locale)	Default = Mexico. Select the locale that matches the area of usage. Note that changing the locale will return the MFC Group settings to the defaults for the selected locale. Currently supported locales are: • **Argentina** • **Brazil** • **China** • **India** • **Korea** • **Mexico** • **None**
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected. The table at the base of the form displays the settings for the individual channels provided by the line. For details of the channel settings see the E1-R2 Channel form. To edit a channel, either double-click on it or right-click and select **Edit**. This will display the Edit Channel dialog box. To edit multiple channels at the same time select the channels whilst pressing the Shift or Ctrl key. Then right-click and select **Edit**.

Related links

E1 R2 Line on page 401

E1-R2 Channels

Navigation: **System Settings** > **Line** > **E1–R2 Channels**

The channel settings are split into two sub-tabs, **E1R2 Edit Channel** and **Timers**.

The **Timers** tab displays the various timers provided for E1-R2 channels. These should only be adjusted when required to match the line provider's settings.

This tab allows settings for individual channels within the trunk to be adjusted. To edit a channel, select the required channel or channels and click **Edit**.

The following settings are mergeable:

- **Incoming Group ID**
- **Outgoing Group ID**
- **Admin**

The remaining settings are not mergeable. Changes to these settings require a system reboot.

Field	Descriptions
Channel	The channel or channels being edited.
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.
Outgoing Group ID	Default = 1. Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID. In a Server Edition network, the **Outgoing Group ID** used on a system must also be unique within the network. The same ID cannot be used in the configuration of any lines on another server system in the network. For Standard Edition deployments, the same ID can be used for multiple lines. **Reserved Group ID Numbers:** • **90000 - 99999** Reserved for system use (not enforced). • **99999 and 99998** In a Server Edition network, reserved for the IP Office lines to the Primary Server and Secondary Server respectively. • **99901 to 99930** In a Server Edition network, reserved for the IP Office lines from the Primary Server to each expansion system in the network. • **0** In a Server Edition network, the ID 0 cannot be used. • **98888** For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.
Direction	Default = Both Directions The direction of calls on the channel. The options are: • **Incoming** • **Outgoing** • **Both Directions**

Table continues…

Field	Descriptions
Bearer	Default = Any The type of traffic carried by the channel. The options are: • **Voice** • **Data** • **Any**
Admin	Default = Out of Service. This field can be used to indicate whether the channel is in use or not. On trunks where only a limited number of channels have been requested from the trunk provider (known as sub-equipped trunks), those channels not provided should be set as **Out of Service**. For channels that are available but are temporarily not being used select **Maintenance**.
Line Signaling Type	Default = R2 Loop Start The signaling type used by the channel. Current supported options are: • **R2 Loop Start** • **R2 DID** • **R2 DOD** • **R2 DIOD** • **Tie Immediate Start** • **Tie Wink Start** • **Tie Delay Dial** • **Tie Automatic** • **WAN Service** • **Out of Service**
Dial Type	Default = MFC Dialing The type of dialing supported by the channel. The options are:, or . • **MFC Dialing** • **Pulse Dialing** • **DTMF Dialing**

Related links

E1 R2 Line on page 401

E1–R2 MFC Group

Navigation: **System Settings** > **Line** > **E1–R2 MFC Group**

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

These tabs show the parameter assigned to each signal in an MFC group. The defaults are set according to the Country (Locale) on the Line tab. All the values can be returned to default by the **Default All** button on the **Advanced** tab.

These settings are not mergeable. Changes to these settings will require a reboot of the system.

To change a setting either double-click on it or right-click and select **Edit**.

Related links

E1 R2 Line on page 401

E1-R2 Advanced

Navigation: **System Settings** > **Line** > **E1–R2 Advanced**

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Zero Suppression	Default = HDB3 Selects the method of zero suppression used (HDB3 or AMI).
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available. • Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source. • In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.

Table continues…

Field	Description
Line Signaling	Default = CPE The options are: • **CPE** • **CO** • **CO** The feature is intended to be used primarily as a testing aid. It allows T1 and E1 lines to be tested in a back-to-back configuration, using crossover (QSIG) cables. The CO feature operates by modifying the way in which incoming calls are disconnected for system configuration in Brazil and Argentina. In these locales, the CO setting uses Forced-Release instead of Clear-Back to disconnect incoming calls. The Brazilian Double-Seizure mechanism used to police Collect calls, is also disabled in CO mode.
Incoming Routing Digits	Default = 4 Sets the number of incoming digits used for incoming call routing.
CRC Checking	Default = On Switches CRC on or off.
Default All Group Settings	Default the MFC Group tab settings.
Line Signaling Timers	To edit one of these timers, either double-click on the timer or right-click on a timer and select the action required.

Related links

E1 R2 Line on page 401

T1 Line

Related links

PRI Trunks on page 391
US T1 Line on page 406
T1 Channels on page 409

US T1 Line

Navigation: **System Settings** > **Line** > **US T1 Line**

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Line Number	Allocated by the system.

Table continues…

Field	Description
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Network Type	Default = Public. This option is available if **System Settings** > **System** > **Telephony** > **Restrict Network Interconnect** is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Line Sub Type	Default = T1 Set to T1 for a T1 line.
Channel Allocation	Default = 24 | 1 The order, 24 to 1 or 1 to 24, in which channels are used.
Prefix	Default = Blank Enter the number to prefix to all incoming numbers for callback. This is useful if all users must dial a prefix to access an outside line. The prefix is automatically placed in front of all incoming numbers so that users can dial the number back.
Framing	Default = ESF Selects the type of signal framing used. The options are: • **ESF** • **D4**
Zero Suppression	Default = B8ZS Selects the method of zero suppression used. The options are: • **B8ZS** • **AMI ZCS**

Table continues…

Field	Description
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available. • Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source. • In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.
Haul Length	Default = 0-115 feet. Sets the line length to a specific distance.
Channel Unit	Default = Foreign Exchange This field should be set to match the channel signaling equipment provided by the Central Office. The options are: • **Foreign Exchange** • **Special Access** • **Normal**
CRC Checking	Default = On Turns CRC on or off.
Line Signaling	Default = CPE This field affects T1 channels set to Loop-Start or Ground-Start. The field can be set to either CPE (Customer Premises Equipment) or CO (Central Office). This field should normally be left at its default of CPE. The setting CO is normally only used in lab back-to-back testing.
Incoming Routing Digits	Default=0 (present call immediately) Sets the number of routing digits expected on incoming calls. This allows the line to present the call to the system once the expected digits have been received rather than waiting for the digits timeout to expire. This field only affects T1 line channels set to E&M Tie, E&M DID, E&M Switched 56K and Direct Inward Dial.

Table continues…

Field	Description
CSU Operation	Enable this field to enable the T1 line to respond to loop-back requests from the line.
Enhanced Called Party Number	Default = Off This option is not supported for systems set to the United States locale. Normally the dialed number length is limited to 15 digits. Selecting this option increases the allowed dialed number length to 30 digits.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.

Related links

T1 Line on page 406

T1 Channels

Navigation: **System Settings** > **Line** > **T1 Channels**

The settings for each channel can be edited. Users have the option of editing individual channels by double-clicking on the channel or selecting and editing multiple channels at the same time. Note that the Line Appearance ID cannot be updated when editing multiple channels.

When editing a channel or channels, the settings available are displayed on two sub-tabs; T1 Edit Channel and Timers.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Channel	Allocated by the system.
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.

Table continues…

Field	Description
Outgoing Group ID	Default = 1. Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID. In a Server Edition network, the **Outgoing Group ID** used on a system must also be unique within the network. The same ID cannot be used in the configuration of any lines on another server system in the network. For Standard Edition deployments, the same ID can be used for multiple lines. **Reserved Group ID Numbers:** • **90000 - 99999** Reserved for system use (not enforced). • **99999 and 99998** In a Server Edition network, reserved for the IP Office lines to the Primary Server and Secondary Server respectively. • **99901 to 99930** In a Server Edition network, reserved for the IP Office lines from the Primary Server to each expansion system in the network. • **0** In a Server Edition network, the ID 0 cannot be used. • **98888** For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.
Line Appearance ID	Default = Auto-assigned. Range = 2 to 9 digits. Used for configuring Line Appearances with button programming. The line appearance ID must be unique and not match any extension number. Line appearance is not supported for trunks set to QSIG operation and is not recommended for trunks be used for DID.
Direction	Default = Bothway The direction of calls on the channel. The options are: • **Incoming** • **Outgoing** • **Bothway**
Bearer	Default = Any The type of traffic carried by the channel. The options are: • **Voice** • **Data** • **Any**
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.

Table continues…

Field	Description
Type	Default = Loop-Start. The T1 emulates the following connections: • **Ground-Start** • **Loop-Start** • **E&M - TIE** • **E&M - DID** • **E&M Switched 56K** • **Direct Inward Dial** • **Clear Channel 64K** Trunks set to **E&M - DID** will only accept incoming calls. If **E&M - TIE** is selected and the **Outgoing Trunk Type** is set to **Automatic**, no secondary dial tone is provided for outgoing calls on this line/trunk.
Dial Type	Default = DTMF Dial Select the dialing method required. The options are: • **DTMF Dial** • **Pulse Dial**
Incoming Trunk Type	Default = Wink-Start Used for E&M types only. The handshake method for incoming calls. The options are: • **Automatic** • **Immediate** • **Delay Dial** • **Wink-Start**
Outgoing Trunk Type	Default = Wink-Start Used for E&M types only. The handshake method for outgoing calls. The options are: • **Automatic** • **Immediate** • **Delay Dial** • **Wink-Start** If the line Type is set to **E&M-TIE** and the **Outgoing Trunk Type** is set to **Automatic**, no secondary dial tone is provided for outgoing calls on this line/trunk.
Tx Gain	Default = 0dB. The transmit gain in dB.

Table continues…

Field	Description
Rx Gain	Default = 0dB. The receive gain in dB.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.

Timer Settings

This sub-tab allows various timers relating to operation of an individual channel to be adjusted. These should only be adjusted to match the requirements of the line provider. The following is a list of the default values. To reset a value, click on the current value and then right click and select from the default, minimize and maximize options displayed.

Incoming Automatic Delay: 410.

Incoming Wink Delay: 100.

Wink Signal: 200.

Incoming Dial Guard: 50.

First Incoming Digit: 15000.

Incoming Inter Digit: 5000.

Maximum Inter Digit: 300.

Flash Hook Detect: 240.

Incoming Disconnect: 300.

Incoming Disconnect Guard: 800.

Disconnected Signal Error: 240000.

Outgoing Disconnect: 300.

Outgoing Disconnect Guard: 800.

Ring Verify Duration: 220.

Ring Abandon: 6300.

Ping Verify: 600.

Long Ring Time: 1100.

Silent Interval: 1100.

Outgoing Seizure: 10.

Wink Start: 5000.

Wink Validated: 80.

Wink End: 350.

Delay End: 5000.

Outgoing Dial Guard: 590.

Outgoing IMM Dial Guard: 1500.

Outgoing Pulse Dial Break: 60.

Outgoing Pulse Dial Make: 40.

Outgoing Pulse Dial Inter Digit: 720.

Outgoing Pulse Dial Pause: 1500.

Flash Hook Generation: 500.

Outgoing End of Dial: 1000.

Answer Supervision: 300.

Incoming Confirm: 20.

Related links

T1 Line on page 406

T1 PRI Line

Related links

PRI Trunks on page 391
T1 ISDN on page 413
T1 ISDN Channels on page 417

T1 ISDN TNS on page 419
T1 ISDN Special on page 420
Call By Call (US PRI) on page 421

T1 ISDN

Navigation: **System Settings** > **Line** > **T1 ISDN Line**

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Variable	Description
Line Number	Allocated by the system.
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Network Type	Default = Public. This option is available if **System Settings** > **System** > **Telephony** > **Restrict Network Interconnect** is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Line Sub Type	: Default = PRI Set to **PRI**. If set to T1 see Line Form (T1). If set to **ETSI**, **ETSI CHI**, **QSIG A** or **QSIG B** see Line (E1). QSIG trunks trunks are not supported on IP500 V2 systems without IP500 Voice Networking licenses.
Channel Allocation	Default = 23 | 1 The order, 23 to 1 or 1 to 23, in which channels are used.
Switch Type	Default = NI2 The options are • **4ESS** • **5ESS** • **DMS100** • **NI2**

Table continues…

Variable	Description
Provider	Default = Local Telco Select the PSTN service provider (**AT&T**, **Sprint**, **WorldCom** or **Local Telco**).
Prefix	Default = Blank Enter the number to prefix to all incoming numbers for callback. This is useful if all users must dial a prefix to access an outside line. The prefix is automatically placed in front of all incoming numbers so that users can dial the number back.
Add 'Not-end-to-end ISDN' Information Element	Default = Never*. Sets whether the optional 'Not end-to-end ISDN' information element should be added to outgoing calls on the line. The options are • **Never** • **Always** • **POTS** (only if the call was originated by an analog extension) *The default is **Never** except for the following locales; for Italy the default is **POTS**, for New Zealand the default is **Always**.
Progress Replacement	Default = None. Progress messages are defined in the Q.931 ISDN connection control signaling protocol. Generally, If a progress message is sent, the caller does not get connected and so typically does not accrue call costs. Not all ISDN lines support Q.931 Progress messages. Use this setting to configure alternative signaling to the ISDN line for internally generated Progress messages. The options are: • **Alerting**: Map to Q.931 Alerting. The call is not connected. The caller does not hear the message and typically does not accrue call costs. • **Connect**: Map to Q.931 Connect. The caller hears the message and typically will accrue call costs.
Send Redirecting Number	Default = Off. This option can be used on ISDN trunks where the redirecting service is supported by the trunk provider. Where supported, on twinned calls the caller ID of the original call is passed through to the twinning destination. This option is only used for twinned calls.
Send Names	This option is available when the **Switch Type** above is set to **DMS100**. If set, names are sent in the display field. The **Z** shortcode character can be used to specify the name to be used.
Names Length	Set the allowable length for names, up to 15 characters, when **Send Names** is set above.
Test Number	Used to remember the external telephone number of this line to assist with loop-back testing. For information only.

Table continues…

Variable	Description
Framing	Default = ESF Selects the type of signal framing used (ESF or D4).
Zero Suppression	Default = B8ZS Selects the method of zero suppression used (B8ZS or AMI ZCS).
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available. • Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source. • In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.
CSU Operation	Tick this field to enable the T1 line to respond to loop-back requests from the line.
Haul Length	Default = 0-115 feet Sets the line length to a specific distance.
Channel Unit	Default = Foreign Exchange This field should be set to match the channel signaling equipment provided by the Central Office. The options are • **Foreign Exchange** • **Special Access** • **Normal**
CRC Checking	Default = On Turns CRC on or off.
Line Signaling	The field can be set to either **CPE** (Customer Premises Equipment) or **CO** (Central Office). This field should normally be left at its default of **CPE**. The setting **CO** is normally only used in lab back-to-back testing.

Table continues…

Variable	Description
Incoming Routing Digits	Default=0 (present call immediately) Sets the number of routing digits expected on incoming calls. This allows the line to present the call to the system once the expected digits have been received rather than waiting for the digits timeout to expire. This field only affects T1 line channels set to **E&M Tie**, **E&M DID**, **E&M Switched 56K** and **Direct Inward Dial**.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.
Send original calling party for forwarded and twinning calls	Default = Off. Use the original calling party ID when forwarding calls or routing twinned calls. This setting applies to the following ISDN lines: • PRI24 with subtypes: - PRI - QSIGA - QSIGB - ETSI - ETSI CHI • PRI30 with subtypes - QSIGA - QSIGB - ETSI - ETSI CHI

Table continues…

Variable	Description
Originator number for forwarded and twinning calls	Default = blank. The number used as the calling party ID when forwarding calls or routing twinned calls. This field is grayed out when the **Send original calling party for forwarded and twinning calls** setting is enabled. This setting applies to the following ISDN lines: • PRI24 with subtypes: - PRI - QSIGA - QSIGB - ETSI - ETSI CHI • PRI30 with subtypes - QSIGA - QSIGB - ETSI - ETSI CHI

Related links

T1 PRI Line on page 412

T1 ISDN Channels

Navigation: **System Settings** > **Line** > **T1 ISDN Channels**

This tab allows settings for individual channels within the trunk to be adjusted. This tab is not available for trunks sets to ETSI or QSIG mode.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Channel	Allocated by the system.
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.

Table continues…

Field	Description
Outgoing Group ID	Default = 1. Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID. In a Server Edition network, the **Outgoing Group ID** used on a system must also be unique within the network. The same ID cannot be used in the configuration of any lines on another server system in the network. For Standard Edition deployments, the same ID can be used for multiple lines. **Reserved Group ID Numbers:** • **90000 - 99999** Reserved for system use (not enforced). • **99999 and 99998** In a Server Edition network, reserved for the IP Office lines to the Primary Server and Secondary Server respectively. • **99901 to 99930** In a Server Edition network, reserved for the IP Office lines from the Primary Server to each expansion system in the network. • **0** In a Server Edition network, the ID 0 cannot be used. • **98888** For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.
Line Appearance ID	Default = Auto-assigned. Range = 2 to 9 digits. Used for configuring Line Appearances with button programming. The line appearance ID must be unique and not match any extension number.
Direction	Default = Both Directions The direction of calls on the channel. The options are: • **Incoming** • **Outgoing** • **Both Directions**
Bearer	Default = Any The type of traffic carried by the channel. The options are: • **Voice** • **Data** • **Any**

Table continues…

Field	Description
Service	Default = None. If the line provider is set to AT&T, select the type of service provided by the channel. The options are: • **Call by Call** • **SDN (inc GSDN)** • **MegaCom 800** • **MegaCom** • **Wats** • **Accunet** • **ILDS** • **I800** • **ETN** • **Private Line** • **AT&T Multiquest** For other providers, the service options are **None** or **No Service**.
Admin	Default = Out of Service Used to indicate the channel status. The options are: • **In Service** • **Out of Service** • **Maintenance**
Tx Gain	Default = 0dB The transmit gain in dB
Rx Gain	Default = 0dB The receive gain in dB.

Related links

T1 PRI Line on page 412

T1 ISDN TNS

Navigation: **System Settings** > **Line** > **T1 ISDN TNS**

This tab is shown when the line Provider is set to AT&T. It allows the entry of the Network Selection settings. These are prefixes for alternative long distance carriers. When a number dialed matches an entry in the table, that pattern is stripped from the number before being sent out. This table is used to set field in the TNS (Transit Network Selection) information element for 4ESS and 5ESS exchanges. It is also used to set fields in the NSF information element.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
TNS Code	The pattern for the alternate long distance carrier. For example: The pattern 10XXX is added to this tab. If 10288 is dialed, 10 is removed and 288 is placed in the TNS and NSF information.

Related links

T1 PRI Line on page 412

T1 ISDN Special

Navigation: **System Settings** > **Line** > **T1 ISDN Special**

This tab is shown when the line Provider is set to AT&T. This table is used to set additional fields in the NSF information element after initial number parsing by the TNS tab. These are used to indicate the services required by the call. If the channel is set to Call by Call, then further parsing is done using the records in the Call by Call tab.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Short code	The number which results from the application of the rules specified in the User or System Short code tables and the Network Selection table and the Call-by-call table to the number dialed by the user.
Number	The number to be dialed to line.
Special	Default = No Operator. The options are: • **No Operator** • **Local Operator** • **Presubscribed Operator**
Plan	Default = National. The options are: • **National** • **International**

Typical values are:

Short Code	Number	Service
011N	N	No Operator, International
010N	N	Local Operator, International
01N	N	Local Operator, National
00N	N	Presubscribed Operator, National
0N	N	Presubscribed Operator, National
1N	1N	No operator, National

Related links

T1 PRI Line on page 412

Call By Call (US PRI)

Navigation: **System Settings** > **Line** > **T1 ISDN Call by Call**

This tab is shown when the line Provider is set to AT&T. Settings in this tab are only used when calls are routed via a channel which has its **Service** set to **Call by Call**.

It allows short codes to be created to route calls to a different services according to the number dialed. Call By Call reduces the costs and maximizes the use of facilities. Call By Call chooses the optimal service for a particular call by including the Bearer capability in the routing decision. This is particularly useful when there are limited resources.

These settings must be edited offline. To enter offline editing, select **Menu Bar Current User Icon** > **Offline Mode**.

Field	Description
Short Code	The number which results from the application of the rules specified in the User or System Short code tables and the Network Selection table to the number dialed by the user.
Number	The number to be dialed to line.
Bearer	Default = Any The type of traffic carried by the channel. The options are: • **Voice** • **Data** • **Any**
Service	Default = AT&T The service required by the call. The options are: • **Call by Call** • **SDN (inc GSDN)** • **MegaCom 800** • **MegaCom** • **Wats** • **Accunet** • **ILDS** • **I800** • **ETN** • **Private Line** • **AT&T Multiquest**

Related links

T1 PRI Line on page 412

Firewall Profile

Navigation: **System Settings** > **Firewall Profile**

The **Firewall Profile** main content pane lists provisioned firewall profiles. The contents of the list depends on the filter options selected. Click the icons beside a record to edit or delete.

Click **Add/Edit Firewall Profile** to open the Add Firewall page where you can provision a firewall. When you click **Add/Edit Firewall Profile**, you are prompted to specify the server where the firewall will be applied.

Related links

System Settings on page 194
Add Firewall Profile on page 422

Add Firewall Profile

Navigation: **System Settings** > **Firewall Profile** > **Add/Edit Firewall Profile**

Additional configuration information

This type of configuration record can be saved as a template and new records created from a template. See Working with Templates on page 518.

Configuration settings

The system can act as a firewall, allowing only specific types of data traffic to start a session across the firewall and controlling in which direction such sessions can be started.

The system supports Static NAT address translation by a firewall profiles. If the Firewall Profile contains any Static NAT records, all packets received by the firewall must match one of those static NAT records to not be blocked.

If Network Address Translation (NAT) is used with the firewall (which it typically is), then you must also configure the setting **System Settings** > **Services** > **Add/Edit Service** > **Normal / WAN / Internet** > **Primary Trans. IP Address** if you wish sessions to be started into your site (typically for SMTP) from the Internet.

On Server Edition Linux systems, to ensure that the firewall starts after a reboot, you must enable the **Activate** setting in the Web Control menus. See *Using the Server Edition Web Control Menus*.

System firewall profiles can be applied in the following areas of operation.

System:

A firewall profile can be selected to be applied to traffic between LAN1 and LAN2.

User:

Users can be used as the destination of incoming RAS calls. For those users a firewall profile can be selected on the user's Dial In tab.

Service:

Services are used as the destination for IP routes connection to off-switch data services such as the internet. A Firewall Profile can be selected for use with a service.

By default, any protocol not listed in the standard firewall list is dropped unless a custom firewall entry is configured for that protocol.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

Field	Description		
Name	Range = Up to 15 characters. Enter the name to identify this profile.		
Protocol Control	For each of the listed protocols, the options **Drop**, **In** (Incoming traffic can start a session), **Out** (Outgoing traffic can start a session) and **Both Directions** can be selected. Once a session is started, return traffic for that session is also able to cross the firewall.		
	Protocol	**Default**	**Description**
	TELNET	Out	Remote terminal log in.
	FTP	Out	File Transfer Protocol.
	SMTP	Out	Simple Mail Transfer Protocol.
	TIME	Out	Time update protocol.
	DNS	Out	Domain Name System.
	GOPHER	Drop	Internet menu system.
	FINGER	Drop	Remote user information protocol.
	RSVP	Drop	Resource Reservation Protocol.
	HTTP/S	Bothway	Hypertext Transfer Protocol.
	POP3	Out	Post Office Protocol.
	NNTP	Out	Network News Transfer Protocol.
	SNMP	Drop	Simple Network Management Protocol.
	IRC	Out	Internet Relay Chat.
	PPTP	Drop	Point to Point Tunneling Protocol.
	IGMP	Drop	Internet Group Membership Protocol.
Service Control	For each of the listed services, the options **Drop**, **In**, **Out** and **Both Directions** can be selected. Once a session is started, return traffic for that session is also able to cross the firewall.		

Table continues…

Field	Description		
	Protocol	**Default**	**Description**
	SSI	In	System Status Application access.
	SEC	Drop	TCP security settings access.
	CFG	Drop	TCP configuration settings access.
	TSPI	In	TSPI service access.
	WS	Drop	IP Office web management services.

Related links

Firewall Profile on page 422

Authorization Code

Navigation: **System Settings** > **Authorization Code**

The **Authorization Code** main content pane lists provisioned authorization codes. The contents of the list depends on the filter options selected. Click the icons beside a record to edit or delete.

Click **Add/Edit Authorization Code** to open the Authorization Codes page where you can provision an authorization code. When you click **Add/Edit Authorization Code**, you are prompted to specify the server where the authorization code will be applied.

Related links

System Settings on page 194
Add Authorization Code on page 424

Add Authorization Code

Navigation: **System Settings** > **Authorization Code** > **Add/Edit Authorization Code**

Note:

In release 9.1, authorization codes can no longer be associated with User Rights. If an authorization code was configured in relationship with User Rights in an earlier release configuration, this authorization code will be lost during upgrade. The administrator must re-configure the authorization code, after upgrade. The authorization code must be associated with a user.

Authorization codes are enabled by default.

Each authorization code is associated with a particular user. The user can then dial numbers which are set to trigger forced authorization code entry. Once a code is entered, the short code settings of the user with which the code is associated are used to completed the call.

This can be used to allow authorized users to make otherwise restricted calls from any extension without first having to log in to that extension and then log out after the call. Valid/invalid authorization code entry can be recorded in the SMDR output.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

Field	Description
Authorization Code	Range = Up to 12 digits. The digits used for the authorization code. Each code must be unique. Wildcards are not usable with authorization codes.
User	This field is used to select a user with which the authorization code is associated. The authorization code can then be used to authorize calls made by that user.

Related links

Authorization Code on page 424

RAS

Navigation: **System Settings** > **RAS**

The **RAS** main content pane lists provisioned remote access servers (RAS). The contents of the list depends on the filter options selected. Click the icons beside a record to edit or delete.

Click **Add/Edit RAS**to open the **RAS** page where you can provision a **RAS**. When you click **Add/Edit RAS**, you are prompted to specify the server where the **RAS** will be added.

Related links

System Settings on page 194
Add RAS on page 425

Add RAS

Navigation: **System Settings** > **RAS**

RAS

A Remote Access Server (RAS) is a piece of computer hardware which sits on a corporate LAN and into which employees dial on the public switched telephone network to get access to their email and to software and data on the corporate LAN.

This form is used to create a RAS service that the system offers Dial In users. A RAS service is needed when configuring modem dial in access, digital (ISDN) dial in access and a WAN link. Some systems may only require one RAS service since the incoming call type can be automatically sensed.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

Field	Description
Name	A textual name for this service. If **Encrypted Password** below is used, this name must match the **Account Name** entered in the Service form.
Extension	Enter an extension number if this service is to be accessed internally.
COM Port	For future use.
TA Enable	Default = Off Select to enable or disable - if enabled RAS will pass the call onto a TA port for external handling.
Encrypted Password	Default = Off This option is used to define whether Dial In users are asked to use PAP or CHAP during their initial log in to the RAS Service. If the Encrypted Password box is checked then Dial In users are sent a CHAP challenge, if the box is unchecked PAP is used as the Dial In Authorization method.

PPP

PPP (Point-to-Point Protocol) is a Protocol for communication between two computers using a Serial interface, typically a personal computer connected by phone line to a server.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

Field	Description
CHAP Challenge Interval (secs)	Default = 0 (disabled). Range = 0 to 99999 seconds. The period between successive CHAP challenges. Blank or 0 disables repeated challenges. Some software, for example Windows 95 DUN, does not support repeated CHAP challenges.
Header Compression	Default = Off Enables the negotiation and use of IP Header Compression as per RFC2507, RFC2508 and RFC2509.
PPP Compression Mode	Default = MPPC This option is used to negotiate compression (or not) using CCP. If set to MPPC or StacLZS the system will try to negotiate this mode with the remote Control Unit. If set to Disable CCP is not negotiated. The options are: • **Disable** Do not use or attempt to use compression. • **StacLZS** Attempt to use and negotiate STAC compression (the standard, Mode 3) • **MPPC** Attempt to use and negotiate MPPC (Microsoft) compression. Useful for dialing into NT Servers.

Table continues…

Field	Description
PPP Callback Mode	Default = Disable The options are: • **Disable**: Callback is not enabled • **LCP**: (Link Control Protocol) After authentication the incoming call is dropped and an outgoing call to the number configured in the Service will be made to reestablish the link. • **Callback CP**: (Microsoft's Callback Control Protocol) After acceptance from both ends the incoming call is dropped and an outgoing call to the number configured in the Service is made to reestablish the link. • **Extended CBCP**: (Extended Callback Control Protocol) Similar to Callback CP however the Microsoft application at the remote end will prompt for a telephone number. An outgoing call will then be made to that number to reestablish the link.
Data Pkt. Size	Default = 0. Range = 0 to 2048. This is the number of data bytes contained in a Data Packet.
BACP	Default = Off Allows negotiation of the BACP/BCP protocols. These are used to control the addition of additional B channels to simultaneously improve data throughput.
Multilink	Default = Off When enabled the system attempts to negotiate the use of the Multilink protocol (MPPC) on the link(s) into this Service. Multilink must be enabled if the more than one channel is allowed to be Bundled/Multilinked to this RAS Service.

Related links

RAS on page 425

WAN Port

Navigation: **System Settings** > **WAN Port**

The **WAN Port** main content pane lists provisioned WAN ports. The contents of the list depends on the filter options selected. Click the icons beside a record to edit or delete.

Click **Add/Edit WAN Port** to open the Add WAN Port page where you can provision a firewall. When you click **Add/Edit WAN Port**, you are prompted to specify the server where the WAN port will be configured.

Related links

System Settings on page 194
Add WAN Port — Sync PPP on page 428
Add WAN Port — Sync Frame Relay on page 428

Add WAN Port — Sync PPP

Navigation: **System Settings** > **WAN Port** > **Add/Edit WAN Port** > **Sync PPP**

Use these settings to configure a WAN port.

On IP500 V2 systems, these settings configure the leased line connected to the WAN port on the Control Unit. Normally this connection is automatically detected by the control unit. If a WAN Port is not displayed, connect the WAN cable, reboot the Control Unit and receive the configuration. The WAN Port configuration form is now be added.

These settings are not mergeable. Changes to these settings will require a reboot of the system.

Field	Description
Name	The physical ID of the Extension port,. This parameter is not configurable; it is allocated by the system.
Speed	The operational speed of this port. For example for a 128K connection, enter 128000. This should be set to the actual speed of the leased line as this value is used in the calculation of bandwidth utilization. If set incorrectly, additional calls may be made to increase Bandwidth erroneously.
Mode	Default = SyncPPP Select the protocol required. The options are: • **SyncPPP** For a data link. • **SyncFrameRelay** For a link supporting Frame Relay.
RAS Name	If the **Mode** is **SyncPPP**, selects the RAS service to associate with the port. If the **Mode** is **SyncFrameRelay**, the RAS Name is set through the DLCIs tab.

Related links

WAN Port on page 427

Add WAN Port — Sync Frame Relay

Navigation: **System Settings** > **WAN Port** > **Add/Edit WAN Port** > **Sync Frame Relay**

These settings are for Frame Relay configuration.

These settings are not mergeable. Changes to these settings will require a reboot of the system.

Field	Description
Frame Management Type	This must match the management type expected by the network provider. Selecting **AutoLearn** allows the system to automatically determine the management type based on the first few management frames received. If a fixed option is required the following options are supported: • **Q933 AnnexA 0393** • **Ansi AnnexD** • **FRFLMI** • **None**
Frame Learn Mode	This parameter allows the DLCIs that exist on the given WAN port to be provisioned in a number of different ways. • **None** No automatic learning of DLCIs. DLCIs must be entered and configured manually. • **Mgmt** Use LMI to learn what DLCIs are available on this WAN. • **Network** Listen for DLCIs arriving at the network. This presumes that a network provider will only send DLCIs that are configured for this particular WAN port. • **NetworkMgmt** Do both management and network listening to perform DLCI learning and creation.
Max Frame Length	Maximum frame size that is allowed to traverse the frame relay network.
Fragmentation Method	The options are: • **RFC1490** • **RFC1490+FRF12**

DLCIs

DLCIs are created for Frame Relay connections. These settings are not mergeable. Changes to these settings will require a reboot of the system.

Field	Description
Frame Link Type	Default = PPP Data transfer encapsulation method. Set to the same value at both ends of the PVC (Permanent Virtual Channel). The options are: • **None** • **PPP** Using PPP offers features such as out of sequence traffic reception, compression and link level connection management. • **RFC 1490** RFC 1490 encapsulation offers performance and ease of configuration and more inter-working with third party CPE. • **RFC1490 + FRF12** Alternate encapsulation to PPP for VoIP over Frame Relay. When selected all parameters on the Service | PPP tab being used are overridden.

Table continues…

Field	Description
DLCI	Default = 100 This is the Data Link Connection Identifier, a unique number assigned to a PVC end point that has local significance only. Identifies a particular PVC endpoint within a user's physical access channel in a frame relay.
RAS Name	Select the RAS Service you wish to use.
Tc	Default = 10 This is the Time Constant in milliseconds. This is used for measurement of data traffic rates. The Tc used by the system can be shorter than that used by the network provider.
CIR	(Committed Information Rate) Default = 64000 bps This is the Committed Information Rate setting. It is the maximum data rate that the WAN network provider has agreed to transfer. The committed burst size (Bc) can be calculated from the set Tc and CIR as Bc = CIR x Tc. For links carrying VoIP traffic, the Bc should be sufficient to carry a full VoIP packet including all its required headers. See the example below.
EIR	(Excess Information Rate) Default = 0 bps This is the maximum amount of data in excess of the CIR that a frame relay network may attempt to transfer during the given time interval. This traffic is normally marked as De (discard eligible). Delivery of De packets depends on the network provider and is not guaranteed and therefore they are not suitable for UDP and VoIP traffic. The excess burst size (Be) can be calculated as Be = EIR x Tc.

Advanced

These settings are used for Frame Relay connections.

These settings are not mergeable. Changes to these settings will require a reboot of the system.

Field	Description
Address Length	The address length used by the frame relay network. The network provider will indicate if lengths other than two bytes are to be used.
N391	Full Status Polling Counter Polling cycles count used by the CPE and the network provider equipment when bidirectional procedures are in operation. This is a count of the number of link integrity verification polls (T391) that are performed (that is Status Inquiry messages) prior to a Full Status Inquiry message being issued.
N392	Error Threshold Counter Error counter used by both the CPE and network provider equipment. This value is incremented for every LMI error that occurs on the given WAN interface. The DLCIs attached to the given WAN interface are disabled if the number of LMI errors exceeds this value when N393 events have occurred. If the given WAN interface is in an error condition then that error condition is cleared when N392 consecutive clear events occur.
N393	Monitored Events Counter Events counter measure used by both the CPE and network provider equipment. This counter is used to count the total number of management events that have occurred in order to measure error thresholds and clearing thresholds.

Table continues…

Field	Description
T391	Link Integrity Verification Polling Timer The link integrity verification polling timer normally applies to the user equipment and to the network equipment when bidirectional procedures are in operation. It is the time between transmissions of Status Inquiry messages.
T392	Polling Verification Timer The polling verification timer only applies to the user equipment when bidirectional procedures are in operation. It is the timeout value within which to receive a Status Inquiry message from the network in response to transmitting a Status message. If the timeout lapses an error is recorded (N392 incremented).

Related links

WAN Port on page 427

User Rights

Navigation: **System Settings** > **User Rights**

Additional configuration information

This section provides the **User Rights** field descriptions.

For additional configuration information, see Configuring User Rights on page 575.

Main content pane

The **User Rights** main content pane lists provisioned user rights. The contents of the list depends on the filter options selected. Click the icons beside a record to edit or delete.

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

Click **Add/Edit User Right** to open the Add User Rights window where you can provision a user right. When you click **Add/Edit User Right**, you are prompted to specify if the user right will be a common object or specific to a server.

Related links

System Settings on page 194
Add User Right on page 432
User on page 432
Short Codes on page 432
Button Programming on page 433
Telephony on page 434
User Rights Membership on page 438
Voicemail on page 438
Forwarding on page 440

Add User Right

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right**

Related links

User Rights on page 431

User

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **User**

Used to set and lock various user settings.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Description
Name	The name for the user rights . This must be set in order to allow the user rights to be selected within the User Rights drop down list on the User | User tab of individual users.
Application Servers Group	Default = Off. Set to On if the IP Office system is deployed in an IP Office Contact Center solution or an Avaya Contact Center Select solution. Only one user rights record can be configured to be the Application Servers Group. If it is set on any one group then the control is disabled on all other groups.
Locale	Default = Blank Sets and locks the language used for voicemail prompts to the user, assuming the language is available on the voicemail server. On a digital extension it also controls the display language used for messages from the system to the phone. See *Avaya IP Office™ Platform Locale Settings*.
Priority	Default = 5, Range 1 (Lowest) to 5 (Highest) Sets and locks the user's priority setting for least cost routing.
Do Not Disturb	Default = Off Sets and locks the user's DND status setting.

Related links

User Rights on page 431

Short Codes

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Short Codes**

Used to set and lock the user's short code set. The tab operates in the same way as the **User | Short Codes** tab. User and User Rights short codes are only applied to numbers dialed by that user. For example they are not applied to calls forwarded via the user.

Warning:

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

These settings are mergeable. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

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

Related links

User Rights on page 431

Button Programming

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Button Programming**

This tab is used to set and lock the user's programmable button set. When locked, the user cannot use **Admin** or **Admin1** buttons on their phone to override any button set by their user rights.

Buttons not set through the user rights can be set through the user's own settings. When **Apply user rights value** is selected, the tab operates in the same manner as the **User | Button Programming** tab.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Adding Blank Buttons

There are scenarios where users are able to program their own buttons but you may want to force certain buttons to be blank. This can be done through the user's associated **User Rights** as follows:

1. Assign the action **Emulation | Inspect** to the button. This action has no specific function. Enter some spaces as the button label.
2. When pressed by the user, this button will not perform any action. However it cannot be overridden by the user.

Related links

User Rights on page 431

Telephony

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Telephony**

Allows various user telephony settings to be set and locked. These match settings found on the **Call Management** > **Users** > **Add/Edit Users** > **Telephony** tab.

Related links

User Rights on page 431
Call Settings on page 434
Supervisor Settings on page 435
Multi-line Options on page 436
Call Log on page 437

Call Settings

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Telephony** > **Call Settings**

Additional configuration information

For additional information on ring tones, see Ring Tones on page 535.

Configuration settings

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

Field	Description
No Answer Time	Default = Blank (Use system setting). Range = 6 to 99999 seconds. Sets how long a call rings the user before following forwarded on no answer if set or going to voicemail. Leave blank to use the system default setting.
Transfer return Time (secs)	Default = Blank (Off), Range 1 to 99999 seconds. Sets the delay after which any call transferred by the user, which remains unanswered, should return to the user if possible.
Wrap up Time (secs)	Default = 2 seconds, Range 0 to 99999 seconds. Specifies the amount of time after ending one call before another call can ring. You may wish to increase this in a "call center" environment where users may need time to log call details before taking the next call. It is recommended that this option is not set to less than the default of 2 seconds. 0 is used for immediate ringing.

Table continues…

Field	Description
Call waiting on/ Enable call waiting	Default = Off For users on phones without appearance buttons, if the user is on a call and a second call arrives for them, an audio tone can be given in the speech path to indicate a waiting call (the call waiting tone varies according to locale). The waiting caller hears ringing rather than receiving busy. There can only be one waiting call, any further calls receive normal busy treatment. If the call waiting is not answered within the no answer time, it follows forward on no answer or goes to voicemail as appropriate. User call waiting is not used for users on phones with multiple call appearance buttons.
Busy on held/ Enable busy on Held	Default = Off If on, when the user has a call on hold, new calls receive busy tone (ringing for incoming analog call) or are diverted to voicemail if enabled, rather than ringing the user. Note this overrides call waiting when the user has a call on hold. Not supported (should be set to off) for users with call appearance buttons.

Related links

Telephony on page 434

Supervisor Settings

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Telephony** > **Supervisor Settings**

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

These settings are mergeable. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Description
Can Intrude	Default = Off Check this option if the User can interrupt other user's calls. This setting and the setting below are used to control the use of the following short code and button features: • Call Intrude • Call Listen • Call Steal • Dial Inclusion
Cannot be Intruded	Default = On If checked, this user's calls cannot be interrupted or acquired. In addition to the features listed above, this setting also affects whether other users can use their appearance buttons to bridge into a call to which this user has been the longest present user.

Table continues…

Field	Description
Deny Auto Intercom Calls	Default = Off. When enabled, any automatic intercom calls to the user's extension are automatically turned into normal calls.
Force Login	Default = Off If checked, the user must log in using their Login Code to use an extension. For example, if Force Login is ticked for User A and user B has logged into A's phone, after B logs off A must log back. If Force Login was not ticked, A would be automatically logged back in.
Force Account Code	Default = Off If checked, the user must enter a valid account code to make an external call.
Inhibit Off-Switch Forward/Transfer	: Default = Off When enabled, this setting stops the user from transferring or forwarding calls externally. Note that all user can be barred from forwarding or transferring calls externally by the **System | Telephony | Telephony | Inhibit Off-Switch Forward/Transfers** setting.
Outgoing Call Bar	Default = Off When set, bars the user from making external calls.
Coverage Group	Default = <None> If a group is selected, the system will not use voicemail to answer the users unanswered calls. Instead the call will continue ringing until either answered or the caller disconnects. For external calls, after the users no answer time, the call is also presented to the users who are members of the selected Coverage Group. For further details refer to Coverage Groups.

Related links

Telephony on page 434

Multi-line Options

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Telephony** > **Multi-line Options**

Additional configuration information

For additional configuration information, see Appearance Button Operation on page 943.

Configuration settings

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

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

Field	Description
Individual Coverage Time (secs)	Default = 10 seconds, Range 1 to 99999 seconds. This function sets how long the phone will ring at your extension before also alerting at any call coverage users. This time setting should not be equal to or greater than the No Answer Time.

Related links

Telephony on page 434

Call Log

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Telephony** > **Call Log**

The system can store a centralized call log for users. Each users' centralized call log can contain up to 30 call records for user calls. When this limit is reached, each new call records replaces the oldest previous record.

On Avaya phones with a fixed **Call Log** or **History** button (1400, 1600, 9500 and 9600 Series), that button can be used to display the user's centralized call log. The centralized call log is also used for M-Series and T-Series phone. The user can use the call log to make calls or to store as a personal speed dial. They can also edit the call log to remove records. The same call log is also used if the user logs into one-X Portal for IP Office.

The centralized call log moves with the user if they log on and off from different phones. This includes if they hot desk within a network.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

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

Related links

Telephony on page 434

User Rights Membership

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **User Rights Membership**

The tabs display the users associated with the user rights and allows these to be changed.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Description
Members of this User Rights	This tab indicates those users associated with the user rights. If the user has an associated Working hours time profile, their association to the user rights applies only during the periods defined by the time profile. If the user does not have an associated Working hours time profile, they are associated with the user rights at all times.
Members when out of service	This tab indicates those users associated with the user rights outside the time periods defined by their Working hours time profile. The Members when out of service tab is not populated unless there are time profiles available within the configuration.

Related links

User Rights on page 431

Voicemail

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Voicemail**

Display the users associated with the user rights and allows these to be changed.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Description
Voicemail On	Default = On When on, the mailbox is used by the system to answer the user's unanswered calls or calls when the user's extension returns busy. Note that selecting off does not disable use of the user's mailbox. Messages can still be forward to their mailbox and recordings can be placed in it. The mailbox can also still be accessed to collect messages.

Table continues…

Field	Description
Voicemail Ringback	Default = Off When enabled and a new message has been received, the voicemail server calls the user's extension to attempt to deliver the message each time the telephone is put down. Voicemail will not ring the extension more than once every 30 seconds.
DTMF Breakout When a caller is directed to voicemail to leave a message, they can be given the option to be transferred to a different extension. The greeting message needs to be recorded telling the caller the options available. The extension numbers that they can be transferred to are entered in the fields below. These system default values can be set for these numbers and are used unless a different number is set within these user settings. The Park & Page feature is supported when the system voicemail type is configured as **Embedded Voicemail** or **Voicemail Pro**. Park & Page is also supported on systems where Avaya Aura Messaging, Modular Messaging over SIP, or CallPilot (for Enterprise Branch with CS 1000 deployments) is configured as the central voice mail system and the local Embedded Voicemail or Voicemail Pro provides auto attendant operation. The Park & Page feature allows a call to be parked while a page is made to a hunt group or extension. This feature can be configured for Breakout DTMF 0, Breakout DTMF 2, or Breakout DTMF 3.	
Reception/ Breakout (DTMF 0)	The number to which a caller is transferred if they press `0`while listening to the mailbox greeting rather than leaving a message (***0** on Embedded Voicemail in IP Office mode). For voicemail systems set to Intuity emulation mode, the mailbox owner can also access this option when collecting their messages by dialing ***0**. If the mailbox has been reached through a Voicemail Pro call flow containing a **Leave Mail** action, the option provided when **0** is pressed are: • For IP Office mode, the call follows the **Leave Mail** action's **Failure** or **Success** results connections depending on whether the caller pressed **0** before or after the record tone. • For Intuity mode, pressing **0** always follows the **Reception/Breakout (DTMF 0)** setting. When Park & Page is selected for a DTFM breakout, the following drop-down boxes appear: • **Paging Number –** displays a list of hunt groups and users (extensions). Select a hunt group or extension to configure this option. • **Retries –** the range is 0 to 5. The default setting is 0. • **Retry Timeout –** provided in the format M:SS (minute:seconds). The range can be set in 15-second increments. The minimum setting is 15 seconds and the maximum setting is 5 minutes. The default setting is 15 seconds
Breakout (DTMF 2)	The number to which a caller is transferred if they press `2`while listening to the mailbox greeting rather than leaving a message (***2** on Embedded Voicemail in IP Office mode)
Breakout (DTMF 3)	The number to which a caller is transferred if they press `3`while listening to the mailbox greeting rather than leaving a message (***3** on Embedded Voicemail in IP Office mode).

Related links

User Rights on page 431

Forwarding

Navigation: **System Settings** > **User Rights** > **Add/Edit User Right** > **Forwarding**

Additional configuration information

For additional configuration information, see the section “DND, Follow Me, and Forwarding” in the chapter **Configure user settings** in *Administering Avaya IP Office™ Platform with Web Manager*.

For additional configuration information, see DND, Follow Me, and Forwarding on page 598.

Configuration settings

Display the users associated with the user rights and allows these to be changed.

These settings are mergeable.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Field	Description
Block Forwarding	
Enable Block Forwarding	Default = Off. When enabled, call forwarding is blocked. The following actions are blocked: • Follow me • Forward unconditional • Forward on busy • Forward on no answer • Call Coverage • Hot Desking The following actions are not blocked: • Do not disturb • Voicemail • Twinning

Related links

User Rights on page 431

Chapter 7: Security Manager

Navigation: **Security Manager**

Related links

Service Users on page 441
Certificates on page 443

Service Users

Navigation: **Security Manager** > **Service Users**

Selecting **Service Users** from the **Security Manager** window menu bar opens the Service Users page. The main content pain lists the configured service users.

Related links

Security Manager on page 441
Synchronize Service User and System Password on page 441
Add Service User on page 442
User Preferences on page 443

Synchronize Service User and System Password

Navigation: **Security Manager** > **Service Users** > **Synchronize Service User and System Password**

Each IP Office system has a security database to authenticate users. Synchronizing the databases enables single sign on for all systems and applications across the solution. To enable single sign on, you must configure a service user with security web service rights and with the same credentials (user ID and password) on each system in the Server Edition solution. You then use this common user to manage all other service users. Note that performing a security settings reset from Manager or Web Manager will disable single sign on since there is no longer a common user with common credentials. In this case, log in to the system where the security settings were reset using the URL `https://<IP_address>:8443/WebMgmtEE/webmanagement.html`. Reset the password of the common user to the common value.

Related links

Service Users on page 441

Add Service User

Navigation: **Security Manager** > **Service Users** > **Add/Edit Service User**

Click **Add/Edit Service User** to open the Add Service User window.

Field	Description
Name	Range = Up to 31 characters. Sets the service user's name. The minimum name length is controlled through **General settings**. **Note:** If changing the user name and/or password of the current service user used to load the security settings, after saving the changes Manager should be closed. Not closing Manager will cause error warnings when attempting to send any further changes.
Password	Range = Up to 31 characters. Sets the service user's password. To change the current password click **Change**. Enter and confirm the new password. Note that an error will be indicated if the password being entered does not meet the password rules set through General settings. To clear the cache of previous password details used by the password rules setting, click **Clear Cache**. For example, if the rule restricting the reuse of old passwords has been enabled, clearing the cache allows a previous password to be used again.
Set New Password	Click the button to change your existing password. The button to set a new password appears only for a logged in Service User when the Service User tries to change it's own password. If the button is clicked, the IP Office system asks the Service User to type in the following details: • **Password**: New password for the logged in Service User. • **Confirm Password**: New password for the logged in Service User. • **Old Password**: The old password is used to re-authenticate the Service User for changing the password.
Account Expiry	Default = <None> (No Expiry). Not applicable to Web Manager. This option can be used to set a calendar date after which the account will become locked. The actual expiry time is 23:59:59 on the selected day. To prompt the user a number of days before the expiry date, set an **Expiry Reminder Time** on the security General Settings tab.
Rights Group Membership	The check boxes are used to set the **Rights Groups** to which the user belongs. The user's rights will be a combination of the rights assigned to the groups to which they belong.

Related links

Service Users on page 441

User Preferences

Navigation: **Security Manager** > **Service Users** > **User Preferences**

Selecting **User Preferences** for a user in the **Service Users** table, opens the Service User Preferences window which displays the user name and password for the service user.

Note that selecting **Preferences** from the menu bar opens the Preferences window for the Administrator user ID.

Related links

Service Users on page 441

Certificates

Navigation: **Security Manager** > **Certificates**

Additional Configuration Information

For additional information on certificates, see Certificate Management on page 500.

Services between the system and applications may, depending on the settings of the service being used for the connection, require the exchange of security certificates. The system can either generate its own certificate or certificates provided from a trusted source can be loaded.

Warning:

The process of 'on-boarding' (see *Deploying Avaya IP Office™ Platform SSL VPN Services*) automatically adds a certificate for the SSL VPN to the system's security settings when the on-boarding file is uploaded to the system. Care should be taken not to delete such certificates except when advised by Avaya.

Configuration Settings

Field	Description
Identity Certificate:	
The **Identity Certificate** is an X.509v3 certificate that identifies the system to a connecting another device using TLS, for example a PC running IP Office Manager set to Secure Communications. By default, the system provides its own self-generated certificate, automatically generated when the system is first installed. Alternatively, a certificate from another source can be uploaded to the system if required. The system's certificate is advertised (used) by Services which have their **Service Security Level** set to a value other than **Unsecure Only**.	

Table continues…

Field	Description
Offer Certificate	Default = On. This is a fixed value for indication purposes only. This sets whether the system will offer a certificate in the TLS exchange when the IP Office is acting as a TLS server, which occurs when accessing a secured service.
Offer ID Certificate Chain	Default = Off. When set to On, this setting instructs IP Office to advertise a chain of certificates in the TLS session establishment. The chain of certificates is built starting with the identity certificate and adding to the chain all certificates it can find in the IP Office Trusted Certificate Store based on the Common Name found in the "Issued By" Subject Distinguished Name field in each of the certificates in the chain. If the Root CA certificate is found in the IP Office Trusted Certificate Store, it will be included in the chain of certificates. A maximum of six certificates are supported in the advertised chain of certificates.
Issued to	Default = IP Office identity certificate. Common name of issuer in the certificate.

Table continues…

Field	Description
Set	This option can is used to load a certificate and associated private key. The certificate and key must be a matching pair. IP Office supports certificates with RSA key sizes of 1024, 2048 and 4096 bits. The use of RSA key size 4096 may impact system performance. The recommended key size is 2048. IP Office supports signature algorithms of SHA-1, SHA-256, SHA-384, and SHA-512. Using signature size larger than SHA-256 may impact system performance. The recommended signature algorithm is SHA-256. The source may be: • Current User Certificate Store. • Local Machine Certificate Store. • File in the PKCS#12 (.pfx) format • Pasted from clipboard in PEM format, including header and footer text. This method must be used for PEM (.cer) and password protected PEM (.cer) files. The identity certificate requires both the certificate and private key. The .cer format does not contain the private key. For these file types select **Paste from clipboard** and then copy the certificate text and private key text into the Certificate Text Capture window. **Using a file as the certificate source:** In Manager, when using the file option, the imported "p12" "pfx" or "cer" file for setting the identity certificate can only contain the private key and identity certificate data. It cannot contain additional Intermediate CA certificates or the Root CA certificate. The Intermediate CA certificates or the Root CA certificate must be imported separately in the IP Office Trusted Certificate Store. This does not apply to Web Manager. **Note:** Web Manager does not accept the file of type "cer" with extension ".cer". This file type can only be used in Manager.
View	This command displays details of the current identity certificate. The certificate source, details and valid dates are displayed. The certificate view menu can also be used to install the certificate (but not its private key) into the viewing PC's local certificate store for use by the PC for secure connection to the system or to export the certificate from the PC.
Export	This command is used to export the certificate from the PC.

Table continues…

Field	Description
Regenerate	This command deletes the current identity certificate and generates a new self-signed certificate. **Important:** Regenerating the certificate can take up to a minute during which system performance may be impacted. Therefore it is recommended to only perform this action during a maintenance window. The regeneration takes places after saving the changes to security settings. Clicking **Regenerate** opens the Regenerate Certificate window where you are prompted to enter the following information: • **Signature**: Default = SHA256/RSA2048. This setting configures both the signature algorithm and the RSA key length to use when generating the IP Office identity certificate. The options are: - SHA256/RSA2048 - SHA1/RSA1024 If any other combinations are needed, the Security Administrator will need to construct the IP Office identity certificate outside of Manager and use the **Set** action to install it. • **Default Subject Name**: Default = None Specifies a common name for the subject of this certificate. The subject is the end-entity or system that owns the certificate (public key). Example: `ipoffice-0123456789AB.avaya.com`. If the field is blank, a system generated subject name is used. • **Subject Alternative Name(s)**: Default = None The Subject Alternative Name (SAN) field allows a list of alternate names to be bound to the subject of the certificate. The input field will allow the user to enter multiple Subject Alternate Names, each separated by the comma “,” character. Each SAN consists of a PREFIX, followed by the colon “:” character, followed by VALUE. The list of allowed PREFIX strings are “DNS”, “URI”, “IP”, “SRV”, and “email”. The VALUE can be any text character except the comma. (The comma is reserved as a field separator.) The input field has a maximum size limit of 511 characters. Example: `”DNS: ipoffice-0123456789AB.avaya.com, IP: 192.168.137.29, URI:http://avaya_example_url.com/, email:jack@my_email_server.com”` Supported Subject Alternative Name types include: a DNS Name, a Uniform Resource Identifier, an IP Address, an SRV record, or an electronic mail address.

Table continues…

Field	Description
	Although a PREFIX must be specified to select the type of name, no validation is performed on the value. If this field is blank, a system generated subject alternative name field value is used.
Certificate Expiry Warning Days	Default = 60, Range = 30 to 180 IP Office Manager can display a warning when a system's security certificate is due to expire. This setting is used to set the trigger for certificate warnings.

Trusted Certificate Store This section displays a list of the certificates held in the system's trusted certificate store.	
Installed Certificates	Default = A set of fixed Avaya provided Intermediate CA or Root CA certificates. The certificate store contains a set of trusted certificates used to evaluate received client certificates. Up to 25 X.509v3 certificates may be installed.
Add	Add a trusted certificate. The source may be: • Current User Certificate Store. • Local Machine Certificate Store. • File in one of the following formats: - PEM (.cer) - password protected PEM (.cer) - DER (.cer) - password protected DER (.cer) • Pasted from clipboard in PEM format, including header and footer text. This method must be used for PKCS#12 (.pfx) files. The PKCS#12 (.pfx) format contains a private key and a trusted certificate cannot contain a private key. For this file type, select **Paste from clipboard** and then copy the certificate text into the Certificate Text Capture window. IP Office supports certificates with RSA key sizes of 1024, 2048 and 4096 bits. The use of RSA key size 4096 may impact system performance. The recommended key size is 2048. IP Office supports signature algorithms of SHA-1, SHA-256, SHA-384, and SHA-512. Using signature size larger than SHA-256 may impact system performance. The recommended signature algorithm is SHA-256.
View	View the currently selected certificate. The certificate (not the private key) may also be installed into the local PC certificate store for export or later use when running the manager in secured mode.
Delete	Delete the currently selected certificate.

Related links

Security Manager on page 441

Chapter 8: Applications

Navigation: **Applications**

Related links

Synchronizing Server Edition passwords in Web Manager on page 448
Launch Manager on page 449
Voicemail Pro — System Preferences on page 450
Voicemail Pro — Call Flow Management on page 461
one-X Portal on page 462
WebRTC Configuration on page 462
File Manager on page 466
Media Manager on page 467
Web License Manager on page 474

Synchronizing Server Edition passwords in Web Manager

In order to open IP Office Manager for a Server Edition solution, all IP Office systems in the solution must have a service user with common credentials. If the security settings on any system are reset, service user passwords are reset to the default value. In this case, when a system does not have a service user with common credentials, launch of IP Office Manager fails.

Before you begin

You must know the user ID and password of the service user that is common to all systems in the solution.

Procedure

1. For the system where the security settings were reset, open Web Manager using the address `https://<ip_address>:7070/WebManagement/WebManagement.html`.
2. Log on as **Administrator**.
3. In Web Manager, select **Security Manager** > **Service Users**.
4. Create the common service user.
5. Log out of this Web Manager session.

6. Start another Web Manager session on the system using the address `https://<ip_address>/index.html`.
7. Log on as the common service user.
8. In Web Manager, select **Security Manager** > **Service Users**.
9. Click **Synchronize Service User and System Password**.
10. Select **Applications** > **IP Office Manager**.

Related links

Applications on page 448

Launch Manager

Navigation: **Applications** > **IP Office Manager**

Note:

This option is not available on IP500 V2 systems.

Use the **Manager** application to configure IP Office settings that are not configurable in Web Manager. Selecting **IP Office Manager** from the **Applications** menu launches a locally installed instance of the **Manager** application. **Manager** automatically loads the IP Office configuration file from the Primary Server. To load an alternate IP Office configuration file, select a server from the list before selecting **IP Office Manager**.

When the **Manager** application launches, you are automatically logged into **Manager** with the Primary Server configuration loaded. If the Primary server is not available, you are logged into **Manager** with the Secondary Server configuration loaded.

Requirements

- Java version 1.6 or higher is required. If Java is not installed, or an older version is installed, an error message will open and provide a link to the Java download web site.
- If the current version of Manager is not installed, you are prompted to download the current version. To perform the download, Web Control must be online.

Manager software version

The **IP Office Manager** action launches a locally installed version of the Manager application. The application launch behavior depends on the version of Manager installed.

Manager version is current: If the Manager version is current, Manager launches without a login prompt and loads the configuration file for the server.

Manager version is not current: If the Manager version is not current, you are prompted to download and install the latest version and a link is provided. You can continue to use the currently installed version or download the current version. Upgrading to the current version requires a browser restart.

Manager is not installed: If Manager is not installed, you are prompted to download and install the latest version and a link is provided. Once Manager is installed, a browser restart is required before launching Manager.

Synchronizing Server Edition passwords

In order to open IP Office Manager for a Server Edition solution, all IP Office systems in the solution must have a service user with common credentials.

For more information, see Synchronizing Server Edition Passwords in Web Manager on page 448 Synchronizing Server Edition Passwords in .

Related links

Applications on page 448

Voicemail Pro — System Preferences

Navigation: **Applications** > **Voicemail Pro — System Preferences**

Note:

This option is not available on IP500 V2 systems.

Related links

Applications on page 448
General on page 450
Email on page 452
Gmail Integration on page 455
Housekeeping on page 456
SNMP Alarm on page 457
Outcalling on page 458
Voicemail Recording on page 458
Syslog on page 459
Alarms on page 459
User Group on page 461

General

Navigation: **Applications** > **Voicemail Pro — System Preferences** > **General**

Field	Description
Default Telephony Interface	Default = Intuity. Use this field to select the mailbox operation mode for all mailboxes. The options are: • Intuity • IP Office
Min. Message Length (secs)	Default = 0 seconds (in IP Office mode) and 3 seconds (in Intuity mode). Use this field to set a restriction on the minimum length for a message. The minimum value that you can set is 0 seconds, and the maximum value is 10 seconds. Messages that are of shorter length than the set minimum length are deleted immediately. In IP Office mode, this field is unavailable.
Voicemail Password	Default = Blank. A voicemail password is optional for the Voicemail Pro server. If you set a password here, it must match the **Voicemail Password** configured in the IP Office security settings.
Max. Message Length (secs)	Default = 120 seconds. Use this field to set a restriction on the maximum length for a message. The maximum value that you can set is 3600 seconds (60 minutes). A message with the message length of 1 minute occupies approximately 1MB of disk space.
Max. Call\VRL Record Length (secs)	Default = 3600 seconds. Use this field to set a restriction on the maximum recording length for the calls. The minimum value that you can set is 5 seconds. The maximum value that you can set is 18000 seconds (300 minutes).
Play Advice on Call Recording	Default = On Use this check box to set whether to play an advice warning to the callers when their calls start getting recorded. It is a legal requirement in some countries to inform the callers before recording their calls, and so confirm before you clear this check box.
Failback Option	Default = Graceful Use this field to configure the mode of failback operation in a voicemail system with a backup Voicemail Pro server. Note that this field is unavailable if you are not using a voicemail system with a backup Voicemail Pro server and not logged on to the active Voicemail Pro server using an Administrator account. Failback is only considered if the preferred and back-up voicemail servers have started their synchronization operation (SMTP exchange of messages, etc). • **Manual**The system administrator has to initiate the failback operation. • **Graceful** *(Default)* The backup server initiates the failback operation once all current calls on the backup voicemail server end. • **Automatic** The backup server initiates the failback operation once all current calls on the backup voicemail server end or, if exceeded, after the specified timeout period set (maximum 60 minutes).

Table continues…

Field	Description
System Fax Number	Default = Blank Use this field to set the number of the fax machine to which all incoming faxes are to be directed. If you are using a fax board, the number that you enter must match the extension number that is connected to the fax board of the fax server computer.
Use as a Prefix	If your fax system does not use prefix addressing, leave this box unchecked. For this feature to work, you also need to set up a short code.
Enable Fax Sub-Addressing	Most fax servers perform fax forwarding based on DTMF signaling received with the fax call. Select the Enable Fax Sub-Addressing check box so that the DTMF signal is passed to the fax server after the call has been answered so that the fax can be forwarded to the e-mail address of the intended recipient.
Enable Voicemail Pro Client Interface	Default = Yes. Used to manage communication between the Voicemail Pro server and the client. When set to No, Voicemail Pro clients cannot connect to this Voicemail Pro server. When set to Yes, communication between the server and clients is allowed.

Related links

Voicemail Pro — System Preferences on page 450

Email

Navigation: **Applications** > **Voicemail Pro — System Preferences** > **Email**

Note:

If you are using Voicemail Pro in a distributed environment, a distributed server delivers a recorded message to the central Voicemail Pro server on completion of the recording. However, the presentation to the Voicemail Pro server for message waiting indication (MWI) and access via telephone might be delayed because of the internal processing of the message and the network latency. The delay might be up to 2 minutes in high traffic situations.

Field	Description
Enable MAPI/EWS	Default = MAPI <Description> The options are: • MAPI • EWS • None
MAPI Service	
Address	Default = Blank.
Port	Default = 50792

Table continues…

Field	Description
SMTP Sender These settings are used to configure the SMTP server and the server account that Voicemail Pro server uses for sending e-mails through SMTP. Multiple servers can be configured. The first entry specifies the default SMTP server used for sending e-mails if there is no other entry matching the domain specified in the e-mail destination address. Additional servers can be added when different settings are required for sending e-mails to specific domains. For example, the default can be configured for the customer's internal network exchange server with additional entries added for e-mails to external e-mail domain addresses such as yahoo.com. VPNM, distributed Voicemail Pro servers, and primary/backup Voicemail Pro servers all use SMTP to exchange information and messages between Voicemail Pro servers. When that is the case, the first entry in the SMTP Sender list must be the one used and needs to be configured for that service with the domain and server setting both matching the IP address or fully-qualified domain of the Voicemail Pro server.	
Logging	Default = No. Set to Yes to enable SMTP logging. For information on SMTP logging see *Avaya IP Office Platform Voicemail Pro Administration*.
Add SMTP Sender	Click to open the SMTP Sender Configuration window.
Test Connection	Click to validate the SMTP configuration. When clicked, Voicemail Pro serves the SMTP server test connectivity request based on the input provided in the SMTP Sender Configuration window and provides a success or failure response. You must fill up all the four fields to test the connection. However, Voicemail Pro uses the values provided in the **Mail Server** and **Port** fields to validate the connection.

Table continues…

Field	Description
Mail Domain	Default = Blank. This field is used differently depending on whether it is the first entry in the list or not. **First server entry in the list:** This is the default outgoing e-mail setting. It also sets the mail destination domain on which the Voicemail Pro server filters incoming messages (see below) and so is repeated in the SMTP Receiver settings. For messaging between Voicemail Pro servers, the first entry in the SMTP Sender list must be the one configured and used. Each server uses the SMTP server service on the same server computer as the voicemail service. For example a Windows-based server uses the SMTP e-mail provided by the IIS on the same server. The voicemail service also uses the domain set to filter incoming SMTP mails received by the SMTP server. For this to work, the domain entered should be the fully-qualified name of the server on which the Voicemail Pro server is running, for example vmpro1.example.com. Any incoming messages where the recipient mail domain is not exactly the same as the specified domain are ignored. The recipient can either by vmsyncmaster, vmsyncslave, or the name or extension of a mailbox on the Voicemail Pro server, for example `Extn201@vmprocentral.example.com` or `201@vmprocentral.example.com`. **Subsequent entries:** The domain specifies that these settings should be used for e-mails sent to the matching domain. The entry must be a fully-qualified name resolvable by DNS or an IP address.
Mail Server	Default = Blank. Specifies the IP address or fully-qualified domain name of the SMTP server to which messages are sent. Voicemail Pro supports SMTP communication over both - SSL/TLS and plain text. **First server entry in the list:** Where messaging between Voicemail Pro servers is being used (central, backup and or distributed servers), the first entry is used and will match the domain set above. **Subsequent entries:** It will be the address of the e-mail server that will handle e-mails for recipients other than another Voicemail Pro server on the network.
Port	Default = Blank. The port number on the SMTP server to which the messages are sent. Port number for an external SMTP server can be different depending on whether you want to send the messages in secure mode or non-secure

Table continues…

Field	Description
Sender	Default = Blank. Note that some servers will only accept e-mails from a specific sender or sender domain. If left blank, the Voicemail Pro server will insert a sender using either the e-mail address set for the voicemail mailbox user if set or otherwise using the best matching name it can resolve from the IP Office.
Server Requires Authentication	Default = No. Indicates whether the connection to send SMTP messages to the mail server requires authentication with that server. The authentication will typically be to the name and password of a mailbox account configured on that server. Setting to **Yes** enables the **Account Name** and **Password** fields.
Account Name	Default = Blank. Sets the name to use for authentication.
Password	Default = Blank. Set the password to use for authentication.
SMTP Receiver These settings are used to set where the Voicemail Pro server checks for incoming SMTP messages.	
SMTP Receiver	Default = Internal. The options are: • **Internal**: Use this option for Voicemail Pro servers running on the IP Office Application Server. The Internal setting can also be used when the Voicemail Pro server should check the appropriate account on an SMTP server for waiting messages. The server settings will be pre-populated using the **SMTP Sender** settings. • **External**: Use this option when the Voicemail Pro server is on a server where is co-exists with a third-party SMTP application, for example an IIS server with SMTP enabled.
Port	Default = 25 The port on which the Voicemail Pro server listens for incoming messages.
Domain	Default = The domain set by the first server entry in the **SMTP Sender** list. The domain destination address for which the server will accept incoming e-mails.

Related links

Voicemail Pro — System Preferences on page 450

Gmail Integration

Navigation: **Applications** > **Voicemail Pro — System Preferences** > **Gmail Integration**

Additional configuration information

For additional information, see Configuring Gmail Integration on page 581.

Field	Description
Enable Gmail Integration	Default = No. This setting only applies to Server Edition systems. The system setting to enable the use of Gmail for voicemail. When set to Yes, you can configure users for Gmail on **Call Management** > **Users** > **Add/Edit Users** > **Voicemail**.
Upload Google Service account generated keys	You must register the Voicemail Pro application for the Gmail API in the Google Developer's console. You must create a Google service account and generate the JSON and P12 key files. Use the **JSON Key File** and **P12 Key File** buttons to upload the files to Web Manager. Web Manager transfers the files to the Voicemail Pro application.

Related links

Voicemail Pro — System Preferences on page 450

Housekeeping

Navigation: **Applications** > **Voicemail Pro — System Preferences** > **Housekeeping**

Use the Housekeeping settings to:

- Set the duration after which the Voicemail Pro server deletes messages and recordings automatically.
- Set the default playback order of messages. Playback can be set to **Oldest First** or **Newest First**.

Note:

The housekeeping deletion settings do not apply to the messages forwarded to an Exchange server. The messages that are forwarded to an Exchange server are deleted from the Voicemail Pro server in accordance with the **Deleted messages** settings.

Field	Description
New Messages	This status is applied to messages where neither the header nor the message content has been played.
Old Messages	This status is applied to messages where the user has played the message content but has not marked the message as saved.
Saved Messages	This status is applied to messages that have been marked as saved by the user.
Unopened Messages	This status is used for messages where, in Intuity emulation mode, the user has played the message header but has not played the message content.
New Recordings	This status is used for recordings that have not been played.
Old Recordings	This status is used for recordings that have been played.

Table continues…

Field	Description
Deleted Messages	This status is used for messages that have been marked as deleted through mailbox access.

Related links

Voicemail Pro — System Preferences on page 450

SNMP Alarm

Navigation: **Applications** > **Voicemail Pro — System Preferences** > **SNMP Alarm**

IP Office can be configured to generate alarms. These alarms can be sent using SNMP, SMTP e-mail, or Syslog alarm formats. These settings are used to set the levels at which the Voicemail Pro server will indicate to the IP Office to send an alarm.

Field	Description
Alarm Threshold Unit	Default = Recording Time Left (mins). The units, minutes or MB, used to set the alarm. The options are: • Recording Time Left (mins) • Disk Space Left (MB)
Alarm Threshold Level	Default = 60. The level at which SNMP alarms are to be triggered. The minimum value that you can enter is 11. the following additional alarms are set based on the **Alarm Threshold Level**. • **Space OK Alarm**: Triggered when the amount of available space returns to above a level set at **Alarm Threshold Level** plus 30. • **Critical Alarm**: This alarm is set at 30. If the **Alarm Threshold Level** is set at less than 40, the critical alarm is set at **Alarm Threshold Level** minus 10. Note that the critical alarm value decreases if you decrease the **Alarm Threshold Level**, but the critical alarm value does not increase if you increase the **Alarm Threshold Level**. So, the critical alarm value keeps on decreasing and remains set at the least value that it takes. To reset the critical alarm back to 30, click **Default Settings**. • For Voicemail Pro Server Edition, IP Office sends SNMP alarms based on the percentage of the available free space of the total disk space. The SNMP alarms are as follows: - **Disk State Critical**: Free disk space is less than 5% - **Disk State OK**: Free disk space is between 5 to 10% - **Disk State Free**: Free disk space is greater than 10% - **Disk State Stop Recording**: Free disk space is 0.

Table continues…

Field	Description
Default Settings	Return to the default alarm settings. Alarm Threshold Level is reset to 60. The Space OK level is reset to 90. The Critical Alarm level is reset to 30.

Related links

Voicemail Pro — System Preferences on page 450

Outcalling

Navigation: **Applications** > **Voicemail Pro — System Preferences** > **Outcalling**

Field	Description
System Times **Prime Time** is the period that outcalling is to be active as default for the system. **Peak Time** is the busiest working hours.	
From Prime Times	Default = 7:30. Set the beginning of the prime time interval.
To Prime Times	Default = 19:30 Set the end the prime time interval.
From Peak Times	Default = 7:30. Set the beginning of the peak interval.
To Peak Times	Default = 19:30 Set the end the peak interval.
System Retries Settings	
Number of Retries	Default = 5. Range = 0 to 10. If the message is not collected after the last retry, no notification is sent until another new message is delivered in the user's mailbox.
Retry Interval	The interval between each successive try. The interval is the length of time between each attempt to connect to the target number again. The 6th to 10th retries use the default retry interval.

Related links

Voicemail Pro — System Preferences on page 450

Voicemail Recording

Navigation: **Applications** > **Voicemail Pro — System Preferences** > **Voicemail Recording**

Use the Voicemail Recording page to configure an SFTP connection on a Linux-based Voicemail Pro server to transfer call recordings to the Voice Recording Library (VRL) application Avaya IP Office ContactStore .

Before you configure the Voicemail Recording settings, you must have configure an SFTP server running on the computer that runs the ContactStore application. For details on the SFTP server requirements, see *Avaya IP Office Implementing Voicemail Pro* (15-601064).

Field	Description
FTP User Name	The user name used to log in to the FTP server.
FTP Password	The password used to log in to the FTP server.
Remote FTP Location	<IP address>?
Remote FTP Host	The FTP server host name.
Test Connection	Click to test the connection.

Related links

Voicemail Pro — System Preferences on page 450

Syslog

Navigation: **Applications** > **Voicemail Pro — System Preferences** > **Syslog**

You can configure the Voicemail Pro server to write syslogs to a syslog server.

Field	Description
Enable Syslog	Default = No. Click Yes to enable logging.
IP Address	Default = Blank. The IP address of the syslog server.
Port	Default = 514 A UDP port number on which target syslog server is listening for syslog records.

Related links

Voicemail Pro — System Preferences on page 450

Alarms

Navigation: **Applications** > **Voicemail Pro — System Preferences** > **Alarms**

The Voicemail Pro client can display the alarm calls that have been configured for the Voicemail Pro to perform.

The Voicemail Pro is limited to 2 outgoing alarm calls at the same time (subject to voicemail port availability). Any additional alarm calls are delayed until the existing alarm calls have been completed.

Field	Description
Add Alarm Click to configure the following alarm settings.	
Target	
Time	Default = 00:00. Set the alarm time in 24-hour format (hh:mm or hhmm). A time value can be entered or a call variable can be used. If left blank or if the call variable used is not a valid time value, the call flow user will be asked to enter a time the same as if **Ask Caller** was selected.
Frequency	Default = Single. Sets how often the alarm should occur. The options are: • **Single** • **Daily** • **Weekly**
Day	Default = Today. Set the day for the alarm. You can select a specific day or **Today**.
File	Default = Blank. Optional. If a file is specified here it is used for the alarm call. If no file is specified the default alarm message "This is an alarm call, please hang up" is used.
Display Text	Default = Blank. By default the alarm will display "Alarm" on the target if it is an Avaya display telephone. This field can be used to customize the text used.
Ring Time	Default = 60 seconds. Range = 5 to 120 seconds. Set the length of ring time used for the alarm call if not answered.
Retries	Retries: Default = 0 (Off). Range = 0 to 10. Used to specify how many times the alarm should be repeated if it is not answered and cleared. When a value other than 0 is selected, the Interval option becomes available to specify the interval between repeats.
Interval	Default = Blank (Off). If a number of retires is specified, this option can be used to select the number of minutes between repeated alarm attempts until the alarm is cleared.
Enable Cancel Code	Default = No. When off, the alarm is cleared if the alarm call is answered. When on, a dialing code can be specified. If the correct code is not dialed in response to an alarm, the alarm is not cleared and will repeat if retries have been specified.

Table continues…

Field	Description
Cancel Code	Default = * , Range = Up to 4 digits. used to enter the dialing required to clear the alarm call. The value * will match any dialing. To cancel the alarm, the cancel code must be entered followed by the hash key (#). The file used to play the alarm message must mention the cancel code and the fact that cancel code must be followed by the hash key (#).
Alarms The following additional fields are displayed in the Alarms table.	
Created	
Next Activation	
Type	
When	
Number	

Related links

Voicemail Pro — System Preferences on page 450

User Group

Navigation: **Applications** > **Voicemail Pro — System Preferences** > **User Group**

Field	Description
User Group	
Name	

Related links

Voicemail Pro — System Preferences on page 450

Voicemail Pro — Call Flow Management

Navigation: **Applications** > **Voicemail Pro — Call Flow Management**

Select **Voicemail Pro** to launch a locally installed version of the Voicemail Pro application.

Note:

This option is not available on IP500 V2 systems.

Voicemail Pro software version

The **Launch Voicemail Pro** action launches a locally installed version of the Voicemail Pro application. The application launch behavior depends on the version of Voicemail Pro installed.

Voicemail Pro version is current: If the Voicemail Pro version is current, Voicemail Pro launches without a login prompt.

Voicemail Pro version is not current: If the Voicemail Pro version is not current, you are prompted to download and install the latest version and a link is provided. You can continue to use the currently installed version or download the current version. Upgrading to the current version requires a browser restart.

Voicemail Pro is not installed: If Voicemail Pro is not installed, you are prompted to download and install the latest version and a link is provided. Once Voicemail Pro is installed, a browser restart is required before launching Voicemail Pro.

Related links

Applications on page 448

one-X Portal

Navigation: **Applications** > **one-X Portal**

Select **one-X Portal** to launch a locally installed version of the one-X Portal application. Note that this option is only usable for portal administration access.

Note:

This option is not available on IP500 V2 systems.

Note:

In order to open a client application (for example Manager), you must log into Web Manager using the IP Office LAN 1 IP address.

Related links

Applications on page 448

WebRTC Configuration

Navigation: **Applications** > **WebRTC Configuration**

Note:

This option is not available on IP500 V2 systems.

Related links

Applications on page 448
System Settings on page 463
SIP Server Settings on page 464
Media Gateway Settings on page 465

System Settings

Navigation: **Applications** > **WebRTC Configuration** > **System Settings**

The system settings which are applicable to all components of the WebRTC Gateway.

File	Description
Network Interface	Default = eth0. A list of available network interfaces on the Server. It is recommended to use the same network interface selected at IP Office configuration.
Local IP Address	Default = IP address of default network interface. A read-only field to show the IP address of the selected network interface.
Gateway Listen Port	Default = 42004. The local listen port used by the WebRTC Gateway to accept SIP connections.
SIP Trunk Listen Port	Default = 42008. Local listen port used by WebRTC Gateway to accept SIP trunk connections.
Logging Level	Default = Info. Available log levels for the WebRTC Gateway. Changing the log level causes the WebRTC Gateway to restart. The options are • **Error** • **Warn** • **Info** • **Debug** • **Trace**
Allow Origins	Default = localhost Type the Domain names and IP addresses you want IP Office to accept connections from. If there are more than one entry, separate the entries by a semicolon (;). These Domain names and IP addresses are added to the WebRTC Gateway's CORS filter. WebRTC Gateway accepts WebSocket connections only from the Domain names and IP addresses whitelisted in the field. The Gateway maintains a list of Domain names and IP addresses to comply with Cross-Origin Resource Sharing (CORS) that enables cross-domain requests from Web browsers to servers and Web APIs. Adding a `*` in this field allows connections from all Domains and IP addresses including Chrome extensions. Example: "`203.0.113.56`"; "`203.0.113.57`"; "`*.example.com`" If the above values entered in the field, connections from the IP addresses `203.0.113.56`, `203.0.113.57`, and any domains ending with `example.com` is allowed.

Related links

WebRTC Configuration on page 462

SIP Server Settings

Navigation: **Applications** > **WebRTC Configuration** > **SIP Server Settings**

The IP Office SIP settings used by WebRTC Gateway.

Field	Description
Configuration Mode	Default = Auto. The options are: • **Auto**: The settings are automatically populated and read-only. • **Manual**: Set to **Manual** to change any automatically populated value.
Domain Name	Default = Automatically populated value or blank. The SIP domain name of the Server Edition Primary server.
Private IP Address	Default = Automatically populated value or blank. Private IP address of the Server Edition Primary server.
Private TCP Port	Default = Automatically populated value or blank. Private TCP port of the Server Edition Primary server.
Private UDP Port	Default = Automatically populated value or blank. Private UDP port of the Server Edition Primary server.
Private TLS Port	Default = Automatically populated value or blank. Private TLS port of the Server Edition Primary server.
Public IP Address	Default = Automatically populated value or blank. Public IP address of the Server Edition Primary server.
Public TCP Port	Default = Automatically populated value or blank. Public TCP port of the Server Edition Primary server.
Public UDP Port	Default = Automatically populated value or blank. Public UDP port of the Server Edition Primary server.
Public TLS Port	Default = Automatically populated value or blank. Public TLS port of the Server Edition Primary server.
Transport Type	Default = Automatically populated value or blank. Transport type used by the WebRTC gateway, to connect to IP Office. The options are: • TCP • TLS

Related links

WebRTC Configuration on page 462

Media Gateway Settings

Navigation: **Applications** > **WebRTC Configuration** > **Media Gateway Settings**

File	Description
RTP Port Range (Private) Minimum	Default = 58002. Minimum RTP port value used for WebRTC media termination from the private interface.
RTP Port Range (Private) Maximum	Default = 60002. Maximum RTP port value used for WebRTC media termination from the private interface.
RTP Port Range (Public) Minimum	Default = 56000. Minimum RTP port value used for WebRTC media termination from the public interface.
RTP Port Range (Public) Maximum	Default = 58000. Maximum RTP port value used for WebRTC media termination from the public interface.
Codecs — Audio	The audio codecs used by the WebRTC Gateway, listed by priority. Use the arrows to change the priority. The options are: 1. PCMU 2. PCMA 3. telephone-event
Codecs — Video	The audio codecs used by the WebRTC Gateway. The options are: 1. VP8
DTMF Payload Type	Default = 101. RFC2833 default payload type used by the WebRTC Gateway.
STUN Server Address	Default = Blank. STUN server address (optional).
STUN Server Port	Default = Blank. STUN server port (optional).
TURN Server Address	Default = Blank. TURN server address (optional).
TURN Server Port	Default = Blank. TURN server port (optional).

Table continues…

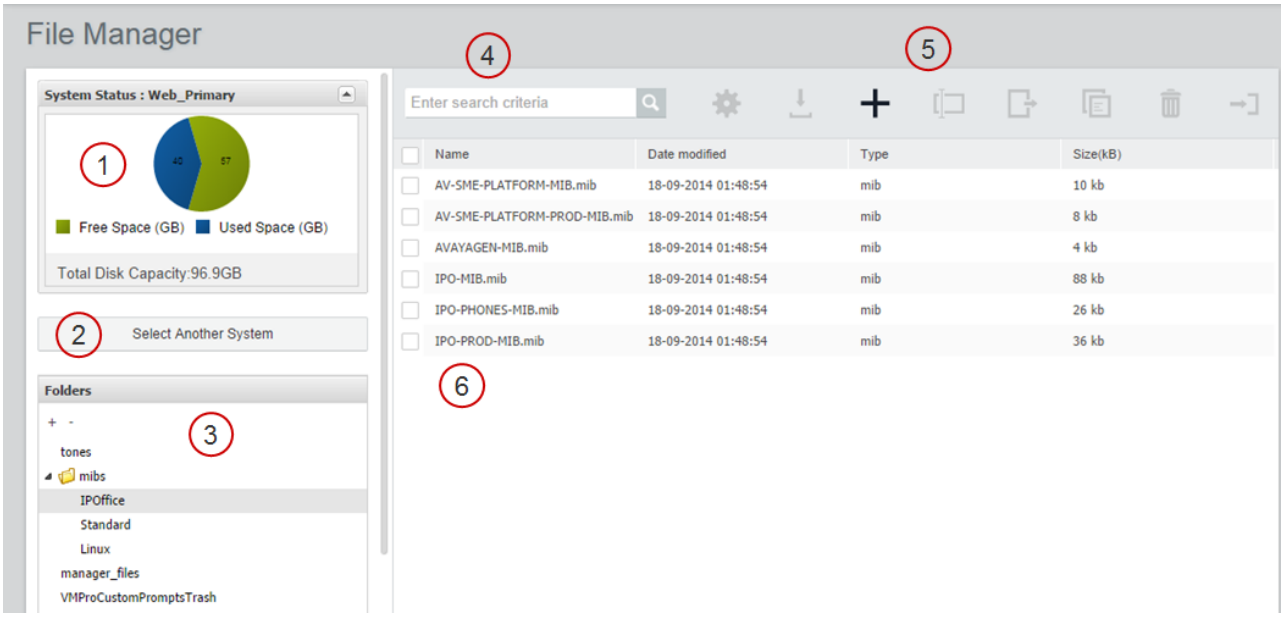
File	Description
TURN User Name	Default = Blank. TURN user name (optional).
TURN Password	Default = Blank. Password for Turn user name, if used.
Enforce TURN	Default = No. When set to Yes, enforces media traffic via the TURN server.

Related links

WebRTC Configuration on page 462

File Manager

Navigation: **Applications** > **File Manager**



1	Graphic representation of disk capacity for the currently selected system.
2	Click to load a server into the File Manager.
3	The system folder directory. Select a folder to display the contents in the file list.
4	File search tool.
5	File management tool bar. Select a file in the file list to enable the tools.
6	File list.

Related links

Applications on page 448

Media Manager

Navigation: **Applications** > **Media Manager**

Note:

This option is not available on IP500 V2 systems.

Related links

Applications on page 448
Configuration on page 467

Applications > **Media Manager** > **Configuration**

Connector on page 469

Applications > **Media Manager** > **Connector**

Alarms on page 470

Applications > **Media Manager** > **Alarms**

Recording on page 470

Applications > **Media Manager** > **Recording**

Migration on page 472
Audit Trail on page 473

Applications > **Media Manager** > **Audit Trail**

Configuration

Applications > **Media Manager** > **Configuration**

Name	Description
Profile	Default = Blank The unique name that identifies a configuration profile.

Table continues…

Name	Description
Log Level	Default = INFO The type of log level. The options are: • INFO • DEBUG • ERROR
Handover Folder	Default = `/opt/vmpro/MM/VRL` The Voicemail Pro path from where IP Office Media Manager picks up the recordings. Voicemail Pro writes call recording files to this folder.
Call Storage Path	Default = Blank. The path to a local Hard Disk Drive (HDD) partition that IP Office Media Manager uses to store the recordings after collecting them from the directory specified in the **Handover Folder**. If the additional drive was added using the path `/additional-hdd#1`, enter `/additional-hdd#1/partition1`. The additional drive path used can be seen using the Platform View menus of the server If you must change the value after you have already started recording, copy all the sub-directories and files in the old directory to the new directory before you resume recording.
Months to Retain Calls	Default = 60 The number of months for which the database retains the call details. After the said period, IP Office Media Manager can delete the call recordings. To disable the deletion of call recordings, enter **0** in this field.
Audit Retain Period (Days)	Default = 180 days The number of days for which the Audit Trail or recordings are retained in IP Office Media Manager. The minimum value for this field is 1 day and the maximum 365 days.
Active Connector	The connector that is currently being used for remote archiving. The drop-down menu lists all the available connectors where you can archive your recordings. Changing the connector results in a change in the archive destination. However, the recordings from the pervious archives are still available for the users.
Send Email	Default = No The option to select whether the system must send emails for alarms and events. The options are: • Yes • No
SMTP Mail Server	Default = Blank The SMTP mail server that IP Office Media Manager uses to send email messages about alarms and events. If you leave this field blank, system cannot send email messages for alarms and events.

Table continues…

Name	Description
SMTP Port	Default = Blank The SMTP port to which the service sends email messages.
Secured Connection	Default = No The option to indicate whether the connection is secured. A secured connection uses Transport Layer Security (TLS) protocol to communicate. The options are: • Yes • No
SMTP User Name	Default = Blank The user name for the SMTP server. You can leave this field blank if SMTP server does not require sender authentication. If required, set the user name here.
SMTP Password	Default = Blank The password for the SMTP server. You can leave this field blank if SMTP server does not require sender authentication. If required, set the password here.
SMTP Mail "From" Address	The address from which the SMTP emails containing the alarms and events originate.
Send Alarm/Event Emails To	The email addresses to which alarms and events must be sent. You can add more than one email address by adding a semi colon (;) between two email addresses.

Related links

Media Manager on page 467

Connector

Applications > **Media Manager** > **Connector**

Name	Description
Add	The drop-down menu to select a connector. The options are: • NAS • Google drive • DVD
Name	The name of the connector.
Type	The type of connector selected.
Active	The state of the connector.

Table continues…

Name	Description
Reachable	The field that indicates whether the connector is reachable.
Pending Files #	The files that are yet to be archived.
Lasts Successful Archive Time	The time when the last successful archive was done using the selected connector.

Related links

Media Manager on page 467

Alarms

Applications > **Media Manager** > **Alarms**

Name	Description
Date	The date on which the alarm was generated.
Severity	The severity of the alarm. The options are: • Information • Warnings • Minor Alarms • Major Alarms • Critical Alarms
Description	A brief description about the alarm.

Related links

Media Manager on page 467

Recording

Applications > **Media Manager** > **Recording**

Name	Description
Call Date	The date of the call.
Length	The duration of the recording.
Parties	The users that participated in a conference call.
Call Direction	The field indicates whether the call was Internal, Incoming, or Outgoing.
Agents	The agents involved in the call.

Table continues…

Name	Description
Owner	The owner of the recording. Each recording has an owner; the owner is the number of the extension that recorded the call. Any one of the following can be an owner: • Calling party extension • Called party extension • Hunt group extension • A line number • An account code • An agent extension
Targets	The phone numbers of the recipients of the call.
Skills	The skill set of the agent involved in the call.
Call ID	The unique identification number associated with the call recording.

Filter

Name	Description
Recording Range (Date and Time)	The date and time range between which the call was recorded. Use the calendars to select the dates and the adjacent drop-down menus to specify the time.
Recording Length	The length of the recording. Select one of the signs and enter the time in seconds. The available signs are: • = : Equal to the recording length you have specified. • < : Less than the recording length you have specified. • > : Greater than the recording length you have specified. • >= : Greater than or equal to the recording length you have specified. • <= : Less than or equal to the recording length you have specified.
Call Direction	The direction of the call, that is, whether the call is Internal, Incoming, or Outgoing. Use the drop-down menu to select a Filter criterion.
Parties	The parties involved in the call. Type the names of the parties. For more than one party, type the names separated by a comma.
Agents	The agents involved in the call. Type the names of the agents. For more than one agent, type the names of agents separated by a comma.
Target Number	The phone number of the recipient of the call. Type the target number.
Skills	The skill set of the agent involved in the call.
Call ID	The unique identification number associated with the call recording.

Button	Description
Apply Filter	Click to apply the filter. All the recordings matching your search criteria are displayed on the right pane.
Show All	The system displays all the recordings on the right pane.
Delete	Use the button to delete the selected recordings. You can select one or more recording using the check boxes corresponding to the recordings.
Download	Use the button to download multiple recordings to your computer. Select the recordings and click the Download button. Type a password to protect the recordings. IP Office Media Manager saves the recordings in `.opus` file format in your computer.

Related links

Media Manager on page 467

Migration

IP Office Release 11 does not support Contact Recorder. However, existing customers of Contact Recorder can migrate their call record database to Media Manager, which is the only archiving solution in IP Office Release 11. The migration process includes migration of only the metadata of the call records stored in Contact Recorder locally, or remotely on DVD or NAS. The migration process does not move the actual media files. Using the migrated metadata, Media Manager identifies the call recordings and provides playback, downloading, and housekeeping facility. VRLA records migrated from Contact Recorder can still be verified for tampering using the Media Manager interface Thus Media Manager becomes a single interface for all call records, whether archived through Media Manager for newer recordings or the older recordings archived through Contact Recorder.

Existing Contact Recorder users can migrate to Media Manager through Web Manager. Administrators can migrate the Contact Recorder database to Media Manager using **Applications** > **Media Manager** > **Migration**. For detailed instructions, see the *Administering Avaya IP Office Platform Media Manager* guide.

Note:

Contact Recorder customers must back up their database prior to upgrading to IP Office Release 11.

Related links

Media Manager on page 467

Audit Trail

Applications > **Media Manager** > **Audit Trail**

Name	Description
Search on "User Name"	The Search text box to search the audit records of a User. Type the User Name to search the users activities in the recording library.
User Name	The name of the user who used the recording.
Timestamp	The time when the recording was used.
User Action	The type of user action on a recording. This specifies whether a recording was replayed, downloaded, deleted, or searched.
Details	The details of a recording such as owner of the recording, media name, calling party name, and so on.
Start Date	The date and time after which the event has occurred. Use the calendar to select the date and the adjacent drop-down menu to specify the time.
End Date	The date and time before which the event has occurred. Use the calendar to select the date and the adjacent drop-down menu to specify the time.
Event Type	The type of events you want to view. IP Office Media Manager keeps track of the following type of operation on the recordings: • **Delete**: Displays the recordings that are deleted. • **Download**: Displays the recordings that are downloaded. • **Replay**: Displays the recordings that are replayed. • **Search**: Displays the recordings that are searched.
Export	The option to export the filtered audit results as a zipped `.CSV` file on your computer. The file contains four columns with the following information: • **User Name** • **Timestamp** • **User Action** • **Details**

Filter

Button	Description
Apply Filter	Use the button to refine your search. You can filter your search based on any one of the following criteria or both: • **Start Date and End Date**: Filters the recordings used between these two dates. • **Event Type**: Filters the recordings based on the type of use.
Clear Filter	Use the button to clear the filter.

Related links

Media Manager on page 467

Web License Manager

Navigation: **Applications** > **Web License Manager**

Select **ApplicationsWeb License Manager** to open the Avaya Web License Manager (WeBLM) application in a web browser.

Note:

This option is not available on IP500 V2 systems.

Login Credentials

WebLM credentials are managed separately from IP Office system passwords and are not part of single sign on. You must change the default password for the admin user after the first login. The default credentials are:

- User ID: `admin`
- Password: `weblmadmin`

Related links

Applications on page 448

Chapter 9: Backup and restore

Backup overview

Related links

Backup and restore policy on page 475
Backup and Restore location on page 476
Backup data sets on page 477
Disk Usage on page 478
Managing Disk Space for Backup and Restore on page 480

Backup and restore policy

It is essential to implement a comprehensive, robust and secure backup policy as part of a Business Continuity plan before any failure or other data restoration requirement. It is not possible to define a single approach that would meet all possible customer needs. Each installation should be assessed before a policy is derived.

The following IP Office Server Edition aspects must be considered as part of such a policy:

- Ignition settings. These must be printed or saved for each Linux Server after initial ignition.
- IPOSS/SSLVPN onboarding.xml file: One for each on-boarded system should be saved. If not saved earlier, this file can be retrieved from the file system:
  - IP500 V2: `primary\ws\onb\onb_<date>T<time>.xml`
  - Linux: `system\ws\onb\onb_<date>T<time>.xml`
- License key data: All PLDS license key files must be saved.
- Manual configuration backup for each IP Office after initial installation and major configuration change.
- Manual configuration backup for Voicemail Pro after initial installation and major configuration change.
- Manual configuration backup for one-X Portal after initial installation and major configuration change.
- Periodic configuration backup for every IP Office.
- Periodic configuration backup for one X Portal – Server Edition Primary server and Application Server only
- Periodic configuration backup for Voicemail Pro – Server Edition Primary server only

- Periodic voice mailbox and recording data backup – Server Edition Primary server only
- The timing of backup operation: This should be done when little or no traffic is present on the target system(s), but the backup process itself is not service-affecting.
- The timing of restore operation: This should be done when no traffic is present on the restored system(s). The restore process is service affecting – any restored component will automatically restart immediately the restore is complete.
- Security, integrity, location and capacity of backup data storage.
- Note that backup of an Avaya Linux server does not include any locally-stored backup data. For example, if using the Server Edition Primary server as a backup destination for an Expansion, then performing a backup of the Server Edition Primary server will not create a backup of the whole solution; only the Server Edition Primary servers's data will be saved.
- Security of backup data communication
- Backup prior to and after any software upgrade; in general it is not possible to restore backup data set onto a different software version.
- Backup prior to and after any hardware upgrade.

The period and number of unique instances selected should reflect the frequency of change, the consequence due to data loss, and the storage capacity of the backup data server. Periodic backups using Web Manager have up to 14 instances (plus a single manual backup instance), after which the oldest set is overwritten. These instances are per backup server and regardless of the backup data set; for example two weekly separate backup tasks of all IP Office configurations and Voicemail configuration will overwrite the first set after 7 weeks.

Related links

Backup overview on page 475

Backup and Restore location

IP Office Linux Server as the Backup/Restore location

You can set any Linux Server as the backup and restore location. To create a dedicated IP Office Linux server for backup and restore, install an IP Office Application Server without enabling the Voicemail Pro and one-X Portal for IP Office applications on that server.

Security alert:

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

The following table provides details of backup file store for the following protocols and settings.

Protocol	Port	Remote Path	User Name/ Password	Notes

Table continues…

HTTP	8000	/avaya/backup	none	HTTP supported by all IP Office components. Disabled by default. [1]
HTTPS	5443	/avaya/backup	none	HTTPS supported by all IP Office components. Enabled by default.
SFTP	22	/var/www/html/avaya/backup	Any service user with *WebControl Admin* rights, Root (not recommended)	SFTP supported by Linux-based components. Enabled by default.
SCP	22	/var/www/html/avaya/backup	Any service user with WebControl Admin rights, Root (not recommended)	SCP supported by Linux-based components. Enabled by default.

1. To enable HTTP, use the Web Control application. Go to **Settings** > **System** > **HTTP Server** and select the check box for **Enable HTTP file store for backup/restore**.

Note:

To perform a restore, use the same *Remote Server* (protocol, port and path) settings.

Related links

Backup overview on page 475

Backup data sets

The following table provides information about the backup data sets:

Data Set	Content	Notes
IP Office Configuration (V2)	• Configuration • Security Settings • DHCP Allocations • Call log	When selected for IP500 V2 Expansion systems

Table continues…

IP Office Configuration (L)	• Linux Server Settings • Web Management Settings • Configuration • Security Settings • DHCP Allocations • Call log	When selected for Primary, Secondary, one-X Portal Server, and Linux Expansion systems This backup set does not include any back data on the server itself.
One-X Portal Configuration	one-X Portal server settings	
Voicemail Pro Configuration	• Voicemail Pro server preferences • Call flows	
Messages & Recordings	• Voice mailbox contents • Call recordings	
Voicemail Pro Full	• Voicemail Pro server preferences • Call flows • Voice mailbox contents • Call recordings	
Selective Voicemails		

Related links

Backup overview on page 475

Disk Usage

The tables below can be used to calculate the required disk space for backups.

Example:

A Server Edition deployment has 2500 users with 150 nodes and 500 hunt groups. The Primary Server is an R620 machine.

From the server disk usage table, the Primary Server occupies 170 GB of space. A solution backup requires 189 GB. The total is 359 GB.

Since the server disk capacity is 600 GB, the Primary Server has the capacity to act as the backup server.

Table 1: Server disk capacity

Server	R620	DL360	DL120	R210	OVA (default)	OVA (max supported) [1]
Nominal disk capacity (GB)	600	300	250	500	100	166
Max solution users	3,000	2,000	1,500	1,500	750	3,000

1. Requires disk size increase.

Table 2: Primary / Secondary / Expansion server disk usage

Solution	Max No. of users	100	750	1500	2000	2500
	Max No. of nodes	5	50	100	125	150
	Max No. of groups	20	150	300	400	500
Primary / Secondary max disk usage (no backup, one-X collocated) (GB)		75	100	130	150	170
Expansion max disk usage (no backup) (GB)		48	48	48	48	48
one-X standalone max disk usage (no backup) (GB)		49	49	49	49	49
Solution Max backup size (GB)	**Configuration only**	2	13	25	31	37
	All data	35	78	127	158	189

Table 3: Application Server disk usage

No. of VMPro users	20	50	100	150
No. of Hunt Groups	4	12	20	30
Application Server max disk usage (GB)	117	117	117	118
Max backup size config only (GB)	1	1	1	1
Max backup size all data (GB)	30	32	34	37

Related links

Backup overview on page 475

Managing Disk Space for Backup and Restore

Any Server Edition server can be used as a backup server, if there is sufficient disk space. The minimum available disk space required in order to use a Server Edition server or Application Server as a backup server is 60 GB or 120 GB if VMPro is installed. Information on the disk space available for backup is displayed in the Web Control application. On the **System** page, see **Quota available for backup data**.

You can use an Application Server solely as a backup server if the one-X Portal and Voicemail Pro applications are not installed. The disk capacity (total disk space) must be at least 60 GB.

Note:

The backup and restore process uses the OS disk. The additional disk is for Contact Recorder only.

Using a virtual Server Edition machine as a backup server

To use a Primary, Secondary, or Application server as a backup server, you must increase the disk size or uninstall Voicemail Pro. For information on increasing the available disk size, see *Deploying Avaya IP Office™ Platform Server Edition Servers as Virtual Machines*.

A virtual Server Edition expansion system can be used as a backup server without increasing the disk size since by default, Voicemail Pro is not installed.

You can use an Application Server solely as a backup server if the one-X Portal and Voicemail Pro applications are not installed. The disk capacity (total disk space) must be at least 60 GB.

Related links

Backup overview on page 475

Backing up an IP Office Server Edition server

The system backs up the configuration of the server, application and user data in a single file set. You can use this backup file to restore the server or a failed server upgrade. The system backs up the configuration of the application to a local drive, in a predefined directory. You can take a backup of the primary server on a remote file server, which can optionally be the secondary server.

Before you begin

- You can schedule a back up, set the proxy, and a remote server using Web Manager **Solution Settings**.
- Log into Web Manager as *Administrator*.

About this task

You can take a back up of the primary server on a remote file server using Web Manager:

Procedure

1. In the Web Manager menu bar, click **Solution**.
2. In the Solution page, select the component or components that you want to backup.

   To select all the components, click the **Actions** check box .
3. Click **Actions** and select **Backup**.
4. Do one of the following:
   - To back up immediately:
     a. In **Select Remote Server** drop down list, select the remote server that you have set.
   - To back up immediately using a proxy:
     a. In **Select Remote Server** drop down list, select the remote server that you created.
     b. Under **Proxy Settings**, enable **Use Proxy**.
     c. In the **Select Proxy** list, select the proxy details that you created.
   - To back up at a scheduled time:
     a. In **Select Remote Server** drop down list, select the remote server that you have set.
     b. Under **Schedule Options**, enable **Use Schedule**.
     c. In the **Select Schedule** list, select the schedule option that you created.
     d. Set a **Start Date** and a **Start Time**.
     e. To configure a recurring backup, set **Recurring Schedule** to **Yes** and then set the **Frequency** and **Day of Week**.
   - To back up the IP Office sets:
     a. In the **Select Remote Server** drop down list, select the remote server that you have set.
     b. In the **Select IP Office Sets** list, select the IP Office set that you want to back up.
   - To back up one-X Portal sets:
     a. In the **Select Remote Server** drop down list, select the remote server that you have set.
     b. In the **Select one-X Portal Sets** list, select the one-X Portal set that you want to back up.
   - To back up Voicemail Pro sets:
     a. In the **Select Remote Server** drop down list, select the remote server that you have set.
     b. In the **Select Voicemail Pro Sets** list, select the Voicemail Pro set that you want to back up.

- To back up WebLM sets:
  a. In the **Select Remote Server** drop down list, select the remote server that you have set.
  b. In the **Select WebLM Sets** list, select the WebLM set that you want to back up.
- To back up WebRTC sets:
  a. In the **Select Remote Server** drop down list, select the remote server that you have set.
  b. In the **Select WebRTC Sets** list, select the WebRTC set that you want to back up.
- To back up Media Manager sets:
  a. In the **Select Remote Server** drop down list, select the remote server that you have set.
  b. In the **Select Media Manager Sets** drop down list, select the Media Manager configuration you want to back up.

5. In the **Backup Label** field, type a label for the backup.
6. Click **OK**.

Restoring an IP Office Server Edition server

You can restore the primary server using the backup file on a remote file server using Web Manager. You can restore the primary server using the backup file on a local drive or a remote file server, which can optionally be the secondary server.

Note:

You cannot restore the backup data of one component to another component, unless, either the IP Address or the system ID (LAN1 mac address) of the components are the same.

Before you begin

Warning:

Close any Voicemail Pro client before restoring.

The restoration process requires the voicemail service to shutdown and restart. This does not occur if any Voicemail Pro client is connected to the service during the restore and leads to an incorrect restoration of files.

Procedure

1. In the Web Manager menu bar, click **Solution**.
2. In the Solution window, select the component that you want to restore.

   To restore all the components, select the **Actions** check box .

3. Click **Actions** and select **Restore**.
4. Do one of the following:
   - To restore from a remote server:
     a. In the **Select Remote Server** drop down list, select the remote server that you have set.
   - To restore using a proxy:
     a. In the **Select Remote Server** drop down list, select the remote server that you created.
     b. Enable **Use Proxy**.
     c. In the **Select Proxy** list, select the proxy details that you created.
5. Click **Get Restore Points**.

   The system displays the restore points with details such as name of the backup, type of backup, IP address of the server , the version, sets of backup, and the time stamp of the backup in **Select Restore Point** table.
6. Select the restore point from the **Select Restore Point** table.
7. Click **OK**.

Restoring a failed IP Office Server Edition server

Before you begin

Note:

You cannot restore the backup the data of one component to another component, unless, either the IP Address or the system id (LAN1 mac address) of the components are the same.

Ensure that you shutdown all the services on the server.

Procedure

1. Install the IP Office Server Edition server.

   For information about installing IP Office Server Edition, see *Deploying Avaya IP Office™ Platform Server Edition*.
2. Restore the following:
   a. Restore the Server Edition Primary server.
   b. Restore the Voicemail Pro server.
   c. Restore the Avaya one-X® Portal for IP Office server.
3. Add the Server Edition Secondary server.

4. Add the Server Edition Expansion System.

Chapter 10: Configure General System Settings

Applying Licenses

For a description of IP Office licenses and for information on licensing requirements, see *Avaya IP Office Platform™ Solution Description*.

Related links

PLDS licensing on page 485
Web License Manager (WebLM) on page 486
Server Edition Centralized Licensing on page 487
Distributing Server Edition Licenses on page 487
Procedures for Applying Licensing on page 492

PLDS licensing

IP Office uses the Avaya Product Licensing and Delivery System (PLDS) to manage licenses. PLDS is an online, web-based tool for managing license entitlements and electronic delivery of software and related license files. PLDS provides customers, Avaya Partners, distributors, and Avaya Associates with easy-to-use tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads. You can access PLDS from http://plds.avaya.com/.

PLDS license files

Licenses are delivered from PLDS with license files. A PLDS license file is generated for installing on a specific machine. There are two deployment options:

- PLDS Nodal license files are generated for and installed on particular IP Office nodes.
- PLDS WebLM license files are generated for and installed on a WebLM server that can license multiple IP Office nodes.

WebLM centralized licensing is supported in IP Office Server Edition and in IP Office Branch deployments, but not in non-Branch deployments of IP Office Standard mode.

PLDS host ID

PLDS Nodal license files are machine specific and you must specify the host ID in the **PLDS host ID** field on **System Settings** > **Licenses** > **Systems** > **Manage Licenses**.

IP500 V2 systems: You can find the PLDS host ID in the **Licensing** tab of IP Office Manager and Web Manager. The PLDS host ID is made of the two digits “11”, followed by the 10 digit feature key serial number printed on the IP Office SD card. If the SD card is changed, the PLDS host ID will also change.

IP Office Linux servers: The PLDS host ID can be found on the server labeling, the server packaging label, and the system ignition Login screen. The PLDS host ID is derived from the system ID. If the system ID changes, the PLDS host ID will also change.

WebLM: The WebLM host ID is the Mac address of the WebLM server. In a virtual environment, the WebLM host ID is a virtual Mac address that starts with the letter “V”. The WebLM host ID must be used when generating a PLDS license file for the WebLM server in order to implement a centralized licensing scheme for multiple IP Office systems. The WebLM host ID can be found on the server labeling, the server packaging label, the system ignition Login screen, and through the WebLM management interface.

Related links

Applying Licenses on page 485

Web License Manager (WebLM)

The Web License Manager (WebLM) is a web-based application for managing licenses. If you use the WebLM server running on the IP Office server, then you can use IP Office Web Manager to log in to the WebLM server by selecting **Applications** > **Web License Manager**. WebLM credentials are managed separately from IP Office system passwords and are not part of single sign on (SSO).

Note:

- WebLM license management is supported for Server Edition deployments and for Enterprise Branch deployments using the System Manager WebLM server. It is not supported for Standard Mode systems.
- When upgrading from a previous release, all systems must be running the same software level. IP Office Server Edition does not support mixed versioning.

For more information on WebLM, see *Administering standalone Avaya WebLM*.

To establish communication between IP Office and the WebLM server, you must configure the remote server profile on **System Settings** > **Licenses** > **Systems** > **Remote Server** .

Note:

When upgrading from release 9.1, the WebLM server is not started automatically. Perform the following steps to start the WebLM server.

1. Log in to Web Manager.
2. Select **Server Menu** > **Platform View** > **System**.
3. Under **Services**, select the WebLM server and click **Start**.

Related links

Applying Licenses on page 485

Server Edition Centralized Licensing

Before release 10, Server Edition deployments used nodal licensing. This type of licensing can still be used in release 10 and higher. However, it is expected that most deployments will prefer to centralize license management using the Avaya Web License Management (WebLM) server. The WebLM server is automatically installed on the Server Edition Primary server. For newly installed systems, centralized licensing is the default configuration.

All systems in the Server Edition solution must use the same **License Source**.

Nodal licensing

With nodal licensing, license files must be installed on each node in the system. For some licensed features, the required license can be installed on the Server Edition Primary server and used by all nodes in the system. However, for other licensed features, the required license must be installed on the node where the feature is used.

Centralized licensing

As of release 10, you can use the WebLM server running on the Server Edition Primary server to fully centralize license management. With centralized license management, all licenses are contained in a single PLDS file uploaded to WebLM. All nodes in the solution obtain their licenses from WebLM.

The IP Office Secondary server and Expansion systems can be configured to request licenses directly from the WebLM server, or to use a proxy option. When configured to use the proxy option, the license requests are sent through the IP Office Primary server, which proxies the requests to the WebLM server. The Primary server does not allocate licenses, but only acts as a proxy.

Systems using nodal licensing can be converted to use centralized licensing. Since PLDS license files are generated using the host ID of the server where they reside, you must regenerate the license file using the host ID of the WebLM server that will host the license file.

Related links

Applying Licenses on page 485

Distributing Server Edition Licenses

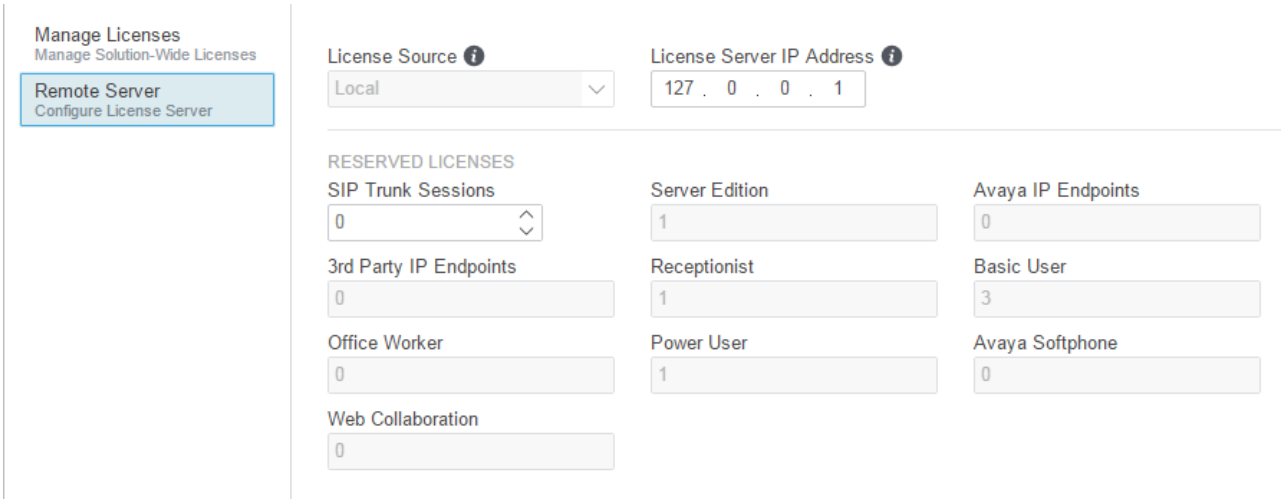
Note:

For a description of IP Office licenses and for information on licensing requirements, see *Avaya IP Office Platform™ Solution Description*.

The **System Settings** > **Licenses** > **Server Menu** > **Remote Server** page displays the **Reserved Licenses** allocated to a Server Edition server.

Note:

The **SIP Trunk Sessions** field has replaced the **System | Telephony | Telephony | Max SIP sessions** setting.



PLDS File Location

How licenses are allocated depends on the location of the PLDS file. For standalone systems, SCN deployments, and Server Edition nodal licensing, each node in the system must have a PLDS file installed.

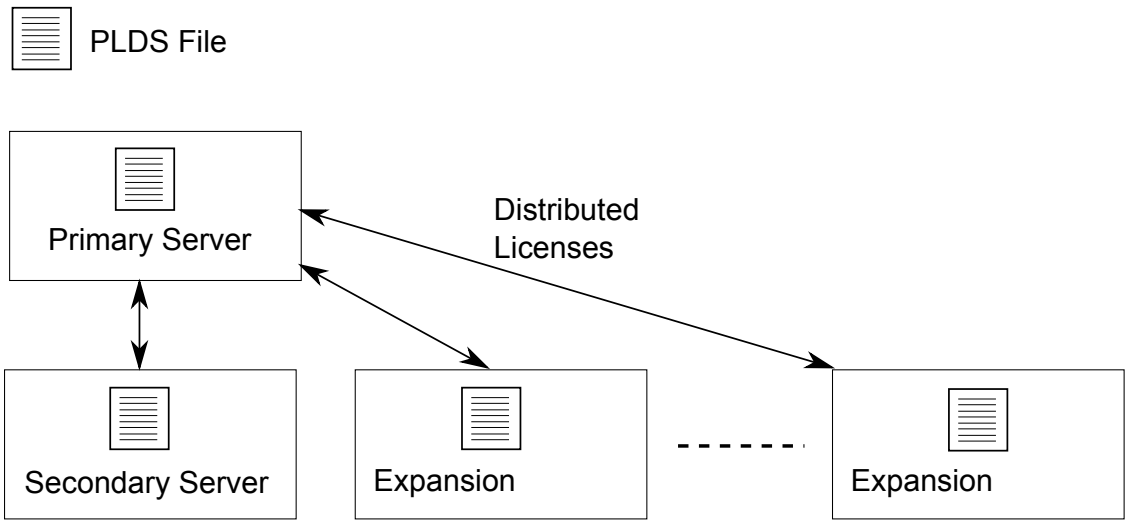


Figure 1: PLDS file location for Server Edition Nodal Licensing

For Server Edition centralized licensing, the PLDS file is located on the WebLM server. The WebLM server can be located on the Primary Server or on a remote server.

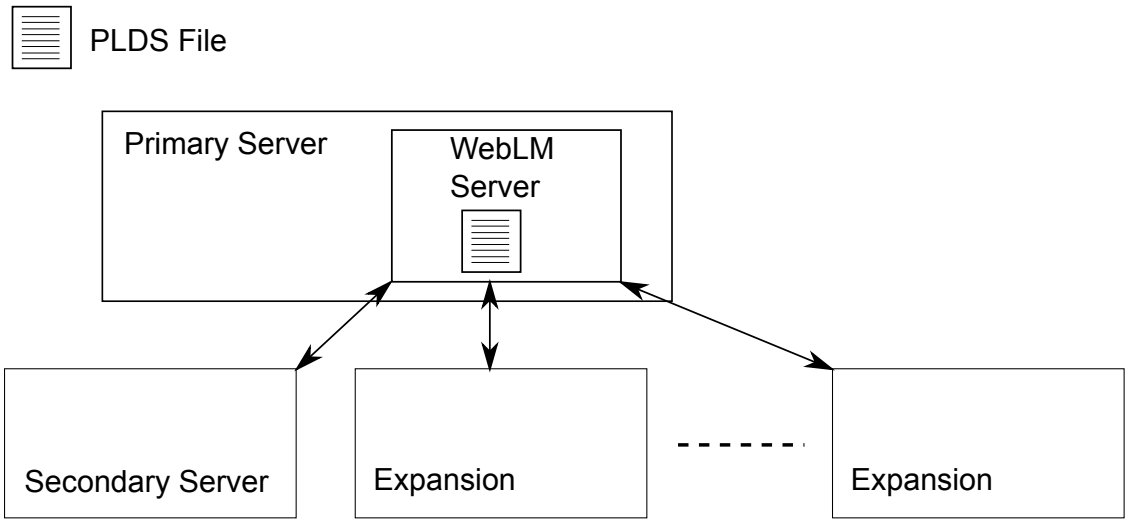


Figure 2: PLDS file location for Server Edition Centralized Licensing

Related links

Applying Licenses on page 485
Nodal license distribution on page 489
Centralized license distribution on page 490

Nodal license distribution

When the **License Source** is **Local**, the **Reserved Licenses** read-only fields indicate licenses that are required for the currently configured features.

Nodal licensing for a Server Edition solution is based on a combination of licensing done through the Server Edition Primary server plus some server-specific licenses. All the user specific and system specific licenses can be managed from the Server Edition Primary server that also acts as a licensing server. Licenses are entered into the configuration of the Server Edition Primary server and are based on the system ID of that server.

Where a license is used to enable features, such as SIP Trunk channels, on other systems, the Server Edition Primary server only allocates those licenses to other systems after it has met its own license needs.

When another system loses connection to the Server Edition Primary server, any license requirements based on those licenses entered in the Server Edition Primary server's configuration are supported for a grace period of 30 days.

Other server specific licenses are entered into the configuration of the server requiring the feature and are based on the System ID of that system.

License	Primary server	Server-specific
Server Edition	Yes	No
Avaya IP endpoints	Yes	No
Third-party IP endpoints	Yes	No
SIP trunk channels	Yes	No
IP500 universal PRI channels	No	Yes
Additional voicemail ports [3]	Yes	No
Web Collaboration	No	Yes
UMS Web Services [1]	No	Yes
Office Worker	Yes	No
Power User	Yes	No
Office Worker to Power User upgrade	Yes	No
Receptionist	No	Yes
CTI Link Pro	No	Yes
Messaging TTS Pro [3]	Yes	No
Voicemail Pro Recording Administrator [2] [3]	Yes	No
WAV User	No	Yes
IPSec tunneling	No	Yes
Video SoftPhone for Mac	No	Yes

1. UMS Web Service licenses are for Hunt Groups only.
2. The Voicemail Pro Recording Administrator license refers to Contact Store. Only one license is required for a Server Edition network.
3. For deployments with dual Voicemail Pro servers, Messaging TTS Pro, Voicemail Pro Recording Administrator, and Additional voicemail ports licenses must be on the Secondary Server.

Related links

Distributing Server Edition Licenses on page 487

Centralized license distribution

When the license source is WebLM, the **Reserved Licenses** read-only fields indicate licenses that are required for the currently configured features. Editable fields can be used to:

- Request additional licenses from the WebLM server.
- Remove licenses from the IP Office node to apply them elsewhere.

Important:

When reallocating licenses, always reduce the number on the IP Office node where they are currently applied before applying them on another node. If you exceed the number of licenses available, you will receive an error message.

Distribution after conversion from Nodal to Centralized licensing

- If the IP Office node needs any of the following licenses, then you must manually configure the respective **Reserved Licenses** editable fields. This will allow the IP Office node to request the licenses from the WebLM server.
  - **VMPro Recordings Administrators**
  - **VMPro TTS Professional**
  - **CTI Link Pro**

Extension Reserved license setting: When the license source is **Local**, the setting **Extension** > **VoIP** > **Reserve License** is set to **None**. Switching the license source to WebLM changes the setting to **Reserve Avaya IP endpoint license**. If required, you must manually change this setting to **Reserve 3rd party endpoint license** or **Both**.

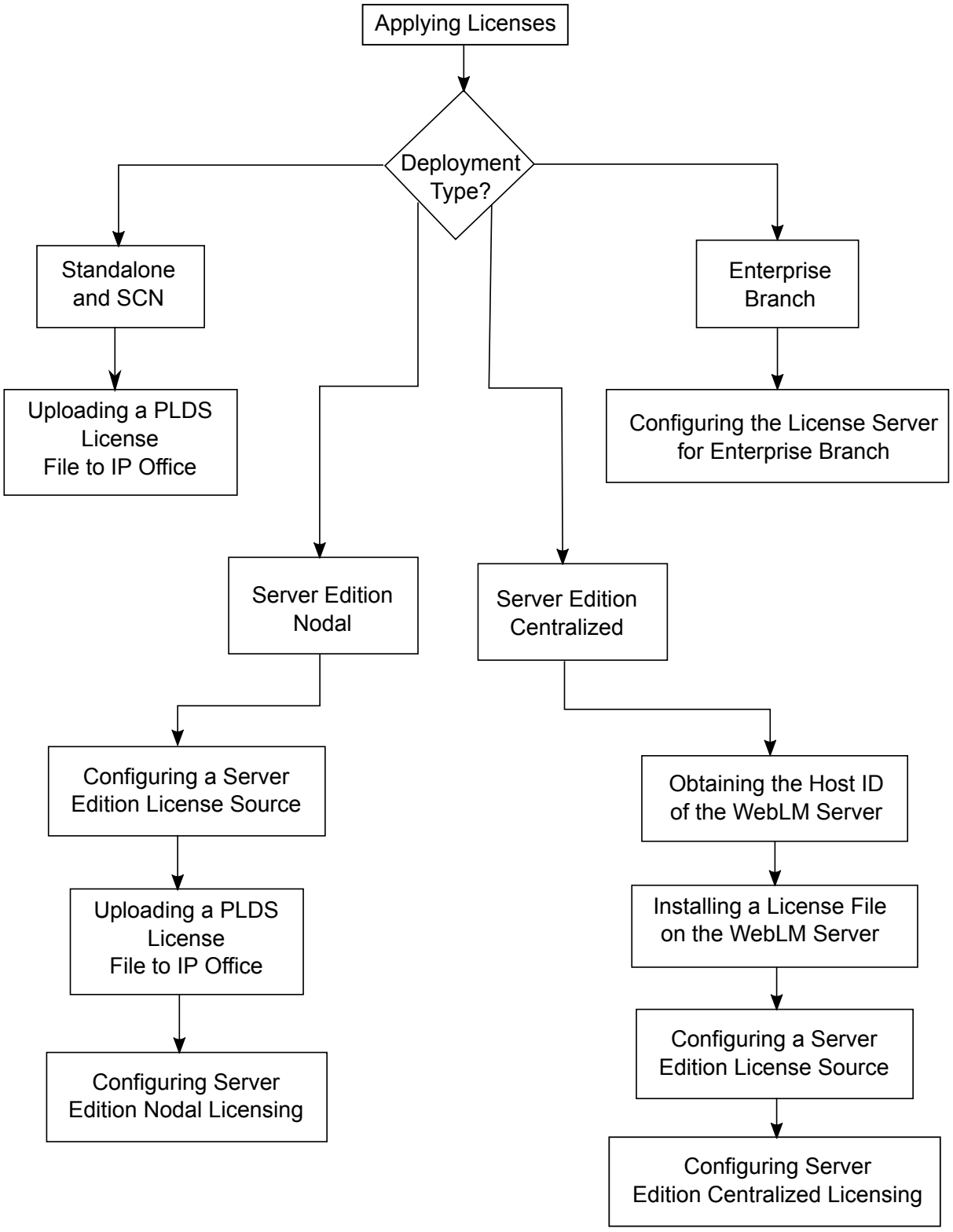
License allocation in WebLM

You can use WebLM to view the licenses used by each node in IP Office Server Edition. In the WebLM navigation pane on the left, click **Licensed Products**. The Acquired licenses table displays information about the licenses acquired for each client ID. In IP Office, the WebLM client ID for each node is displayed on the license Remote Server page.

Related links

Distributing Server Edition Licenses on page 487

Procedures for Applying Licensing



Related links

Applying Licenses on page 485
Obtaining the Host ID of the WebLM Server on page 493
Installing a License File on the WebLM Server on page 493
Configuring the Server Edition License Source on page 494
Uploading a PLDS License File to IP Office on page 494
Configuring Server Edition Nodal Licensing on page 495
Configuring Server Edition Centralized Licensing on page 495
Configuring the License Server in an Enterprise Branch Deployment on page 497

Obtaining the Host ID of the WebLM Server

The WebLM Host ID is required to generate a PLDS license file for centralized licensing. The license file is uploaded to the WebLM server.

Procedure

1. In Web Manager, select **Applications** > **Web License Manager**.
2. Log in to WebLM.
3. In the navigation pane on the left, click **Server Properties**.

   The Server Properties page displays the Host ID. The host ID is the MAC address of the Server Edition Primary server.

   Record the host ID.

Related links

Procedures for Applying Licensing on page 492

Installing a License File on the WebLM Server

Use Web Manager to log in to the WebLM license server and install a license file.

Before you begin

Obtain the license file from the Avaya Product Licensing and Delivery System (PLDS) Web site at https://plds.avaya.com.

You must know the user ID and password for the WebLM server. WebLM credentials are managed separately from IP Office system passwords and are not part of single sign on.

Procedure

1. Log in to Web Manager.
2. Select **Applications** > **Web License Manager**.
3. Log in to the WebLM server.
4. In the left navigation pane, click **Install license**.
5. On the Install license page, click **Browse** to select the license file.

6. Click **Install** to install the license file.

   WebLM displays a message upon successful installation of the license file.

   If the installation is not successful, for troubleshooting information see *Administering Avaya WebLM*, available on the Avaya support site at https://downloads.avaya.com/css/P8/documents/100157154.

Related links

Procedures for Applying Licensing on page 492

Configuring the Server Edition License Source

For Server Edition deployments, the license source can be centralized or nodal.

- With centralized licensing, the PLDS license file resides on the WebLM server. The WebLM server is the license source and all nodes in the solution receive licenses from the WebLM server. The WebLM server can run on a remote machine or on the Primary Server.
- With nodal licensing, a PLDS license file is uploaded to each node.

All systems in the Server Edition solution must use the same license source. The license source is defined by the configuration setting **System Settings** > **Licenses** > **Server Menu** > **Manage Licenses** > **License Source**. Use this procedure to set all nodes to use the same license source.

Procedure

1. Log in to Web Manager.
2. Click **Solution** > **Configure** > **Set All Nodes License Source**
3. In the Select License Source window, select either
   - **Local/Primary Server** for nodal licensing.
   - **WebLM** for centralized licensing.

   All nodes in the solution are set to the same license source.

Related links

Procedures for Applying Licensing on page 492

Uploading a PLDS License File to IP Office

Use this procedure to upload a PLDS license file for nodal license management. Nodal license management is used for standalone IP500 V2 systems and is an option for Server Edition systems.

Before you begin

The PLDS license file must be on the local machine where IP Office Web Manager is running

Procedure

1. In IP Office Web Manager, select **System Settings** > **Licenses** > **Server Menu** > **Manage Licenses**.

2. Click **PLDS Licenses** and select **Send To IP Office** and then click **OK**.
3. In the Select PLDS License File window, click **Browse** and navigate to the license file.
4. Select the file and click **OK**.

Related links

Procedures for Applying Licensing on page 492

Configuring Server Edition Nodal Licensing

With nodal licensing, licenses are managed using license files installed on each node in the system. For information on license distribution, see Distributing Nodal Licenses on page 489.

Procedure

1. In IP Office Web Manager, select **System Settings** > **Licenses**. Click on the **Server Menu** to the right of the Primary Server and then on the License Configuration page, select **Remote Server**.
2. In the **Licence Source** field, select **Primary**.

   Note:

   All systems in the Server Edition solution must use the same **License Source**. In Manager, on the Solution page, you can select **Set All Nodes License Source** to configure the setting for all nodes in the solution.
3. Enter the Server Edition Primary server IP address in the **License Server IP Address** field.
4. Under **Reserved Licenses**, the right hand column indicates which licenses have been reserved for this system. Use the left hand column to request additional licenses for this system.
5. Click **OK**.

   Licenses are displayed in the table.
6. Repeat steps 1 to 5 for the Server Edition Secondary server and all Server Edition Expansion Systems.

Related links

Procedures for Applying Licensing on page 492

Configuring Server Edition Centralized Licensing

With centralized licensing, licenses are managed from a central WebLM server.

Before you begin

You must have a PLDS license file activated with the host ID of the WebLM server

Procedure

1. In IP Office Web Manager, select **System Settings** > **Licenses**. Click on the **Server Menu** to the right of the Primary Server and then on the License Configuration page, select **Remote Server**.
2. Ensure **Licence Source** is set to **WebLM**.

   Note:

   All systems in the Server Edition solution must use the same **License Source**. In Manager, on the Solution page, you can select **Set All Nodes License Source** to configure the setting for all nodes in the solution.
3. The WebLM server can be located on the Server Edition Primary server or on a separate server. Enter the domain name or IP address of the WebLM server in the **Domain Name (URL)** field.

   Note that the domain name URL must use `https://`.
4. If required, change the path to the WebLM server in the **Path** field.
5. Under **Reserved Licenses**, the right hand column indicates which licenses will be automatically requested from the WebLM server. Use the left hand column to request additional license types for this system.
6. Navigate to the **Remote Server** page for the Server Edition Secondary server.
7. Ensure the **Licence Source** is set to **WebLM**.
8. You can choose to enable the **Enable proxy via Primary IP Office line** check box.

Choice Option	Choice Description
Enabled	The WebLM request is sent to the WebLM server via the IP Office line configured to the Server Edition Primary server. The line must be up and in service
Disabled	The WebLM request is sent directly to the WebLM server.

9. If **Enable proxy via Primary IP Office line** is enabled, enter the Server Edition Primary server IP address in the **Primary IP Address** field.
10. If **Enable proxy via Primary IP Office line** is disabled:
    a. Enter the domain name or IP address of the WebLM server in the **Domain Name (URL)** field.
    b. If required, change the path to the WebLM server in the **Path** field.
    c. If required change the default **Port Number**.

       For information on port usage see the IP Office Port Matrix document on the Avaya support site at https://support.avaya.com/helpcenter/getGenericDetails?detailId=C201082074362003.
11. Click **OK**.

    Licenses are displayed in the **License | License** table.

12. Repeat steps 8 to 12 for all Server Edition Expansion Systems.

    Note:

    In Manager, on the Solution page, you can select **Set All Nodes License Source**.

Related links

Procedures for Applying Licensing on page 492

Configuring the License Server in an Enterprise Branch Deployment

Use this procedure to configure WebLM centralized licensing where a shared PLDS license file is installed on the WebLM server. This is the recommended method for installing license files on IP Office systems that are centrally managed by System Manager.

For a complete description of deploying Enterprise Branch, see *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

Procedure

1. Log in to Web Manager and select **License | Remote ServerSystem Settings** > **Licenses** > **Systems** > **Remote Server**.
2. Select the **Enable Remote Server** check box.

   The **Reserved Licenses** information is displayed.
3. In the **Domain Name (URL)**, field, enter the domain name or IP address of the WebLM server or the domain name of System Manager if the system is under System Manager control.
4. **(Optional)** If a secondary System Manager is configured, enter the domain name in the **Secondary Domain Name (URL)** field.
5. If required, change the path to the WebLM server in the **Path** field.
6. If required change the default **Port Number**.

   For information on port usage see the IP Office Port Matrix document on the Avaya support site at https://support.avaya.com/helpcenter/getGenericDetails?detailId=C201082074362003.
7. Under **Reserved Licenses**, the right hand column indicates which licenses will be automatically requested from the WebLM server. Use the left hand column to request additional licenses for this system.

Related links

Procedures for Applying Licensing on page 492

Converting from Nodal to Centralized Licensing

If you are upgrading from an earlier release, perform the procedure Migrating Licenses to PLDS on page 499.

Note:

When upgrading from a previous release, all system must be running the same software level. The IP Office Server Edition Solution does not support mixed versioning.

Procedure

1. You must generate a license file using the WebLM host ID. Perform the following steps to find the WebLM host ID.
   a. In Web Manager, select **Applications** > **Web License Manager**.
   b. Log in to WebLM.
   c. In the navigation pane on the left, click **Server Properties**.

      The Server Properties page displays the Host ID. The host ID is the MAC address of the Server Edition Primary server.

      Record the host ID.
2. Generate a PLDS license file using the WebLM host ID.
3. Upload the license file.
   a. In Web Manager, select **ApplicationsWeb License Manager**.
   b. In the navigation pane on the left, click **Install license**.
   c. Click **Browse** to select the license file.
   d. Click **Install** to install the license file.
4. All nodes in the solution must have the same license source. To configure centralized licensing, all nodes must have the **License Source** set to **WebLM**. You can use Manager to set all nodes to the same license source. On the Manager Solution page, on the right hand side, select **Set All Nodes License Source** and then select **WebLM**.
5. If you are performing this procedure after an upgrade, you must ensure that the **Domain Name (URL)** field is populated on the Server Edition Primary server.
   a. In Web Manager select **System Settings** > **Licenses** > **Server Menu** > **Remote Server** for the Server Edition Primary server.
   b. Ensure that the **Domain Name (URL)** field contains the domain name or IP address of the Server Edition Primary server.
6. Reallocate the licenses as required. See Distributing Centralized Licenses on page 490.

   Note that the previously install local licenses are listed as obsolete. You can use this list to determine which licenses to request from the WebLM server. Once licenses have been reallocated, you can delete the obsolete licenses.

Migrating Licenses to PLDS

IP Office release 10 and higher supports only the Product Licensing and Delivery System (PLDS) to manage license files. If you are upgrading from a previous release, you must migrate all of your pre-R10 licenses (ADI, PLDS, mix of ADI/PLDS, virtual) to R10 PLDS licenses. The license migration tool extracts all the licensing information from an IP Office system and saves it to a file. This file can then be used prepare a software upgrade quote in the Avaya One Source Configurator in order to obtain the required new PLDS R10 licenses.

For Server Edition deployments, the License Migration tool collects licensing information from every node in the solution.

Note:

- You must use the release 10 or higher Manager client to generate the license inventory file.

  You can install Manager before upgrading to release 10. See the procedure “Installing Manager” in *Administering Avaya IP Office™ Platform with Manager*.
- License migration is supported on all IP Office modes, release 6.0 and higher.
- The license migration tool can only be used with an online configuration. The **Tools** > **License Migration** option is disabled for offline configurations.
- The license migration tool is not available on UCM and Application servers. When you run the license migration tool on a Server Edition server, the tool collects licensing information from every node in the solution.
- The generated file can be read but must not be edited. License migration will fail if the file has been edited.

Before you begin

Ensure all licenses are loaded on the system before performing the license migration. For Server Edition deployments, ensure all nodes are online in order to capture the current view of systems in the solution.

The IP Office configuration must be opened online. The License Migration tool is not available in offline mode.

Procedure

1. Log in to Manager and select **Tools** > **License Migration**.

   The Save As window opens.
2. Select a location to save the file and enter a file name.
3. Click **Save**.

   The file is saved with a `.zip` extension.

Next steps

Use the file to prepare a software upgrade quote in the Avaya One Source Configurator in order to obtain the required new PLDS R10 licenses. Once you have the PLDS license files, apply them to the system.

Certificate Management

Related links

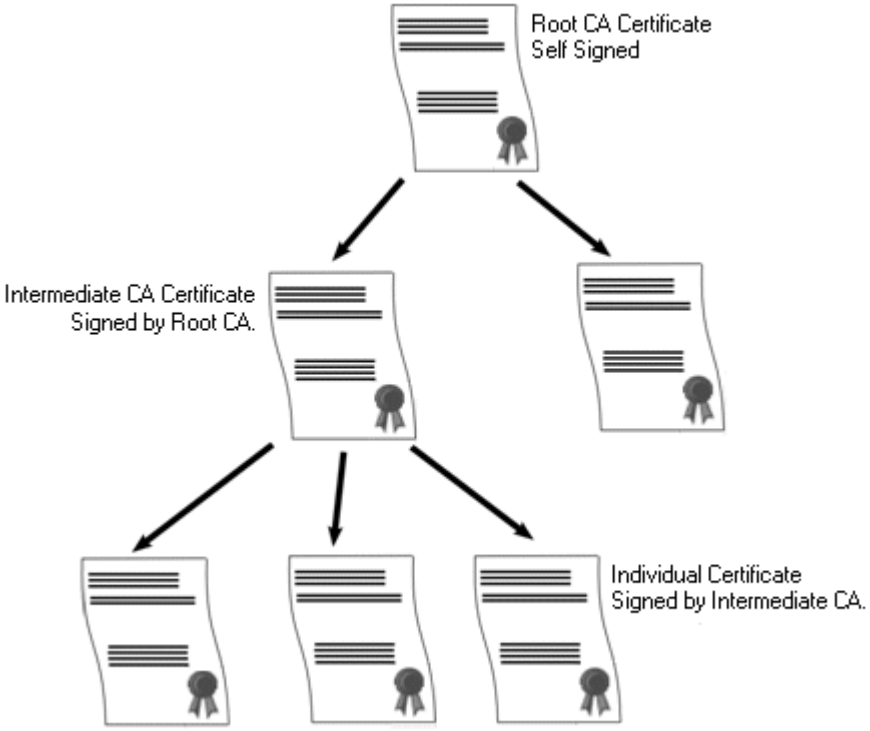
Certificate Overview on page 500
Certificate Support on page 505

Certificate Overview

Public key cryptography is one of the ways to maintain a trustworthy networking environment. A public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

The system used to provide public-key encryption and digital signature services is called a public key infrastructure (PKI). All users of a PKI should have a registered identity which is stored in a digital format and called an Identity Certificate. Certificate Authorities are the people, processes and tools that create these digital identities and bind user names to public keys.

There are two types of certificate authorities (CAs), root CAs and intermediate CAs. In order for a certificate to be trusted and for a secure connection to be established, that certificate must have been issued by a CA that is included in the trusted certificate store of the device that is connecting. If the certificate was not issued by a trusted CA, the connecting device then checks to see if the certificate of the issuing CA was issued by a trusted CA, and so on until either a trusted CA is found. The trusted certificate store of each device in the PKI must contain the required certificate chains for validation.



IP Office Root Certificate Authority

IP Office generates a self-signed certificate. For IP500 V2 systems, a certificate is generated automatically on the first start up. On Linux systems, a certificate is generated during the ignition process.

The following entities can act as the certificate authority.

- The Server Edition Primary Server, an Application Server, or a Unified Communication Module (UCM) can act as the root certificate authority for all nodes in the system.
- In Enterprise Branch deployments, the System Manager can act as the root certificate authority.
- Identity certificates can also be purchased and issued by a third party certificate authority.

Regardless of the method used to provide the IP Office identity, the certificate authority which signs the IP Office identity certificate must be trusted by all the clients and endpoints that need to establish a secure connection with IP Office. They must be a part of the PKI. Therefore, the root CA certificate must be downloaded to client devices and placed in the trusted certificate store. If there are intermediate CAs in the certificate chain, either the intermediate CAs must be added to the client device Trusted Certificate Store or the certificate chain must be advertised by IP Office in the initial TLS exchange.

Certificates and TLS

Telephony signaling like SIP messaging is secured using Transport Layer Security (TLS). TLS provides communication security using certificates to authenticate the other end of the IP Link.

The message exchange in TLS is aimed at verifying the identity of the communicating parties and establishing the keys that will be used to encrypt the signaling data between the two parties.

Typically, the server sends its identity certificate, either self-signed or signed by the CA, to the client. The client must have the CA certificate in its trusted certificate store.

IP Office acts as the TLS server in its interactions with SIP telephony clients. This means that the TLS application on the IP Office must be configured to listen for client connections by enabling TLS in the SIP Registrar on the LAN1 and LAN2 interfaces.

Note:

- Authentication of the client's certificate by the server is not a requirement. IP Office does not support client certificate validation for all SIP endpoint types.
- The E.129 phone does not validate the IP Office identity certificate.

Related links

Certificate Management on page 500
Windows Certificate Store on page 502

Windows Certificate Store

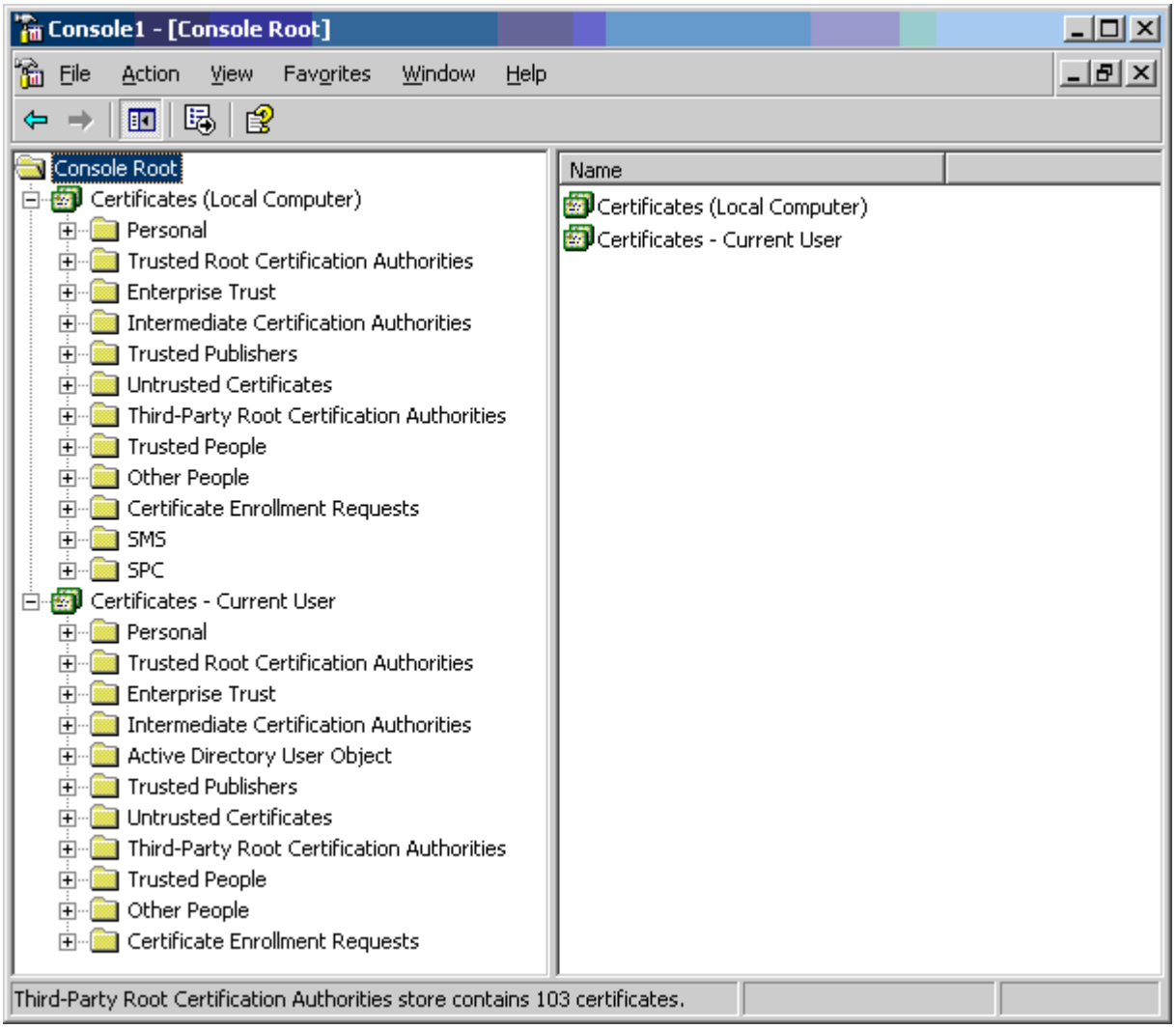
The certificate store used by Manager to save and retrieve X509 certificates is the default one provided by the Windows operating system. The Windows certificate store is relevant to any application running on Windows that uses certificates for security, either TLS or HTTPS. For example, the Avaya Communicator Client.

Warning:

Avaya accepts no responsibility for changes made by users to the Windows operating system. Users are responsible for ensuring that they have read all relevant documentation and are sufficiently trained for the task being performed.

Windows Certificate Store Organization

By default, certificates are stored in the following structure:



Each of the sub folders has differing usage. The Certificates - Current User area changes with the currently logged-in windows user. The Certificate (Local Computer) area does not change with the currently logged-in windows user.

Manager only accesses some of the certificate sub folder:

Certificates (Local Computer) Folder	Manager Use
Personal | Certificates	Folder searched by Manager 1st for matching certificate to send to the system when requested. Certificate matched by the subject name contained in **File | Preferences | Security | Certificate** offered to the system. Folder accessed whenever **'Local Machine certificate store'** used for Security Settings. Folder searched by Manager for matching certificate when certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.
Trusted Root Certification Authorities | Certificates	Folder searched by Manager for matching parent certificates when non-self signed certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.

Certificates – Current User Folder	Manager Use
Personal | Certificates	Folder searched by Manager 2nd for matching certificate (subject name) to send to the system when requested. Certificate matched by the subject name contained in **File | Preferences | Security | Certificate** offered to the system. Folder accessed whenever **'Current User certificate store'** used for Security Settings. Folder searched by Manager for matching certificate when certificate received from IP Office, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.
Trusted Root Certification Authorities | Certificates	Folder searched by Manager for matching parent certificates when non-self signed certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.
Other People | Certificates	Folder searched by Manager for matching parent certificates when non-self signed certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.

Windows Certificate Store Import

In order to use certificates – either for security settings or Manager operation – they must be present in the windows certificate store. Certificates may be placed in the store by the Certificate Import Wizard. The Certificate Import Wizard can be used whenever a certificate is viewed. In

order for Manager to subsequently access this certificate the **Place all certificate in the following store** option must be selected:

- If the certificate is to subsequently identify the system, the Other People folder should be used.
- If the certificate is to subsequently identify the Manager, the Personal folder should be used, and the associated private key saved as well.

Certificate Store Export

Any certificate required outside of the Manager PC must be first saved in the Certificate store, then exported.

If the certificate is to be used for identity checking (i.e. to check the far entity of a link) the certificate alone is sufficient, and should be saved in PEM or DER format.

If the certificate is to be used for identification (i.e. to identify the near end of a link) the certificate and private key is required, and should be saved in PKCS#12 format, along with a password to access the resultant .pfx file.

Related links

Certificate Overview on page 500

Certificate Support

Related links

Certificate Management on page 500
Certificate File Naming and Format on page 505
Identity Certificate on page 506
Trusted Certificate Store on page 508
Signing Certificate on page 510
Certificate File Import on page 511

Certificate File Naming and Format

DER: Distinguished Encoding Rules (DER) format, which is a binary format used to represent a certificate. Typically used to describe just one certificate, and cannot include a private key.

There are four main encodings/internal formats for certificate files. Note that these are encodings, not file naming conventions.

PEM: Privacy Enhanced Mail (PEM) is a Base 64 (i.e. ASCII text) encoding of DER, one certificate is enclosed between '-----BEGIN CERTIFICATE-----' and '-----END CERTIFICATE-----' statements. Can contain a private key enclosed between '-----BEGIN PRIVATE KEY -----' and '-----END BEGIN PRIVATE KEY -----' statements. More than one certificate can be included. PEM can be identified by viewing the file in a text editor. This is an unsecure format and not recommended for private key use unless it is protected with a password.

PKCS#12: Public Key Cryptography Standard (PKCS) #12. A secure, binary format, encrypted with a password. Typically used to describe one certificate, and its associated private key, but can also include other certificates such as the signing certificate(s). This is the recommended format for private key use.

PKCS#7: A Base 64 (i.e. ASCII text) encoding defined by RFC 2315, one or more certificates are enclosed between '——BEGIN PKCS——' & '——END PKCS7——' statements. It can contain only Certificates & Chain certificates but not the private key. Can be identified by viewing the file in a text editor.

There are many common filename extensions in use:

- .CRT — Can be DER or PEM. Typical extension used by Unix/Android systems' public certificates files in DER format.
- .CER — Can be DER or PEM. Typical extension used by Microsoft/Java systems' public certificates files in PEM format.
- .PEM — Should only be PEM encoded.
- .DER — Should only be DER encoded.
- .p12 — Should only be in PKCS#12 format. Typical extension used by Unix/Android systems' identity certificates/private key pair files. Same format as .pfx hence can be simply renamed.
- .pfx — Should only be in PKCS#12 format. Typical extension used by Microsoft systems' identity certificates/private key pair files. Same format as .p12 hence can be simply renamed.
- .pb7 — Should only be in RFC 2315 format. Typical extension used by Microsoft and Java systems for certificate chains.

Related links

Certificate Support on page 505

Identity Certificate

Feature	Support	Notes
Import: Public key size	Yes	RSA 1024, 2048 and 4096 bit public keys must be supported. Any other sizes are optional. Import of RSA public key less than 1024 or greater than 4096 bits to be rejected with an informative error. Import of certificates with 1024 will be imported after a warning 'The certificate public key may not be of sufficient strength. Do you wish to continue?'
Import: Certificate signature algorithm	Yes	SHA-1, SHA-256 SHA-384, and SHA-512 hashing algorithms must be supported. Any other SHA2 algorithms are optional. Import of certificates with SHA-1 will be imported after a warning 'The certificate signature algorithm may not be of sufficient strength. Do you wish to continue?' Import of certificates with other algorithms (for example MD5, ECC) to be rejected with an informative error.
Import: Must have private key	Yes	Must be supplied. Reject and informative error that private key has not been supplied

Table continues…

Feature	Support	Notes
Import: Certificate checks	Yes	Minimum checks for: • Version (v3) • Start + end (present) • Subject Name (present) • Issuer Name (present) • Data integrity (e.g. hash) Reject + informative error if a check fails
Import: Certificate up to 4KB	Yes	Certificates can be varying sizes
Import: Formats	Yes	• PKCS#12 format. '.p12' and '.pfx' file extension. With or without password. This shall be the preferred/default option • PEM format. '.cer' '.pem' and '.crt' file extension. • Pasted from clipboard in PEM format (optional) NOTE that ONLY PKCS#12 file format is acceptable according to 147434–030–P1, however we cannot control what format customers receive their certificates in, hence all should be supported See section below for certificate file import support
Import: Up to 4 other certificates in same file	Yes	Only supported where management of TCS also available. • Any intermediate and root CA certificate included in the PKCS#12 file to be imported into the Trusted Certificate store • The feature is intended for import of intermediate certificates, but can include unrelated certificates. • An informative message to the admin if any have been imported
Import: Certificate chain support	Yes	Where identity certificate is signed by one or more intermediate CAs, search TCS for matching certificates and include in identity certificate chain.

Table continues…

Feature	Support	Notes
View: Certificate Contents	Yes	Minimum viewable attributes (From CEC016: 147434–030–P1): • Serial Number • Subject Name • Issuer Name • Validity Period (that includes notBefore and notAfter dates) • Thumbprint (Hash of the certificate) • Subject Alternative Names • Key Usage Extensions • Extended Key Usage Warnings/errors as per 147434–080–P1: • Error displayed that certificate has expired • Warning displayed that certificate is nearing expiry (within 60 days).
View: Private Key	No	Private key must not be viewable
Export: Formats	Yes	Private key must not be exportable Export formats: • DER format. '.cer' '.der' and '.crt' file extension. • PEM format. '.cer' '.pem' and '.crt' file extension. • PKCS#12 (optional)

Related links

Certificate Support on page 505

Trusted Certificate Store

Feature	Support	Notes
Import: RSA 1024-4096 key size	Yes	RSA 1024, 2048 and 4096 bit public keys must be supported. Any other sizes are optional. Import of RSA public key less than 1024 or greater than 4096 bits to be rejected with an informative error.
Import: Optional private key	Yes	No private key will actually be imported. Informative message (neither warning or error) that private key has not been imported

Table continues…

Feature	Support	Notes
Import: Certificate checks	Yes	Minimum checks for: • Version (v3) • Start + end (present) • Subject Name (present) • Issuer Name (present) • Data integrity (e.g. hash) Reject + descriptive error if a check fails
Import: Certificate up to 4KB	Yes	Certificates can be varying sizes
Import: Formats	Yes	• DER format. '.cer' '.der' and '.crt' file extension. • PEM format. '.cer' '.pem' and '.crt' file extension. • PKCS#12 format. '.p12' and '.pfx' file extension. With or without password. • Pasted from clipboard in PEM format (optional)
Import: Up to 19 other certificates in same file	Yes	All included certificates, up to 20 total. More than 20 in one file can be optionally supported.
View: TCS Certificate	Yes	Minimum viewable attributes (From CEC016: 147434–030–P1): • Serial Number • Subject Name • Issuer Name • Validity Period (that includes notBefore and notAfter dates) • Thumbprint (Hash of the certificate) • Subject Alternative Names • Key Usage Extensions • Extended Key Usage Warnings/errors as per 147434–080–P1: • Error displayed that a certificate has expired • Warning displayed that a certificate is nearing expiry (within 60 days).
Export: Formats	Yes	Export formats: • DER format. '.cer' '.der' and '.crt' file extension. • PEM format. '.cer' '.pem' and '.crt' file extension. • PKCS#12 (optional)

Related links

Certificate Support on page 505

Signing Certificate

Feature	Support	Notes
Import: RSA 1024-4096 key size	Yes	RSA 1024, 2048 and 4096 bit public keys must be supported. Any other sizes are optional. Import of RSA public key less than 1024 or greater than 4096 bits to be rejected with an informative error.
Import: Must have private key	Yes	Must be supplied. Reject and informative error that private key has not been supplied
Import: Certificate checks	Yes	Minimum checks for: • Version (v3) • Start + end (present) • Subject Name (present) • Issuer Name (present) • Data integrity (e.g. hash) Reject and informative error if a check fails
Import: Certificate up to 4KB	Yes	Certificates can be varying sizes
Import: Formats	Yes	• PKCS#12 format. '.p12' and '.pfx' file extension. With or without password. This shall be the preferred/default option • PEM format. '.cer' '.pem' and '.crt' file extension. • Pasted from clipboard in PEM format (optional) NOTE that ONLY PKCS#12 file format is acceptable according to 147434–030–P1, however we cannot control what format customers receive their certificates in, hence all should be supported
Import: Other certificates in same file	No	Informative warning that other certificates have not been imported

Table continues…

Feature	Support	Notes
View: TCS Certificate	Yes	Minimum viewable attributes (From CEC016: 147434–030–P1): • Serial Number • Subject Name • Issuer Name • Validity Period (that includes notBefore and notAfter dates) • Thumbprint (Hash of the certificate) • Subject Alternative Names • Key Usage Extensions • Extended Key Usage Warnings/errors as per 147434–080–P1: • Error displayed that certificate has expired • Warning displayed that certificate is nearing expiry (within 60 days).
Renew existing:	Yes	Regenerate CA keeping all keys and other contents same except: • notBefore and notAfter dates • Serial Number • Thumbprint (Hash of the certificate) • ?? Can this be done to imported CAs or just internally generated ones?
Create new:	Yes	Regenerate CA, including keys
Export: Formats	Yes	Private key must not be exportable Export formats: • DER format. '.cer' '.der' and '.crt' file extension. • PEM format. '.cer' '.pem' and '.crt' file extension. • PKCS#12 (optional)

Related links

Certificate Support on page 505

Certificate File Import

File Content	Identity Certificate Import Command	Trusted Certificate Import Command	Signing Certificate Import Command	Notes
DER				

Table continues…

File Content	Identity Certificate Import Command	Trusted Certificate Import Command	Signing Certificate Import Command	Notes
DER: 1 certificate	No – attempt rejected with 'Invalid certificate format (DER)'	Yes – attempt accepted with 'N certificate(s) imported into Trusted Certificate Store'	No – attempt rejected with 'Invalid certificate format (DER)'	
DER: Any other content	No – attempt rejected with 'Invalid content (DER)'	No – attempt rejected with 'Invalid content (DER)'	No – attempt rejected with 'Invalid content (DER)'	
PKCS#12				
PKCS#12: 1 certificate + private key	Yes – attempt accepted with 'Certificate import successful' Certificate/key imported as ID certificate	No – p12/pfx should not be offered for file selection	Yes – attempt accepted with 'Certificate import successful'	
PKCS#12: 1 certificate + private key, 1 or more other certificates	Yes – attempt accepted with 'Certificate import successful' Certificate/key imported as ID certificate Other certificates imported into TCS with 'N certificate(s) imported into Trusted Certificate Store'	No – p12/pfx should not be offered for file selection	Yes – attempt accepted with 'Certificate import successful' Certificate/key imported as signing certificate Other certificates ignored	At least 20 certificates supported in the same file
PKCS#12: Any other content	No – attempt rejected with 'Invalid content (PKCS#12)'	No – p12/pfx should not be offered for file selection	No – attempt rejected with 'Invalid content (PKCS#12)'	
PEM: 1 Certificate	No – attempt rejected with 'Invalid certificate format (PEM – no private key)'	Yes – attempt accepted with 'N certificate(s) imported into Trusted Certificate Store'	No – attempt rejected with 'Invalid certificate format (PEM – no private key)'	Certificate can be encrypted on unencrypted
PEM				

Table continues…

File Content	Identity Certificate Import Command	Trusted Certificate Import Command	Signing Certificate Import Command	Notes
PEM: N Certificate	No – attempt rejected with 'Invalid certificate format (PEM – no private key)'	Yes – attempt accepted with 'N certificate(s) imported into Trusted Certificate Store'	No – attempt rejected with 'Invalid certificate format (PEM – no private key)'	At least 20 certificates supported in the same file Certificate can be encrypted on unencrypted
PEM: 1 Certificate + private key	Yes – attempt accepted with 'Certificate import successful' Certificate/key imported as ID certificate	No – attempt rejected with 'Invalid certificate format (PEM)'	Yes – attempt accepted with 'Certificate import successful' Certificate/key imported as signing certificate	Certificate or Key can be encrypted on unencrypted
PEM: 1 Certificate + private key, 1 or more other certificates. Private key must be before or after the first certificate	Yes – attempt accepted with 'Certificate import successful' Certificate/key imported as ID certificate. Other certificates imported into TCS with 'N certificate(s) imported into Trusted Certificate Store'	Yes – attempt accepted with 'N certificate(s) imported into Trusted Certificate Store' First certificate and private key ignored	Yes – attempt accepted with 'Certificate import successful' Certificate/key imported as signing certificate Other certificates ignored	Private key must be before or after the first certificate Certificate or Key can be encrypted on unencrypted
PEM: Any other content	No – attempt rejected with 'Invalid content (PEM)'	No – attempt rejected with 'Invalid content (PEM)'	No – attempt rejected with 'Invalid content (PEM)'	Option to include more detail of the rejection cause.e.g. 'Cannot detect Identity Certificate', 'Too many private keys', 'Unrecognized header' etc.

Related links

Certificate Support on page 505

On-boarding

On-boarding refers to the configuration of an SSL VPN service in order to enable remote management services to customers, such as fault management, monitoring, and administration. You must use the Web Manager client to configure on-boarding.

For full details on how to configure and administer SSL VPN services, refer to *Deploying Avaya IP Office™ Platform SSL VPN Services*.

The procedure provided below configures IP Office for Avaya support services. Avaya partners can also use an SSL VPN to provide support services. See the chapter “Configuring an Avaya Partner SSL VPN using an SDK” in *Deploying Avaya IP Office™ Platform SSL VPN Services*.

Related links

Configuring an SSL VPN using an on-boarding file on page 514

Configuring an SSL VPN using an on-boarding file

The on-boarding XML file is available from Avaya. It contains the settings required to establish a secure tunnel between IP Office and an AVG server. When you import the on-boarding XML file, it applies the settings and installs one or multiple TLS certificates.

When you configure the SSL VPN service on a new system, you must begin by generating an inventory file of the IP Office system. When you register your IP Office system, the inventory file that you generated is uploaded to the GRT and the inventory data is populated in the Avaya Customer Support (ACS) database. After you enable remote support, you can download the XML on-boarding file from the GRT web site and upload it into your IP Office system.

The on-boarding process configures:

- SSL VPN service configuration
- short codes for enabling and disabling the SSL VPN service
- SNMP alarm traps
- one or more TLS certificates in the IP Office trusted certificate store

Perform this procedure using the Avaya IP Office Web Manager client.

Warning:

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

Before you begin

Before you begin, you must have the hardware codes and catalog description of your IP Office system. For example, “IP OFFICE 500 VERSION 2 CONTROL UNIT TAA” is a hardware code and catalog description.

Procedure

1. Select **Tools > On-boarding**.

   The On-boarding dialog box displays.

2. If the hardware code for your IP Office system ends with the letters TAA, select the checkbox next to the prompt **Are you using TAA series hardware?**
3. Click **Get Inventory File** to generate an inventory of your IP Office system.
4. Click **Register IP Office**.

   A browser opens and navigates to the GRT web site.

5. Log in to the web site and enter the required data for the IP Office system.
6. Select **Remote Support** for the IP Office system.
7. Click **Download** and save the on-boarding file.
8. Browse to the location where you saved the on-boarding file and click **Upload**.

   A message displays to confirm that the on-boarding file has installed successfully.

Related links

On-boarding on page 514

System Date and Time

For files stored on memory cards the system uses the UTC time. For other activities such as call logs, SMDR records, time display on phones; the local time (UTC + any offsets) is used.

For Linux based servers, the SNTP time source is set through the server's Platform View menus (**Settings | System | Data and Time**). Typically the primary server in a network is set to a know reliable external SNTP source and all other servers are set to use SNTP from the primary server.

For IP500 V2 servers, the time can be set in a number of ways, manual, NTP or SNTP, set through the**Time Setting Config Source** settings on the **System Settings** > **System** > **System** form. The control unit contains a battery backed clock which is used to maintain system time during normal operation and when mains power is removed.

Manually Setting the System Time

The use of automatic time requests can be disabled by setting the time source to None. In that case the time and date used by the system is set manually using a phone configured with System Phone Rights. In both cases the user's login code, if set, is used to restrict access to the time and date settings.

- **1400, 1600, 9500 and 9600 Series Phones** Phones in these series (excluding the 1403/1603 models) can set the system time and date when the extension user is configured with System Phone Rights. The user is able to access menu options to set the time, date and time offset by selecting **Features | Phone User | System Administration**. If automatic time

updates are being used, these controls only display the time and date received from the time source and do not allow it to be changed.

- **Other Phones** The following method is only supported on these phones: 2410, 2420, 4412, 4424, 4612, 4624, 4610, 4620, 4621, 5410, 5420, 5610, 5620, 5621, 6412, 6424. The phone needs to be configured with a **Self Admin 2** button.

Configuring Time Profiles

Time profiles are configured on **System Settings** > **Time Profiles**

Time Profiles are used by different services to change their operation when required. In most areas where time profiles can be used, not setting a time profile is taken as meaning 24-hour operation.

Time profiles consist of recurring weekly patterns of days and times when the time profile is in effect.

Time profiles can include time periods on specified calendar days when the time profile is in effect. Calendar records can be entered for the current and following calendar year.

For a Server Edition network, these settings can be configured at the network level and are then automatically replicated in the configuration of all systems in the network. They can only be seen and edited at the individual system configuration level if record consolidation is switched off.

Time profiles are used by the following record types.

Hunt Group:

A time profile can be used to determine when a hunt group is put into night service mode. Calls then go to an alternate Night Service Fallback group if set, otherwise to voicemail if available or busy tone if not.

Setting and clearing hunt group night service can be done using either manual controls or using a system time profile. The use of both methods to control the night service status of a particular hunt group is not supported.

For automatic voice recording, a time profile can be used to set when voice recording is used.

User:

- Users being used for Dial In data services such as RAS can have an associated time profile that defines when they can be used for that service.
- Users can be associated with a working hours and an out of hours user rights. A time profile can then be used to determine which user rights is used at any moment.
- For automatic voice recording, a time profile can be used to set when that voice recording is used.
- For mobile twinning, a time profile can be used to define when twinning should be used.

Incoming Call Route:

Incoming call routes can also use time profiles to specify when calls should be recorded. Multiple time profiles can be associate with an incoming call route, each profile specifying a destination and fall back destination.

ARS:

ARS forms use time profile to determine when the ARS form should be used or calls rerouted to an out of hours route.

Account Code:

Account Codes can use automatic voice recording triggered by calls with particular account codes. A time profile can be used to set when this function is used.

Auto Attendant :

Embedded voicemail auto attendants can use time profiles to control the different greetings played to callers.

Service:

- A Service can use time profiles in the following ways:
- A time profile can be used to set when a data service is available. Outside its time profile, the service is either not available or uses an alternate fallback service if set.
- For services using auto connect, a time profile can be used to set when that function is used. See Service | Autoconnect.

Related links

Overriding a Time Profile on page 517

Overriding a Time Profile

You can use the **System Settings** > **Time Profiles** > **Add/Edit Time Profile** > **Manual Override** setting to manually override a time profile. The override settings allow you to mix timed and manual settings.

The override options are as follows:

- **Set Time Profile Active Until Next Timed Inactive**

  Use for time profiles with multiple intervals. Make the time profile active until the next inactive interval.

- **Set Time Profile Inactive Until Next Timed Active**

  Use for time profiles with multiple intervals. Make the time profile inactive until the next active interval.

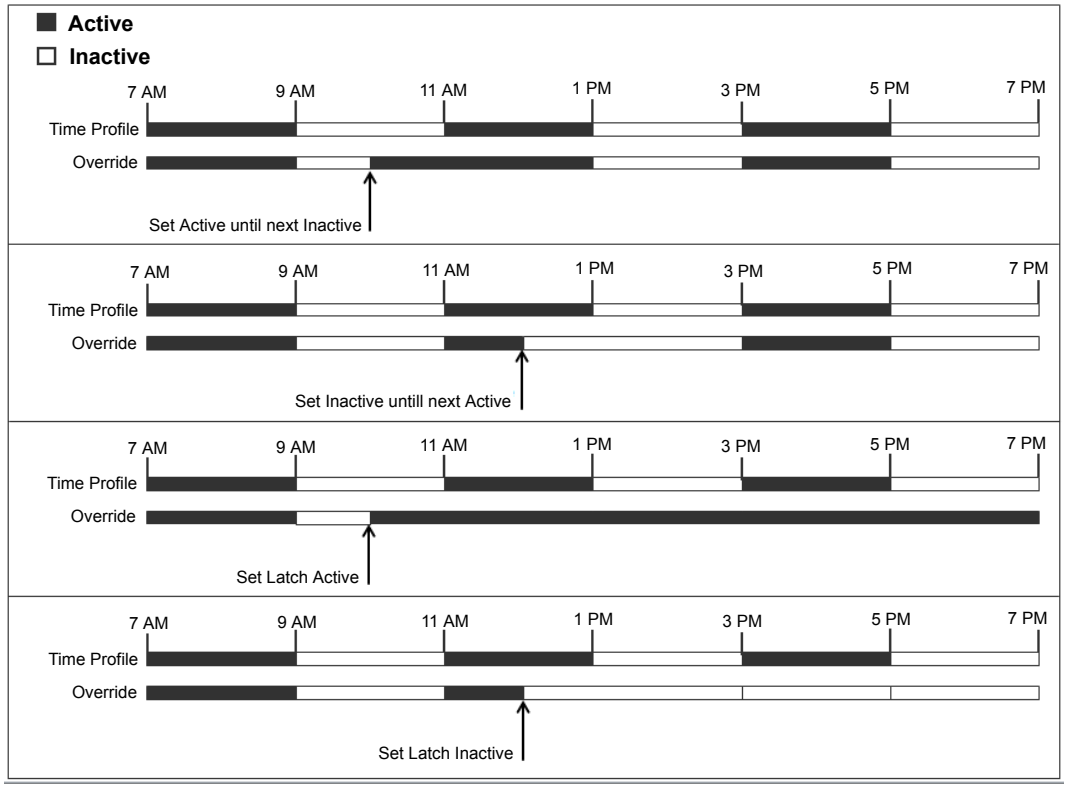
- **Set Time Profile Latch Active**

  Set the time profile to active. Timed inactive periods are overridden and remain active.

- **Set Time Profile Latch Inactive**

  Set the time profile to inactive. Timed active periods are overridden and remain active.

The illustration below provides an example of each override setting.



A time profile can be overridden using the following methods.

- Using the **Override** settings on the Time Profile configuration page.
- Configure short codes for the time profile. See the description for the “Set Time Profile” short code.
- Configure the Time Profile button action for the time profile. See the description for the “Time Profile” button action.

Related links

Configuring Time Profiles on page 516

Working with Templates

IP Office supports a number of template options. The settings for the following types of configuration items can be saved as template files. New records of those types can then be created from the template file.

- User (.usr)
- Extension (H.323, SIP, IP DECT) (.ext)

- Group (.grp)
- Service (.ser)
- Tunnel (.tnlt)
- Firewall Profile (.fpr)
- Time Profile (.tpr)
- IP Route (.ipr)
- ARS (.ars)
- Line (H.323, SIP, IP DECT) (.lne)

Saving Template files

Standard Mode Systems: Standard mode systems export templates to a local folder on the PC where Manager is running. Templates are stored in the default folder `C:\Program Files (x86)\Avaya\IP Office\Manager\manager_files\template`.

Server Edition Systems: Server Edition system templates are stored on the Primary Server. When the system configuration is opened, those templates are downloaded from server to the default folder above. When the configuration is saved, the templates are uploaded back to server.

Caution:

Due to the difference in operation detailed above, any non-Server Edition templates stored in the default folder, are liable to be overwritten when a Server Edition configuration is loaded. Therefore, if you administer both Server Edition and non-Server Edition system, you need to ensure that you store the non-Server Edition templates in a directory other than the default directory.

For Server Edition, if you are working with an offline configuration, any templates created are deleted after you close Manager.

Tested SIP Trunk Templates

The SIP trunk services from selected SIP providers are tested as part of the Avaya DevConnect program. The results of such testing are published as Avaya Application Notes available from the Avaya DevConnect web site (https://devconnect.avaya.com).

Related links

Creating a Template in Manager on page 519
Creating an Analog Trunk Template in Manager on page 520
Creating a New Analog Trunk from a Template in Manager on page 520

Creating a Template in Manager

You can create a template from an existing record.

The options **New From Template** and **Export as Template** are available by:

- right clicking on the record type in the Navigation pane
- right clicking on a record in the Group pane

- using the Details Toolbar in the Details pane

This procedure uses the Group Pane.

Procedure

1. In the Navigation pane, select a record type.
2. In the Group pane, right click on the record on which you want to base your template and select **Export as Template**.
3. The **Save As** window opens at the default template folder. Enter a name for the template.

   A default extension is applied. For example, user templates are saved with the file extension `.usr` and extension templates are saved with file extension `.ext`.
4. Click **Save**.

   You can now create new records using the template.

Related links

Working with Templates on page 518

Creating an Analog Trunk Template in Manager

You can create an analog trunk template from an existing trunk..

Procedure

1. In the Navigation pane, select **Line**.
2. In the Group pane, right click on the record on which you want to base your template and select **Generate Analog Trunk Template**.
3. In the Analog Trunk Template window, you can adjust the settings if required. Click **Export**.
4. In the Template Type Selection window, select the **Service Provider** and then click **Create Template**.
5. In the Browse for Folder window, select `Program Files\Avaya\IP Office\Manager \manager_files\template`.
6. Click **OK**.

Related links

Working with Templates on page 518

Creating a New Analog Trunk from a Template in Manager

You can create a new analog trunk from a template.

Procedure

1. In the Navigation pane, right click **Line** and select **New from Template** > **Open**.
2. In the Open window, select a template and click **Open**.
3. In the Template Type Selection window, select the **Service Provider** and then click **Create**.

Related links

Working with Templates on page 518

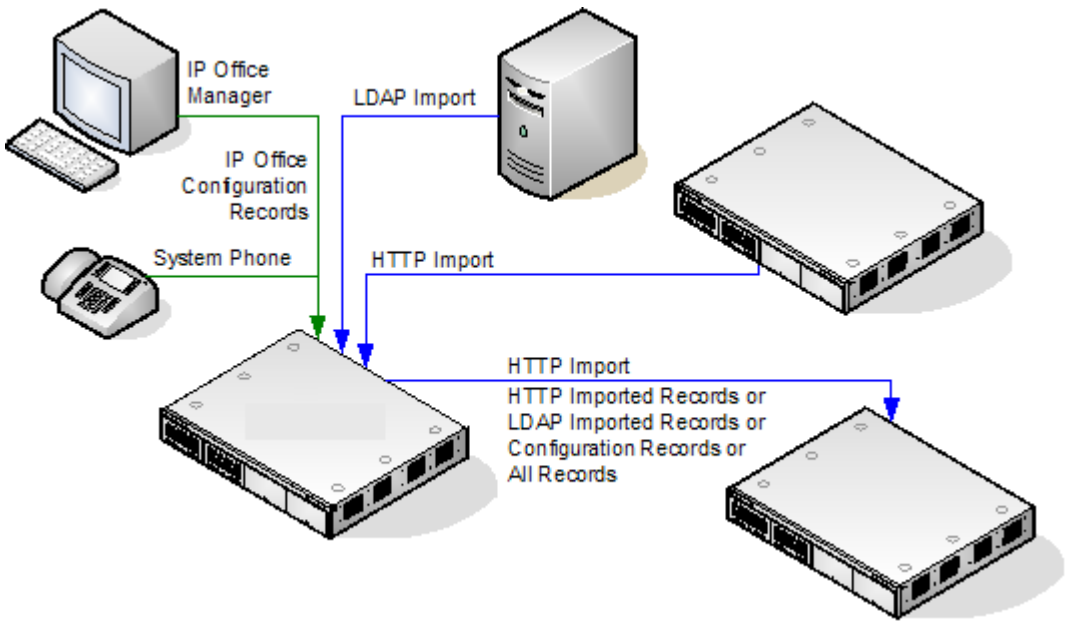
Centralized System Directory

Directory services can be used to import directory records (names and numbers) from external sources. These sets of records are regularly re-imported.

Directory records can come from the following sources:

- **LDAP Import**: The system can import LDAP records for use within directories shown by user phones and applications. LDAP import is configured through the **System Settings** > **System** > **Directory Services** > **LDAP** form. The LDAP used is LDAP Version 2.
- **HTTP Import** : Systems are able to import the directory records from another system using HTTP. HTTP import is configured through the **System Settings** > **System** > **Directory Services** > **HTTP** form by specifying an IP address or multi-site network connection. The records imported can be any or all of the following record types held by the system from which the records are being imported: LDAP imported records, HTTP imported records, configuration records.
- **System Directory Records (Configuration records)**: Records can be entered directly into the system configuration through the **System Settings** > **System Directory** > **Add/Edit Directory Entry** form. System directory records override matching LDAP/HTTP imported records.

  Phones with a **CONTACTS** button and System Phone Rights privileges, can add, delete and edit the system directory records of the system at which they are logged in. They cannot edit LDAP or HTTP imported records.



Server Edition Directory Operation

For a Server Edition network, these settings can only be configured at the network level and they are stored in the configuration of the Primary Server. All other systems in the network are configured to share the directory settings of the Primary Server through the settings at **System Settings** > **System** > **Directory Services** > **HTTP**.

Directory Record Capacity

The directory capacity depends on the type of system. The figures below are applicable for Release 10.0. When using a 1400, 1600, 9500 or 9600 Series phone, system phone users can also edit the configuration directory records.

	System	Number of Directory Records			Total Number of Directory Records
		Configuration	LDAP Import	HTTP Import	
Standalone Systems	**IP500 V2**	2,500	10,000	10,000	10,000
Server Edition	**Primary Server**	10,000	10,000	10,000	10,000
	Secondary Server	–	–	10,000	10,000
	Expansion System (L)	–	–	10,000	10,000
	Expansion System (V2)	–	–	10,000	10,000

Use of Directory Records

Directory records are used for two types of functions, directory dialing and caller name matching.

Directory Dialing:

Directory numbers are displayed by user applications such as SoftConsole. Directory numbers are viewable through the Dir function on many Avaya phones (**Contacts** or **History**). They allow the user to select the number to dial by name. The directory will also contain the names and numbers of users and hunt groups on the system.

The **Dir** function groups directory records shown to the phone user into the following categories. Depending on the phone, the user may be able to select the category currently displayed. In some scenarios, the categories displayed may be limited to those supported for the function being performed by the user:

- **External**: Directory records from the system configuration. This includes HTTP and LDAP imported records.
- **Groups**: Groups on the system. If the system is in a multi-site network, it will also include groups on other systems in the network.
- **Users** or **Index**: Users on the system. If the system is in a multi-site network it will also include users on other systems in the network.
- **Personal**: Available on T3, T3 IP, 1400, 1600, 9500 and 9600 Series phones. These are the user's personal directory records stored within the system configuration.

Speed Dialing: On M-Series and T-Series phones, a Speed Dial button or dialing **Feature 0** can be used to access personal directory records with an index number.

- **Personal**: Dial **Feature 0** followed by ***** and the 2-digit index number in the range 01 to 99.
- **System**: Dial **Feature 0** followed by 3-digit index number in the range 001 to 999.
- The Speed Dial short code feature can also be used to access a directory speed dial using its index number from any type of phone.

Caller Name Matching:

Directory records are also used to associate a name with the dialled number on outgoing calls or the received CLI on incoming calls. When name matching is being done, a match in the user's personal directory overrides any match in the system directory. Note that some user applications also have their own user directory.

- SoftConsole applications have their own user directories which are also used by the applications name matching. Matches in the application directory may lead to the application displaying a different name from that shown on the phone.
- Name matching is not performed when a name is supplied with the incoming call, for example QSIG trunks. On SIP trunks the use of the name matching or the name supplied by the trunk can be selected using the **Default Name Priority** setting (**System | Telephony | Telephony**). This setting can also be adjusted on individual SIP lines to override the system setting.
- Directory name matching is not supported for DECT handsets. For information on directory integration, see *IP Office DECT R4 Installation*.

Directory Special Characters

The following characters are supported in directory records. They are supported in both system configuration records and in imported records.

- **? = Any Digit** Directory records containing a **?** are only used for name matching against the dialed or received digits on outgoing or incoming. They are not included in the directory of

numbers to dial available to users through their phones or applications. The wildcard can be used in any position but typically would be used at the end of the number.

In the following example, any calls where the dialed or received number is 10 digits long and starts 732555 will have the display name Homdel associated with them.

- **Name**: Holmdel
- **Number**: 9732555????

- **(and) brackets = Optional Digits** These brackets are frequently used to enclose an optional portion of a number, typically the area code. Only one pair of brackets are supported in a number. Records containing digits inside ( ) brackets are used for both name matching or user dialling. When used for name matching, the dialed or received digits are compared to the directory number with and without the ( ) enclosed digits. When used for dialling from a phone or application directory, the full string is dialed with the ( ) brackets removed.

  The following example is a local number. When dialed by users they are likely to dial just the local number. However on incoming calls, for the CLI the telephony provider includes the full area code. Using the ( ) to enclose the area code digits, it is possible for the single directory record to be used for both incoming and outgoing calls.

  - **Name**: Raj Garden
  - **Number**: 9(01707)373386

- **Space and - Characters** Directory records can also contain spaces and - characters. These will be ignored during name matching and dialing from the directory.

Imported Records

Imported directory records are temporary until the next import refresh. They are not added to the system's configuration. They cannot be viewed or edited using Manager or edited by a system phone user. The temporary records are lost if the system is restarted. However the system will request a new set of imported directory records after a system restart. The temporary records are lost if a configuration containing Directory changes is merged. The system will then import a new set of temporary records without waiting for the **Resync Interval**. If an configuration record is edited by a system phone user to match the name or number of a temporary record, the matching temporary record is discarded.

Importation Rules

When a set of directory records is imported by HTTP or LDAP, the following rules are applied to the new records:

- Imported records with a blank name or number are discarded.
- Imported records that match the name or number of any existing record are discarded.
- When the total number of directory records has reached the system limit, any further imported records are discarded.

  For capacity information, see the description for the **Directory** tab.

Advice of Charge

The system supports advice of charge (AOC) on outgoing calls to ISDN exchanges that provide AOC information. It supports AOC during a call (AOC-D) and at the end of a call (AOC-E). This information is included in the SMDR output.

AOC is only supported on outgoing ISDN exchange calls. It is not supported on incoming calls, reverse charge calls, QSIG and non-ISDN calls. Provision of AOC signalling will need to be requested from the ISDN service provider and a charge may be made for this service.

For users, display of AOC information is only supported on T3 phones and T3 IP phones.

The user who makes an outgoing call is assigned its charges whilst they are connected to the call, have the call on hold or have the call parked.

If AOC-D is not available, then all indicated by AOC-E are assigned to the user who dialed the call.

If AOC-D is available:

- If the call is transferred (using transfer, unpark or any other method) to another user, any call charges from the time of transfer are assigned to the new user.
- If the call is manually transferred off-switch, the call charges remain assigned to the user who transferred the call.
- If the call is automatically forwarded off switch, subsequent call charges are assigned to the forwarding user.
- AOC-D information will only be shown whilst the call is connected. It will not be shown when a call is parked or held.
- Call charges are updated every 5 seconds.

For conference calls all call charges for any outgoing calls that are included in the conference are assigned to the user who setup the conference, even if that user has subsequently left the conference.

Enabling AOC Operation

1. **Set the System Currency** The Default Currency (System | Telephony | Telephony) setting is by default set to match the system locale. Note that changing the currency clears all call costs stored by the system except those already logged through SMDR.
2. **Set the Call Cost per Charge Unit for the Line** AOC can be indicated by the ISDN exchange in charge units rather than actual cost. The cost per unit is determined by the system using the **Call Cost per Charge Unit** setting which needs to be set for each line. The values are 1/10,000th of a currency unit. For example if the call cost per unit is £1.07, a value of 10700 should be set on the line.
3. **Applying a Call Cost Markup** It may be a requirement that the cost applied to a user's calls has a mark-up (multiplier) applied to it. This can be done using the Call Cost Markup (User | Telephony | Call Settings) setting. The field is in units of 1/100th, for example an entry of 100 is a markup factor of 1.

4. **Enable User AOC Display** By default users do not see call charges. The **Display Charges** setting is used to switch this option on or off. Note that the display of AOC information is only supported on T3 phones.

AOC Short Codes

A number of short code features exist that can be used with AOC. These features can only be used with T3 phones.

AOC Previous Call Displays the call costs of the user's previous call if AOC information was provided with that call.

AOC Total Display the cumulative total cost of the user's calls for which AOC information is available.

AOC Reset Total Set the cumulative total (units and cost) for the user's calls back to zero.

Emergency Call

Manager expects that the configuration of each system should contain at least one short code that is set to use the **Dial Emergency** feature. If no such short code is present in the configuration then Manager will display an error warning. The importance of the **Dial Emergency** feature is that it overrides all external call barring that may have been applied to the user whose dialing has been matched to the short code. You must still ensure that no other short code or extension match occurs that would prevent the dialing of an emergency number being matched to the short code.

The short code (or codes) can be added as a system short code or as an ARS record short code. If the **Dial Emergency** short code is added at the solution level, that short code is automatically replicated into the configuration of all servers in the network and must be suitable for dialing by users on all systems. Separate **Dial Emergency** short codes can be added to the configuration of an individual system. Those short codes will only be useable by users currently hosted on the system including users who have hot desked onto an extension supported by the system.

Determining the Caller's Location

It is the installers responsibility to ensure that a **Dial Emergency** short code or codes are useable by all users. It is also their responsibility to ensure that either:

the trunks via which the resulting call may be routed are matched to the physical location to which emergency service will be despatched

or

the outgoing calling line ID number sent with the call matches the physical location from which the user is dialing.

Hot Desking Users

In addition to the location requirements above, you must also remember that for users who hot desk, from the networks perspective the user's location is that of the system hosting the extension onto which the user is currently hot desked. If that is an IP extension then that location is not necessarily the same as the physical location of the server.

Emergency call setup

Routing of emergency calls is based on a call resolving to a Dial Emergency short code. Based on the location value for the extension making the call, routing is performed as configured in the Emergency ARS. Emergency calls have maximum priority and are not delayed in any way.

Configuring emergency call routing

Create a Dial Emergency system short code. See Dial Emergency.

Note that the **Line Group ID** value in the Dial Emergency short code is the fallback route. If the system cannot find a location or an Emergency ARS, it will try to use the **Line Group ID** to route the call.

1. Create an ARS containing a Dial short code or a Dial Emergency short code. See ARS.
2. Create a Location and set the **Emergency ARS** to the ARS created in step 2. See Location.
3. Open the **Extn** tab for an extension that will use the location defined in step 3 and set the **Location** value to the location defined in step 3. Note that once you define a location, you must set a system **Location** value on the System | System page.

For non-IP based extensions, the system location value is used as the default. For IP based extensions, the location value is set to Automatic. An attempt is made to match the extension's IP address to the subnet configured in the location. If the match is cannot be made, the location value defaults to the system location value.

From the extension used in step 3, dial the Dial Emergency short code. IP Office checks the location value and determines the emergency ARS set for the location. Once the emergency ARS is found, IP Office will try to match the Telephone Number in the Dial Emergency short code to a short code in the ARS and use it to make the emergency call.

Fax Support

Fax on IP500 V2 Systems

IP500 V2 systems can terminate T38 fax calls. For a system with an IP500 VCM, IP500 VCM V2 or IP500 Combo cards, **T38** or **G.711** can be used for fax transmission. Each fax call uses a VCM channel unless it is a T38 fax call between compatibly configured call legs. A SIP line or extension must support Re-Invite.

T38 Fallback can also be specified. On outgoing fax calls, if the called destination does not support T38, a re-invite is sent for fax transport using **G.711**.

Configuring Fax on SIP Lines and Extensions:

To configure Fax on SIP Lines and Extensions:

1. On the **VoIP** page for the line or extension, set **Re-Invite Supported** to **On** in order to enable **Fax Transport Support**
2. Select a value in the **Fax Transport Support** field.

Note the following:

- Direct media is supported.
- If **Fax Transport Support** is set to **T38** or **T38 Fallback**, the T38 Fax page is available. The T38 Fax page provides detailed T38 configuration options.

Configuring Fax on an IP Office Line:

Within a multi-site network, **Fax Transport Support** can also be enabled on the IP Office Lines between the systems. This allows fax calls at one system to be sent to another system.

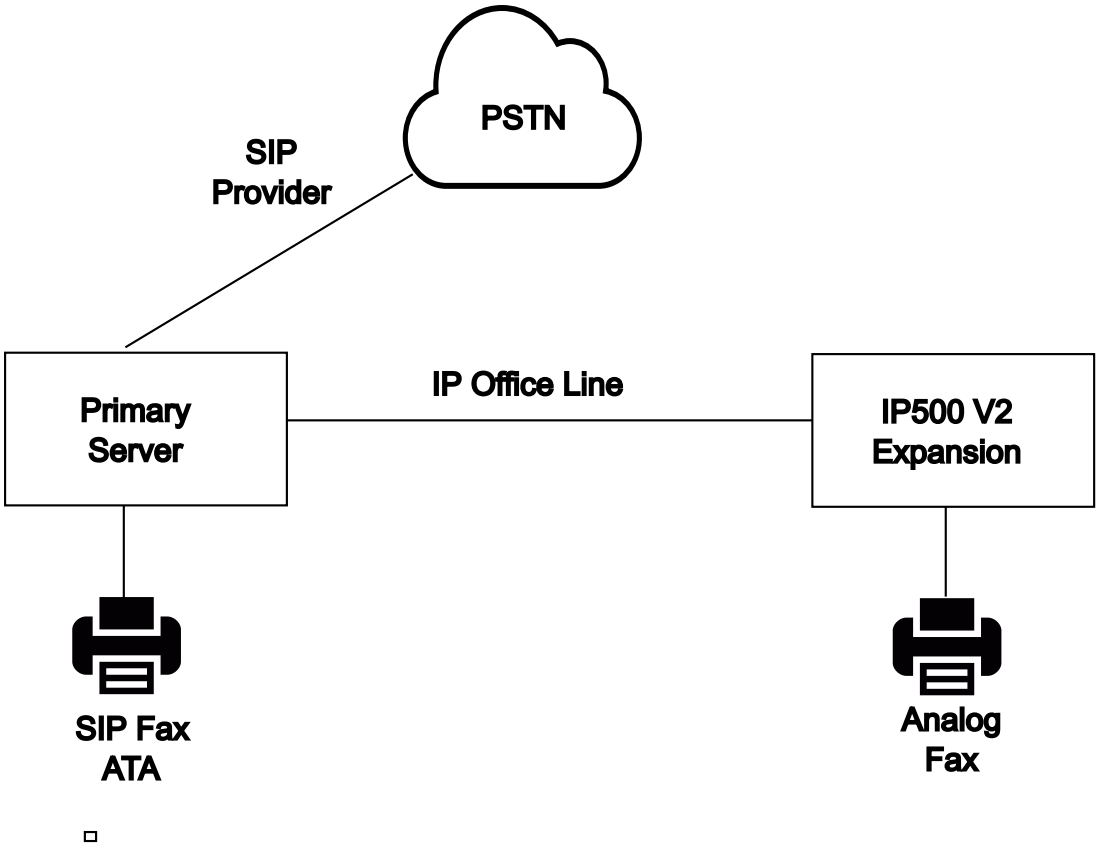
To configure Fax on an IP Office Line:

1. Set **IP Office Line | Line Settings | Networking Level** to **SCN**.
2. Set **IP Office Line | VoIP | Fax Transport Support** to **Fax Relay**.

Related links

Server Edition T38 Fax Support on page 528

Server Edition T38 Fax Support



Fax on Server Edition Linux Servers

IP Office Linux servers cannot terminate T38 fax and therefore, T38 is negotiated end-to-end. When a SIP ATA fax is connected to an IP Office Linux server, the system directly relays negotiation between the SIP ATA Fax and the SIP provider.

Configuring Fax on SIP Lines and Extensions:

To configure Fax on SIP Lines and Extensions, on the **VoIP** page for the SIP line or extension:

1. Set **Re-Invite Supported** to **On** in order to enable **Fax Transport Support**.
2. Select a value in the **Fax Transport Support** field.

Note the following.

- Direct media is supported.
- The **T38 Fax** page is not available.

Fax on Server Edition IP500 V2 Expansion Systems

Since an IP500 V2 system can terminate T38 fax, an analog fax can be connected to an IP500 V2 Expansion system. Fax transport is configured on the IP Office Line connecting the IP500 V2 system to the Server Edition network.

Configuring Fax on an IP Office Line:

To configure Fax on an IP Office Line, on the **Line | IP Office Line | VoIP Settings** page, select a value in the **Fax Transport Support** field. **Fax Relay** is not supported.

Note the following.

- Direct media is supported.
- The **T38 Fax** page is not available.

Related links

Fax Support on page 527

Caller Display

Caller display displays details about the caller and the number that they called. On internal calls, the system provides this information. On external calls it uses the Incoming Caller Line Identification (ICLID) received with the call. The number is also passed to system applications and can be used for features such as call logging, missed calls and to make return calls.

Analog extension can be configured for caller display via the system configuration (Extension | Extn | Caller Display Type).

Adding the Dialing Prefix Some systems are configured to require a dialing prefix in front of external numbers when making outgoing calls. When this is the case, the same prefix must be added to the ICLID received to ensure that it can be used for return calls. The prefix to add is specified through the Prefix field of each line.

Directory Name Matching The system configuration contains a directory of names and numbers. If the ICLID of an incoming call matches a number in the directory, the directory name is associated with that call and displayed on suitable receiving phones.

Applications such as SoftConsole also have directories that can be used for name matching. If a match occurs, it overrides the system directory name match for the name shown by that application.

Extended Length Name Display

In some locales, it may be desirable to change the way names are displayed on phones in order to maximize the space available for the called or calling name. There are two hidden controls which can be used to alter the way the system displays calling and called information.

These controls are activated by entering special strings on the Source Numbers tab of the NoUser user. These strings are:

LONGER_NAMES This setting has the following effects:

- On DS phones, the call status display is moved to allow the called/calling name to occupy the complete upper line and if necessary wrap-over to the second line.
- For all phone types:
- On incoming calls, only the calling name is displayed. This applies even to calls forwarded from another user.
- On outgoing calls, only the called name is displayed.

HIDE_CALL_STATE This settings hides the display of the call state, for example **CONN** when a call is connected. This option is typically used in conjunction with **LONGER_NAMES** above to provide additional space for name display.

Parking Calls

Parking a call is an alternative to holding a call. A call parked on the system can be retrieved by any other user if they know the system park slot number used to park the call. When the call is retrieved, the action is known as Unpark Call or Ride Call. While parked, the caller hears music on hold if available.

Each parked call requires a park slot number. Attempting to park a call into a park slot that is already occupied causes an intercept tone to be played. Most park functions can be used either with or without a specified park slot number. When parking a call without specifying the park slot number, the system automatically assigns a number based on the extension number of the person parking the call plus an extra digit 0 to 9. For example if 220 parks a call, it is assigned the park slot number 2200, if they park another call while the first is still parked, the next parked call is given the park slot number 2201 and so on.

Park slot IDs can be up to 9 digits in length. Names can also be used for application park slots.

The **Park Timeout** setting in the system configuration (System | Telephony | Telephony | Park Timeout) controls how long a call can be left parked before it recalls to the user that parked it. The

default time out is 5 minutes. Note that the recall only occurs if the user is idle has no other connected call.

There are several different methods by which calls can be parked and unparked. These are:

Using Short Codes

The short code features, Call Park and Unpark Call, can be used to create short codes to park and unpark calls respectively. The default short codes that use these features are:

- *37*N# - Parks a call in park slot number N.
- *38*N# - Unparks the call in park slot number N.

Using the SoftConsole Application

The SoftConsole application supports park buttons. SoftConsole provides 16 park slot buttons numbered 1 to 16 by default.

The park slot number for each button can be changed if required. Clicking on the buttons allows the user to park or unpark calls in the park slot associated with each button. In addition, when a call is parked in one of those slots by another user, the application user can see details of the call and can unpark it at their extension.

Using Programmable Buttons

The Call Park feature can be used to park and unpark calls. If configured with a specified park slot number, the button can be used to park a call in that slot, unpark a call from that slot and will indicate when another user has parked a call in that slot. If configured without a number, it can be used to park up to 10 calls and to unpark any of those calls.

Phone Defaults

Some telephones support facilities to park and unpark calls through their display menu options (refer to the appropriate telephone user guide). In this case parked calls are automatically put into park slots matching the extension number.

Configuring Call Admission Control

Call Admission Control (CAC) is a method of controlling system resources using defined locations. Calls into and out of each location are allowed or disallowed based upon configured call constraints. In Manager, use the **Location** tab to define a location and configure the maximum calls allowed for the location.

Related links

Manager location tab on page 532
Assigning a network entity to a location on page 532
System actions at maximum call threshold on page 533
Example on page 533

Manager location tab

Configuring location settings

On the Manager **Location** tab, set the following parameters for a location:

- Location Name
- Subnet Address
- Subnet Mask

Configuring Call Admission Control settings

On the Manager Location tab, set the following CAC parameters:

- **Internal Maximum Calls**: Calls that pass from the location to another configured location.
- **External Maximum Calls**: Calls that pass from the location to an unmanaged location.
- **Total Maximum Calls**: The total internal and external calls permitted.

Related links

Configuring Call Admission Control on page 531

Assigning a network entity to a location

The **Location** field is a drop down list of locations defined on the **Location** tab. Network entities are assigned to a location using the **Location** field on the following Manager tabs.

- **System**
- **Extension**
- **SIP Line | VoIP**
- **H323 Line | VoIP**

The following default settings are applied.

- Each IP Office system can be configured with a defined location. For Server Edition deployments, the configuration of locations is done solution wide. All IP Office systems in the solution share the same location configuration.
- Digital phones default to the system location.
- The default setting for IP phones is **Automatic**. Phones registering from a subnet matching that of a location will be treated as within that location. Otherwise, the phone is assigned the same location as the system. Cloud can be used for phones whose Location is variable or unknown.
- IP Lines default to **Cloud**.

Related links

Configuring Call Admission Control on page 531

System actions at maximum call threshold

- A congestion alarm is raised.
- Calls that exceed the CAC maximum values are not allowed.
- Calls from extensions to public trunks through Alternate Route Selection (ARS) are queued and display **Waiting for Line**.
- Calls from extensions to public trunks which do not route through ARS receive a fast-busy tone and display **Congestion**.
- Idle phones display **Emergency/Local calls only**.
- Alternative routing to a local PSTN gateway follows ARS priority escalation rules.
- SIP calls that would exceed call limits and have no other targets are declined with **cause=486** or **cause = 503**.

Allowed calls

When CAC limits have been reached, the following calls are allowed.

- Emergency calls are always allowed.
- Established calls are never torn down to achieve limits.
- A phone on a remote site that parks a call is always allowed to retrieve it.
- Request Coaching Intrusion calls are allowed.

Related links

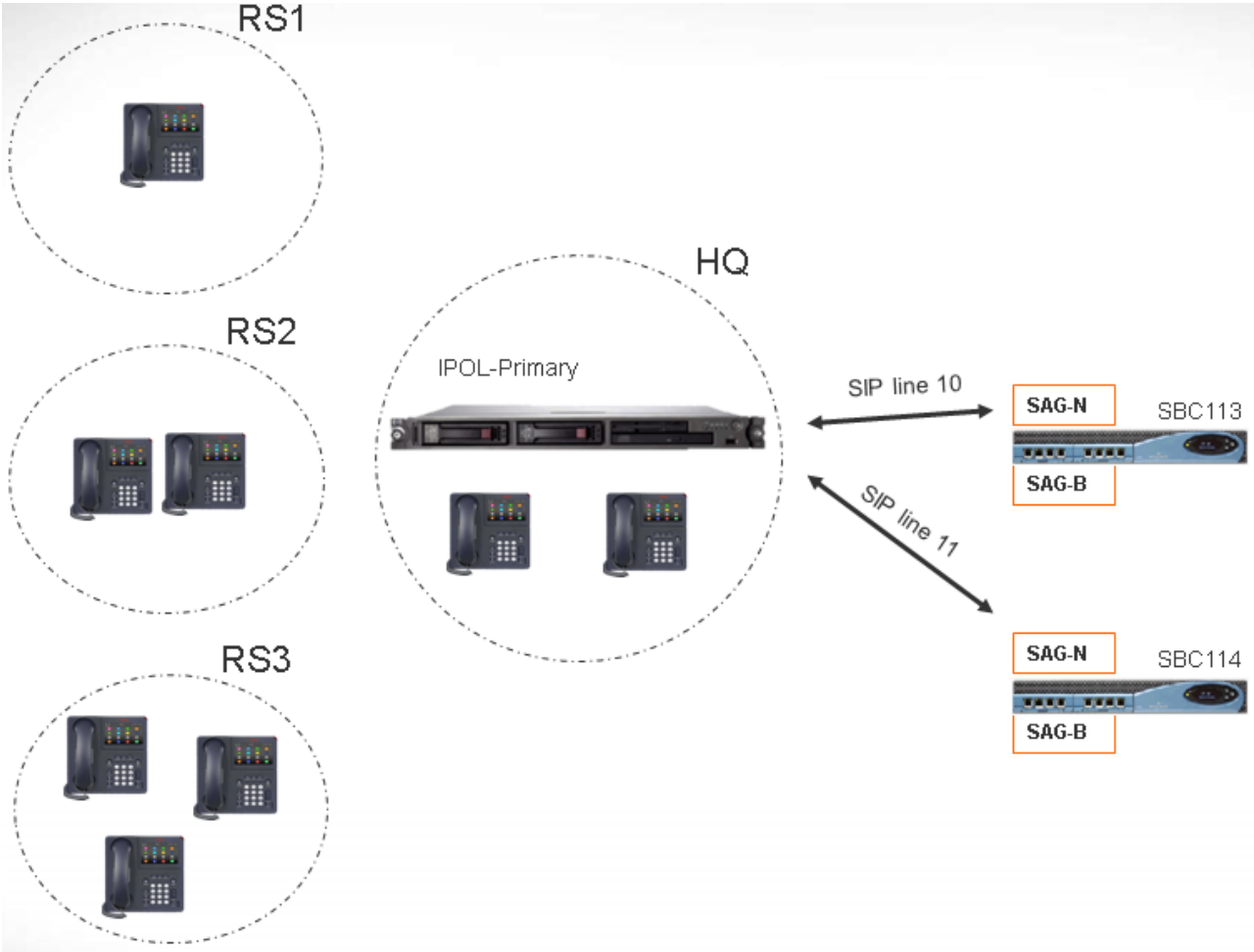
Configuring Call Admission Control on page 531

Example

The example configuration has four locations.

Location	Max Calls
HQ	20
RS1	5
RS2	10
RS3	15
+Cloud	unlimited

SIP Line 10 and SIP Line 11 are configured with 20 channels.



Notes

- Calls between locaton RS1 and SBC113 do not increment the call count for HQ.
- The HQ call count includes calls across the HQ boundary which anchor media inside HQ. SBC113 and SBC 114 are both included.
- The HQ maximum calls value is separate and complementary to the individual trunk call maximum.
- Incoming calls from SIP to RS1 (direct media) only need to verify that the RS1 location maximum call value is not exceeded.
- SIP calls that are not allowed to RS1 may go to HQ voicemail if the HQ call limit is not exceeded.

Related links

Configuring Call Admission Control on page 531

Ring Tones

Ring tones can be defined in the following terms.

Distinctive Ringing - Inside, Outside and Ringback:

A distinctive ring tone can be given for each of the different call types: an internal call, an external call and a ringback calls (voicemail calls, ringback when free calls, calls returning from park, hold or transfer).

The distinctive ringing patterns used for most non-analog phones are as follows:

- **Internal Call**: Repeated single-ring.
- **External Call**: Repeated double-ring.
- **Ringback Call**: Two short rings followed by a single ring.

Note:

For non-analog extensions, the ringing pattern used for each call type by the system is not configurable.

Personalized Ringing:

This term refers to control of the ringing sound through the individual phones. For non-analog phones, while the distinctive ringing patterns cannot be changed, the ringer sound and tone may be personalized depending on the phone's own options. Refer to the appropriate telephone user guide.

Analog Phone Ringing Patterns

For analog extensions, the ringing pattern used for each call type can be set using the settings on **System Settings** > **System** > **Telephony**. The setting for an individual user associated with an analog extension can be configured using the settings on **Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Call Settings**.

Note that changing the pattern for users associated with fax and modem device extensions may cause those devices to not recognize and answer calls.

The selectable ringing patterns are:

- **RingNormal** This pattern varies to match the **Locale** set in the **System | System** tab. This is the default for external calls.
- **RingType1**: 1s ring, 2s off, etc. This is the default for internal calls.
- **RingType2**: 0.25s ring, 0.25s off, 0.25s ring, 0.25s off, 0.25s ring, 1.75s off, etc. This is the default for ringback calls.
- **RingType3**: 0.4s ring, 0.8s off, …
- **RingType4**: 2s ring, 4s off, …
- **RingType5**: 2s ring, 2s off, …
- **RingType6**: 0.945s ring, 4.5s off, …
- **RingType7:** 0.25s ring, 0.24 off, 0.25 ring, 2.25 off, …

- **RingType8**: 1s ring, 3s off, …
- **RingType9**: 1s ring, 4s off, …
- **RingType0**: Same as **RingNormal** for the United Kingdom locale.
- **Default Ring**: Shown on the User | Telephony | Call Setting tab. Indicates follow the settings on the System | Telephony | Tones & Music tab.

Configuring Ring Tone Override for Groups and Incoming Call Routes

You can configure ring tone override for groups and incoming call routes. **Ring Tone Override** is supported on 1400 and 9500 series phones.

Note that you can use short codes to configure a ring tone plan by using the “r” character as part of the short code telephone number field. See Short Code Characters on page 694.

1. In Web Manager, select **System Settings** > **System** > **Telephony** > **Ring Tones**.
2. In the **Ring Tone Plan** table, enter a **Name** for the ring tone. The **Number** field is populated automatically.
3. Under **Ring Tone**, select one of the eight ring tones from the drop down list.
4. Once configured in this table, ring tone names can be selected from the **Ring Tone Override** field at:
   - **Call Management** > **Group** > **Add/Edit Group** > **Group**
   - **System Settings** > **Incoming Call Route** > **Add/Edit Incoming Call Route**

Music On Hold

Each system can provide music on hold (MOH) from either internally stored files or from externally connected audio inputs. Each system has one system source and then a number of alternate sources (up to 3 alternate sources on IP500 V2 and 31 alternate sources on Server Edition).

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

WAV Files

The system can use internal files that it stores in its non permanent memory. The WAV file properties must be in the format listed below. If the file downloaded is in the incorrect format, it will be discarded from memory after the download.

- Mono PCM 8kHz 16-bit
- maximum length 90 seconds on IP500 V2 systems, 600 seconds on Linux based systems.
- The first WAV file, for the system source, must be called `HoldMusic.wav`. Alternate source WAV file names:
  - can be up to 27 IA5 characters
  - cannot contain spaces
  - any extension is allowed

- case sensitive

The files, when specified by the system source or an alternate source setting, are loaded as follows:

- Following a reboot, the system will try using TFTP to download the file or files.
- The initial source for TFTP download is the system's configured **TFTP Server IP Address** (**System | System | LAN Settings**). The default for this is a broadcast to the local subnet for any TFTP server.
- Manager can act as a TFTP server while it is running. If Manager is used as the TFTP server, then the wav file or files should be placed in the Manager applications working directory.

  Note:

  The following Manager settings are disabled by default:

  - **Security Settings | Unsecured Interfaces | Applications Controls | TFTP Directory Read**
  - **File | Preferences | Preferences | Enable BootP and TFTP Servers**
- On Linux based systems, if no successful TFTP download occurs, the system automatically looks for the files in the `opt/ipoffice/tones/mohwavdir` folder (`disk/tones/mohwavdir` when access using file manager).
- The name of the system music .wav file should be **HoldMusic.wav**. The name of alternate source .wav files should be as specified in the **Alternate Sources** table (**System | Telephony | Tones and Music**) minus the **WAV**: prefix.

WAV File Download and Storage:

- If no successful TFTP download occurs:
  - On IP500 V2 systems, the system automatically looks for the file in the `system/primary` folder on the System SD card and downloads it from if found.
  - On Linux based systems, the system automatically looks for the file in the folder `opt/ipoffice/system/primary` folder (`disk/system/primary` when accessed using file manager) and downloads it from there if found.
- If a music on hold file is downloaded, the system automatically write a copy of that file to its memory card, overwriting any existing file of the same name already stored on the card.
- For files downloaded from a System SD card, the system will download the file again if the SD card is shutdown and restarted or if files are uploaded to the card using the Embedded File Manager.
- The system will download the file again if new files are copied to the disk or uploaded using File Manager.

Tone

If no internal music on hold file is available and **External** is not selected as the **System Source**, then the system provides a default tone for music on hold. The tone used is double beep tone (425Hz repeated (0.2/0.2/0.2/3.4) seconds on/off cadence). **Tone** can be selected as the **System Source**, overriding both the use of the external source port and the downloading of **HoldMusic.wav**.

Controlling the Music on Hold Source Used for Calls

Unless specified, the System Source is used for any calls put on hold by system users. For any call, the last source specified for the call is the one used. The following options allow the source to be changed.

- **Hunt Group** Each hunt group can specify a **Hold Music Source** (**Group | Group**). That source is then used for calls presented to the hunt group.

  In a multi system network, a hunt group member will hear the music on hold (MOH) from their local system. For example, a call comes in to site A and rings a hunt group with members from system A and system B. If a hunt group member from system B answers a call and puts the call on hold, the caller hears the MOH from system B.

- **Incoming Call Route** Each incoming call route can specify a **Hold Music Source** (**Incoming Call Route | Standard**). That source is then used for incoming calls routed by that incoming call route.

- **Short Code** The **h** character can be used in the **Telephone Number** field of short codes to specify the hold music to associate with calls routed by that short code. The format **h(X)** is used where **X** is the source number. This method can be used to specify a hold music source for outgoing calls.

Checking Music on Hold

The system short code feature Hold Music can be used to listen to the hold music sources. Dial ***34N#**, replacing **N** with the source number 1 (System Source) or 2 to 32 (Alternate Sources).

Related links

System Source on page 538
Alternate Source on page 538

System Source

The first source is called the **System Source**. This source is numbered source 1. The possible options for this source are:

- **WAV**: A file called `HoldMusic.wav` downloaded by the system.
- **External**: For IP500 V2 systems, use the audio source connected to the back of the control unit. For Linux systems, the first available USB source is used.
- **Tone**: A double beep tone. Used automatically if the System Source is set to WAV and the **HoldMusic.wav** file has not been successfully downloaded.

Related links

Music On Hold on page 536

Alternate Source

You can specify alternate sources on the **System Settings** > **System** > **Telephony** > **Tones and Music** page. The available options depends on the system type. For IP500 V2 systems, up to 3

alternate sources can be specified. For systems on a Linux based server, up to 31 alternate sources can be specified. See the table below for details.

Alternate Option	Description
WAV:<filename>	• The <filename> parameter specifies the filename to be played. • <filename>: - can be up to 27 IA5 characters - cannot contain spaces - any extension is allowed - case sensitive • A TFTP read is attempted first, then the file location `opt/ipoffice/system/primary` (Linux) or `/system/primary` (IP500 V2). • When a MOH source is activated, the playback resumes from where it left off last time, instead of starting every time from the beginning. • At any moment, all users listening to a given MOH source will hear the same thing (instead of every user hearing from a different file position). • For Linux systems, this source is suitable for use with the **LINE** option.
XTN: <extension>	Only supported on IP500 V2 systems. Any analog extension with its Equipment Classification set as MOH Source can be entered as the alternate source. Enter XTN: followed by the extension's Base Extension number. For example ***XTN:224***
WAVRST:<filename>	• Not supported on IP500 V2 systems. • The <filename> parameter specifies the filename to be played. • A TFTP read is attempted first, then the folder `opt/ipoffice/system/primary` (SSH access) (`disk/system/primary` (file manager access)). • When a MOH source is activated, the playback is started every time from the beginning. • At any moment, all users listening to a given MOH source will hear a different WAV file or file position.

Table continues…

Alternate Option	Description
WAVDIR:	• Not supported on IP500 V2 systems. • No additional parameter is required. • The directory used is `opt/ipoffice/tones/mohwavdir` (SSH access) or `/disk/tones/mohwavdir` (file manager access). • Up to 255 files, up to 10 minutes per file. • The files are played in filename order (numerical, lower case, then upper case). • When a MOH source is activated, the playback resumes from where it left off last time. • At any moment, all users listening to this source will hear the same thing. • There can only be one WAVDIR: or WAVDIRRST: entry per system. • This is a streamed source suitable for use with the **LINE** option.
WAVDIRRST:	As per **WAVDIR** above, however • When a MOH source is activated, the playback is started every time from the beginning (start of the first file in the folder). • At any moment, all users listening to this source will hear a different WAV file or file position. • Not suitable for use with the **LINE** option.

Table continues…

Alternate Option	Description
USB: <number>	• Not supported on IP500 V2 systems. • The <number> parameter is the logical USB device number. • USB:1 is the first source found and is automatically used for the **System Source** when set to External. • Additional devices are numbered sequentially. For example, USB:2, USB:3. Up to four USB sources are supported. • IPOffice will auto-configure USB sound devices with settings that work well in most cases. Line input is selected and volume is set close to maximum. If no line input is identified on the card, microphone input is used instead. • Supported with ALSA USB sound cards, The following USB audio devices have been tested: - Creative X-FI GO Pro USB - Asus Xonar U3 • External USB sound devices are hot-pluggable. They can be added and removed from the system at any time. • Care should be taken when adding or removing USB sound cards as this may change the logical number. • When an USB MOH source becomes unavailable, the default MOH tone will be played instead. • A USB MOH source is not supported on virtual servers. • This is a streamed source suitable for use with the **LINE** option.

Table continues…

Alternate Option	Description
LINE:<X,Y>	• Two parameters are supplied. - X = SCN line number to the Linux Server (not outgoing group ID). - Y = The MOH source number on the Linux Server. • The Linux Server is typically the Primary, but the Secondary Server can be used. • The MOH Source must be a stream type (Not WAVRST: or WAVDIRRST:) • Centralised MOH will place a VoIP call to the MOH source when MOH is required. • Takes one call capacity from the trunk and therefore, can be subject to CAC limits. • Uses the SCN trunks' codec preferences. • G.729 not recommended (better results are achieved with G.711). • Calls are dropped after 30s of no use. • If 30s is not appropriate, it can be changed with the NoUser source number HOLD_MUSIC_TIMEOUT=x, where x is number of seconds (range = 0 and 600). 0 means never tear down the call (and never retry – should not be used!) • The status displayed in SSA • Note that as this option can only be specified as an alternate source, centralized MOH cannot be used as the System Source. That is, it cannot be used for internal calls' MOH.

Related links

Music On Hold on page 536

Conferencing

The IP Office system supports a number of conference features and allows multiple simultaneous conferences.

Conference Types

There are 2 types of conference supported by the system:

- **Ad-Hoc Conferencing** An ad-hoc conference is one created on the fly, typically by holding an existing call, making another call and then pressing a conference key on the phone. Other people can be added to the conference by repeating the process.
- **Meet Me Conferencing** Conference Meet Me allows users to join or start a specific numbered conference. This method of operation allows you to advertise a conference number and then let the other parties join the conference themselves.

User Personal Conference Number Each user's own extension number is treated as their own personal conference number. Only that user is able to start a conference using that number as the conference ID. Any one else attempting to start a conference with that number will find themselves in a conference but on hold until the owner also joins. Personal conferences are always hosted on the owner's system. Note, when a user calls from their mobile twinned number, the personal conference feature will only work if they access the conference using an FNE 18 service.

Conference Notes

Other Uses of Conference Resources System features such as call intrusion, call recording and silent monitoring all use conference resources for their operation. On IP500 V2 systems, each Embedded Voicemail call in progress also reduces the conference capacity.

Automatically Ending Conferences The behavior for the system automatically ending a conference varies as follows:

- A conference remains active until the last extension or trunk with reliable disconnect leaves. Connections to voicemail or a trunk without reliable disconnect (for example an analog loop-start trunk) will not hold a conference open.
- The **Drop External Only Impromptu Conference** setting controls whether a conference is automatically ended when the last internal party exits the conference.

Analog Trunk Restriction In conferences that include external calls, only a maximum of two analog trunk calls are supported. This limit is not enforced by the system software.

Recording Conferences If call recording is supported, conference calls can be recorded just like normal calls. Note however that recording is automatically stopped when a new party joins the conference and must be restarted manually. This is to stop parties being added to a conference after any "advice of recording" message has been played.

IP Trunks and Extensions Conferencing is performed by services on the system's non-IP interface. Therefore a voice compression channel is required for each IP trunk or extension involved in the conference.

Call Routing A short code routing calls into a conference can be used as an Incoming Call Route destination.

Conference Tones The system provides conference tones. These will be either played when a party enters/leaves the conference or as a regularly repeated tone. This is controlled by the Conferencing Tone (**System | Telephony | Tones & Music**) option.

Paging

Paging limits

Server Type	Paging Group Maximum size (Select and Non-Select)
Dell R620	256
OVA	256

Table continues…

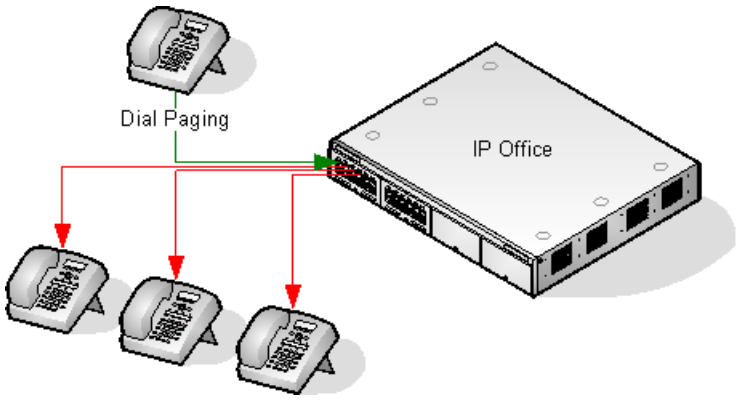
Server Type	Paging Group Maximum size (Select and Non-Select)
DL360G7	128
HP120G7/Dell R210 II	128
IP500 V2	64

- 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%.

Paging Scenarios

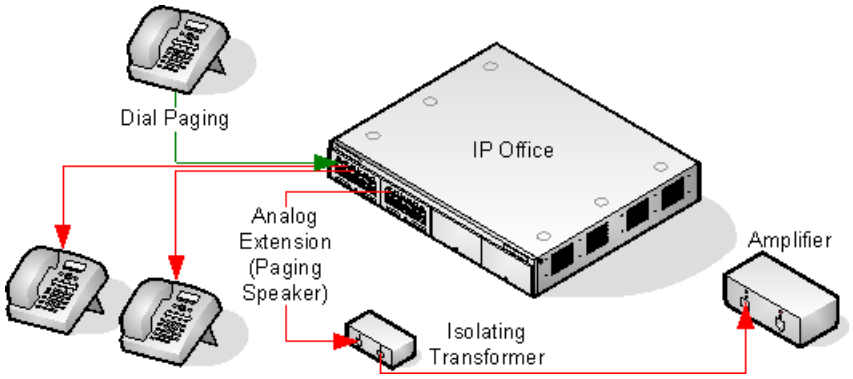
Paging Scenario	Paged Device Connects to...	Short Code/ Button Feature
Phone to Phone: Simple paging to other system extensions.	Digital Station and Avaya H.323 Phones	**Dial Paging**
Mixed Paging: This refers to simultaneous paging to phones and a paging speaker.	Analog Extension (Paging Speaker)	**Dial Paging**
Paging Interface Device: This refers to paging to a paging interface device such as a UPAM.	Analog Extension (IVR Port)	**Dial Extn**
	Analog Trunk	**Dial**

Phone to Phone Paging



- Paging is supported from all phone types. A page call can be to a single phone or a group of phones.
  - From analog and non-Avaya phones, use a Dial Paging short code.
  - From Avaya feature phones, a programmable button set to Dial Paging can be used.
- Paging is only supported to Avaya phones that support auto answer.
- The page is not heard on phones that are active on another call.
- The page is not heard on phones where the user is set to Do Not Disturb or has Forward Unconditional active.
- On Avaya phones with a dedicated **Conference** button, the user can answer a page call by pressing that button. This turns the page into a normal call with the pager.

Mixed Paging



Uses an amplifier connected to an analog extension port via a 600ohm isolating transformer. Some amplifiers include an integral transformer. Avaya/Lucent branded amplifiers are designed for connection to special paging output ports not provided on systems. They are not suitable for supporting mixed paging.

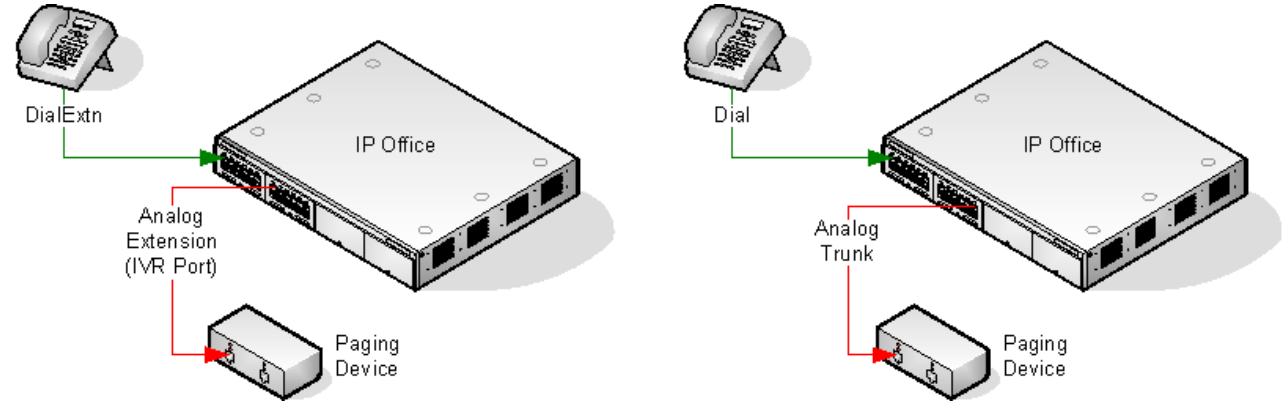
The transformer and amplifier must be connected when the system is restarted.

If background music is required between pages, the amplifier must support a separate background music connection and VOX switching.

The analog extension port is set as a Paging Speaker in the system configuration (**Extn | Analog | Equipment Classification**).

Short code/programmable button: Use DialPaging.

Paging Interface Device



Uses a paging interface device such as a UPAM or amplifier with analog trunk/extension interface. The device can be connected to an analog trunk port or analog extension port.

If connected to a trunk port, use the short code Use Dial and the same Line Group ID as the Outgoing Line ID set for the analog trunk.

If connected to an extension port:

- Set the analog extension as an IVR Port in the system configuration (Extn | Analog | Equipment Classification).
- Short code/programmable button: Use Dial Extn.

Automatic Intercom Calls

Automatic intercom functions allow you to call an extension and have the call automatically answered on speaker phone after 3 beeps. The extension called must support a handsfree speaker. If the extension does not have a handsfree microphone then the user must use the handset if they want to talk. If the extension is not free when called, the call is presented as a normal call on a call appearance button if available.

Making Automatic Intercom Calls

The following programmable button functions can be used to make automatic intercom calls:

- **Automatic Intercom**
- **Dial Direct**
- **Dial Intercom**

The following short code function can be used to make automatic intercom calls:

Dial Direct

On M-Series and T-Series phones, the code **Feature 66** followed by the extension number can be used to make a direct voice (automatic intercom) call.

Deny automatic intercom calls

When enabled, any automatic intercom calls to the user's extension are automatically turned into normal calls.

Deny automatic intercom calls can be configured per user on the **User | Telephony | Supervisor Settings** tab. Deny automatic intercom call can also be enabled using the Auto Intercom Deny On short code or the Auto Intercom Deny button action.

Wide Band Audio Support

IP Office systems support the G.722 64K codec for wide band audio. G.722 can be used with H. 323 and SIP trunks. If can also be used with some SIP and H.323 IP telephones (see below). G. 722 uses a higher speech sample rate (16KHz) than is used by most other audio codecs (8KHz).

G.722 is only supported by systems that are using IP500 VCM, IP500 VCM V2 and or IP500 Combination cards.

Avaya Phone Support

Use of G.722 is supported by the following Avaya phones on a IP Office system:

B179	1140E	9621	9650
1010	9608	9630	J169
1040	9611	9640	J179
1120E	9620	9641	

Using the G.722 Codec

The G.722 codec is not available for use by default. If the codec is to be used, it must first be selected in the system's **Available Codecs** list (System | Codecs). The codec can then be used in the system's default codec preference list and or in the individual codec preferences of IP lines and extensions.

The method of codec selection for specific phones will depend on the phone type. Refer to the appropriate installation manual.

Conferencing

Where devices using G.722 are in a system conference, the system can attempt to ensures that the speech between devices using G.722 remains wide-band even if there are also narrow-band audio devices in the same conference. This is done if the system's High Quality Conferencing option is enabled (**System | Telephony | Telephony**).

Known Limitations

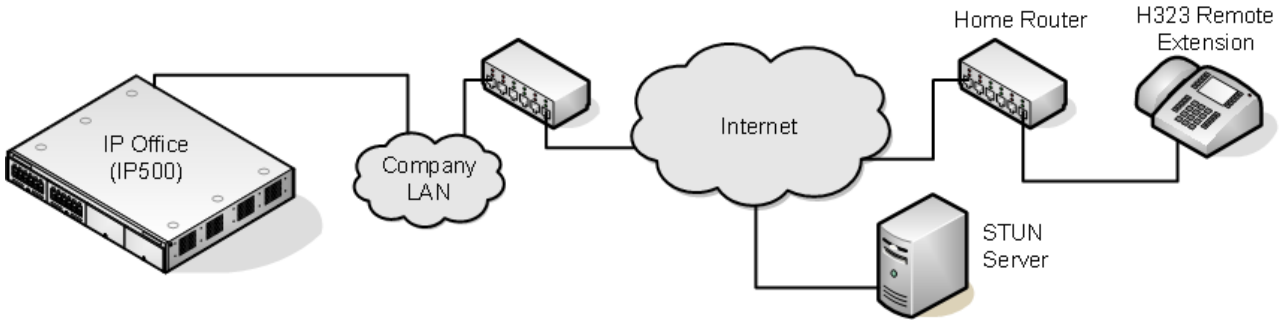
The following limitations apply to G.722 wide band audio operation:

- Call recording uses G.711.
- Page calls only use G.722 when all devices being paged can use G.722.
- Fax is not supported in G.722, use G.711 or T38.
- Soft tones provided by the system use G.711.
- A maximum of 15 G.722 devices receiving wide-band audio are supported in conferences.

Configuring Remote H.323 Extensions

The configuration of remote H.323 extensions is supported without needing those extensions to be running special VPN firmware. This option is intended for use in the following scenario:

- The customer LAN has a public IP address which is forwarded to the IP Office system. That address is used as the call server address by the H.323 remote extensions.
- The user has a H.323 phone behind a domestic router. It is assumed that the domestic router allows all outbound traffic from the home network to pass through and allows all symmetric traffic. That is, if the phone sends RTP/RTCP to a public IP address and port, it will be able to receive RTP/RTCP from that same IP address and port. If this is not the case, the configuration of the user's router to support that is not covered by this documentation.



Other scenarios can be configured. For example one of the IP Office's LAN interfaces can be connected to the public internet.

Supported Telephones: Currently remote H.323 extension operation is only supported with 9600 Series phones already supported by the IP Office system.

License Requirements: For non-Server Edition systems, by default only 4 users can be configured for remote H.323 extension usage. Additional users can be configured if those additional users are licensed and configured with either **Teleworker** or **Power User** user profiles. On Server Edition systems, all users can be configured for remote H.323 extension usage.

Customer Network Configuration

The corporate LAN hosting the IP Office system requires a public IP address that is routed to the LAN interface of the IP Office system configured for remote H.323 extension support.

STUN from the IP Office system to the Internet is used to determine the type of NAT being applied to traffic between the system and the Internet. Any routers and other firewall devices between the H.323 phone location and the IP Office system must allow the following traffic.

Protocol	Port	Description
UDP	**1719**	UDP port 1719 traffic to the IP Office system must be allowed. This is used for H225 RAS processes such as gatekeeper discovery, registration, keepalive, etc. If this port is not open, the phone will not be able to register with the IP Office system.
TCP	**1720**	TCP port 1720 traffic must be allowed. This is used for H225 (call signalling).
TCP	**1300**	TCP port 1300 must be allowed when using TLS.
RTP	**Various**	The ports in the range specified by the system's **RTP Port Number Range (Remote Extn)** settings must be allowed.
RTCP		

User Network Configuration

It is assumed that the domestic router allows all outbound traffic from the home network to pass through and allows all symmetric traffic. That is, if the phone sends RTP/RTCP to a public IP address and port, it will be able to receive RTP/RTCP from that same IP address and port. If this is not the case, the configuration of the user's router to support that is not covered by this documentation.

System Configuration

About this task

This is a summary of the system configuration changes necessary. Additional details and information for H.323 telephone installation are included in the H.323 IP Telephone Installation manual. This section assumes that you are already familiar with IP Office system and H.323 IP telephone installation.

Procedure

1. Licensing:

   For non-Server Edition systems, by default only 4 users can be configured for remote H.323 extension usage. Additional users can be configured if those additional users are licensed and configured with either **Teleworker** or **Power User** user profiles. On Server Edition systems, all users can be configured for remote H.323 extension usage.

2. System Configuration:

   The following needs to be configured on the IP Office system LAN interface to which the public IP address is routed.

   a. Select **System | LAN1/LAN2 | VoIP**.

      Check that the **H.323 Gatekeeper Enable** setting is selected.

   b. Due to the additional user and extension settings needed for remote H.323 extension configuration, we assume that the extension and user records for the remote H.323 extensions and users are added manually.

   c. Select **H.323 Remote Extn Enable**.

   d. Set the **RTP Port Number Range (Remote Extn)** range to encompass the port range that should be used for remote H.323 extension RTP and RTCP traffic. The range setup must provide at least 2 ports per extension being supported.

      Note:

      When the system is configured on an open internet connection, the standard RTP port range is used for all H.323 calls including remote workers. In such a case the **RTP Port Number Range** is used.

3. Network Topology Configuration:

   STUN can be used to determine the type of NAT/firewall processes being applied to traffic between between the IP Office system and the Internet.

   a. Select the **Network Topology** tab.

   b. Set the **STUN Server IP Address** to a known STUN server. Click **OK**. The **Run STUN** button should now be enabled. Click it and wait while the STUN process is run. The results discovered by the process will be indicated by **!** icons next to the fields

c. If STUN reports the **Firewall/NAT Type** as one of the following, the network must be reconfigured if possible as these types are not supported for remote H.323 extensions: **Static Port Block**, **Symmetric NAT** or **Open Internet**.

4. H.323 Extension Configuration:

   H.323 remote extensions use non default settings and so cannot be setup directly using auto-create.

   a. Within Manager, add a new H.323 extension or edit an existing extension.

   b. On the **Extn** tab, set the **Base Extension** number.

   c. On the **VoIP** tab, select **H.323 Remote Extn Enable**.

   d. The other settings are as standard for an Avaya H.323 telephone.

      - The IP Address field can be used to restrict the the source IP address that can used by the Remote Worker. However, it should not used in the case where there is more than one phone behind the domestic router.
      - Regardless of direct media configuration, direct media is not used for remote H.323 extensions except for calls between devices behind the same NAT when **Allow Direct Media Within NAT Location** is set to **On**.

5. User Configuration:

   For non-Server Edition systems, by default only 4 users can be configured for remote H. 323 extension usage.

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

   a. In the user configuration, select **Enable Remote Worker**.

   b. If the user's **Extension Number** matches the **Base Extension** setting of an IP extension, the **H.323 Remote Extn Enable** setting of that extension is automatically changed to match the user's **Enable Remote Worker** setting and vice versa.

Phone Configuration

About this task

The phones do not require any special firmware. Therefore they should first be installed as normal internal extensions, during which they will load the firmware provided by the IP Office system.

Once this process has been completed, the address settings of the phone should be cleared and the call server address set to the public address to be used by remote H.323 extensions.

It is assumed that at the remote location, the phone will obtain other address information by DHCP from the user's router. If that is not the case, the other address setting for the phone will need to be statically administered to match addresses suitable for the user's home network.

Media Connection Preservation

Media Connection Preservation maintains calls that experience end-to-end signalling loss or refresh failures but that still have an active media path.

IP Phones:

The following Avaya H.323 phones attempt to maintain calls when the signal from the host IP Office is lost. The phones must be running the firmware release delivered with IP Office release 9.1 or higher.

- 9608
- 9611
- 9621
- 9641
- J169
- J179

When preserving a call, the phone does not attempt to reregister with their call server or attempt to failover to a standby call server, until the call has been terminated. Softkey call actions and feature menus do not work during this time due to the loss of signalling path. The phone display is not updated and the only permitted action is to terminate the call.

IP Office:

When enabled for a particular IP endpoint type that supports Media Connection Preservation, the call is put into a Preserved state and a Preservation Interval timer is started for that call at the point the signalling loss is detected. The maximum duration of a preserved call on IP Office is two hours. Once put into the Preserved state, a call can only transition to the Terminated state. Call restoration is not supported.

Only the following call types are preserved:

- Connected active calls
- Two party calls where the other end is a phone, trunk, or voicemail
- Conference calls
- Calls on hold and calls to hunt groups are not preserved.

Phone Display:

When a call is in a preserved state but the phone's local signalling connection with its host IP Office is still present, the phone call state display is prefixed with a warning icon. Hold, transfer, and conference actions are not available.

System Configuration

When enabled on **System Settings** > **System** > **Telephony**, Media Connection Preservation is applied at a system level to SCN trunks and Avaya H.323 phones that support connection preservation. All systems in a Small Community Network (SCN) must be enabled for end to end connection preservation to be supported.

When enabled on **System Settings** > **Line** > **Add/Edit Trunk Line** > **SIP Line** > **SIP Advanced**, Media Connection Preservation is applied to the SIP trunk. The value of connection preservation

on public SIP trunks is limited. Media Connection Preservation on public SIP trunks is not supported until tested with a specific service provider. Media Connection Preservation is disabled by default for SIP trunks.

When enabled on **System Settings** > **Line** > **Add/Edit Trunk Line** > **SM Line** > **Session Manager**, Media Connection Preservation is applied to Enterprise Branch deployments. Media Connection Preservation preserves only the media and not the call signaling on the SM Line. Media Connection Preservation does not include support for the Avaya Aura Session Manager Call Preservation feature.

Configuring ARS

When a dialed number matches a short code that specifies that the number should be dialled, there are two methods by which the routing of the outgoing call can be controlled.

Routing Calls Directly to a Line:

Every line and channel has an Outgoing Group ID setting. Several lines and channels can have belong to the same Outgoing Group ID. Within short codes that should be routed via a line within that group, the required Outgoing Group ID is specified in the short code's Line Group ID setting.

Routing Calls via ARS:

The short code for a number can specify an ARS form as the destination. The final routing of the call is then controlled by the setting available within that ARS form.

ARS Features

Secondary Dial Tone:

The first ARS form to which a call is routed can specify whether the caller should receive secondary dial tone.

Out of Service Routing:

ARS forms can be taken out of service, rerouting any calls to an alternate ARS form while out of service. This can be done through the configuration or using short codes.

Out of Hours Routing:

ARS forms can reroute calls to an alternate ARS form outside the hours defined by an associated time profile.

Priority Routing:

Alternate routes can be made available to users with sufficient priority if the initial routes specified in an ARS form are not available. For users with insufficient priority, a delay is applied before the alternate routes become available.

Line Types:

ARS can be used with all line types.

A SIP line is treated as busy and can follow alternate routes based on the SIP line setting **Call Initiation Timeout**. Previously a SIP line was only seen as busy if all the configured channels were in use.

IP lines use the NoUser Source Number setting **H.323SetupTimerNoLCR** to determine how long to wait for successful connection before treating the line as busy and following ARS alternate routing. This is set through the IP line option **Call Initiation Timeout**.

Multi-Site Network Calls:

Calls to multi-site extension numbers are always routed using the appropriate network trunk. ARS can be configured for multi-site network numbers but will only be used if the network call fails due to congestion or network failure.

Main Route:

The ARS form 50, named "Main" cannot be deleted. For defaulted systems it is used as a default route for outgoing calls.

Routing Calls to ARS

1. Create the ARS form.
2. Create the required system, user or user rights short code to match the user dialing.
    a. In the **Telephone Number** field, define the digits that will be used to match a short code in the ARS form.
    b. Use the **Line Group ID** field drop-down to select the ARS form required for routing the call.

Related links

Example ARS Operation on page 553
ARS Operation on page 554

Example ARS Operation

The simplest example for ARS operation are the settings applied to a defaulted system. These vary between U-Law systems and A-Law systems. For Server Edition systems refer to Server Edition Outgoing Call Routing.

A-Law Systems

This set of defaults is applied to A-Law systems, typically supplied to locales other than North America. The defaults allow any dialing that does not match an internal number to be routed off-switch as follows:

System Short Code - ?/Dial/./50:Main:

The default system short code ? will match any dialing for which no other user, user rights or system short code match is found. This short code is set to route all the digits dialed to ARS form 50.

ARS Form - 50:Main:

This form contains just a single short code.

?/Dial3K1/./0 This short code matches any digits passed to the ARS form. It then dials the digits out on the first available line within line group 0 (the default outgoing line group for all lines).

U-Law Systems

This set of defaults is applied to U-Law systems, typically supplied to locales in North America. The defaults route any dialing prefixed with a 9 to the ARS and secondary dial tone.

System Short Code - 9N/Dial/N/50:Main:

The default system short code 9N is used to match any dialing that is prefixed with a 9. It passes any digits following the 9 to ARS form 50.

ARS Form - 50:Main:

This form has secondary dial tone enabled. It contains a number of short codes which all pass any matching calls to the first available line within line group 0 (the default outgoing line group for all lines). Whilst all these short code route calls to the same destination, having them as separate items allows customization if required. The short codes are:

- **11/Dial Emergency/911/0** This short code matches an user dialing 911 for emergency services.
- **911/Dial Emergency/911/0** This short code matches an user dialing 9911 for emergency services.
- **0N;/Dial3K1/0N/0** This short code matches any international calls.
- **1N;/Dial3K1/1N/0** This short code matches any national calls.
- **XN;/Dial3K1/N/0** This short code matches 7 digit local numbers.
- **XXXXXXXXXX/Dial3K1/N/0** This short code matches 10 digit local numbers.

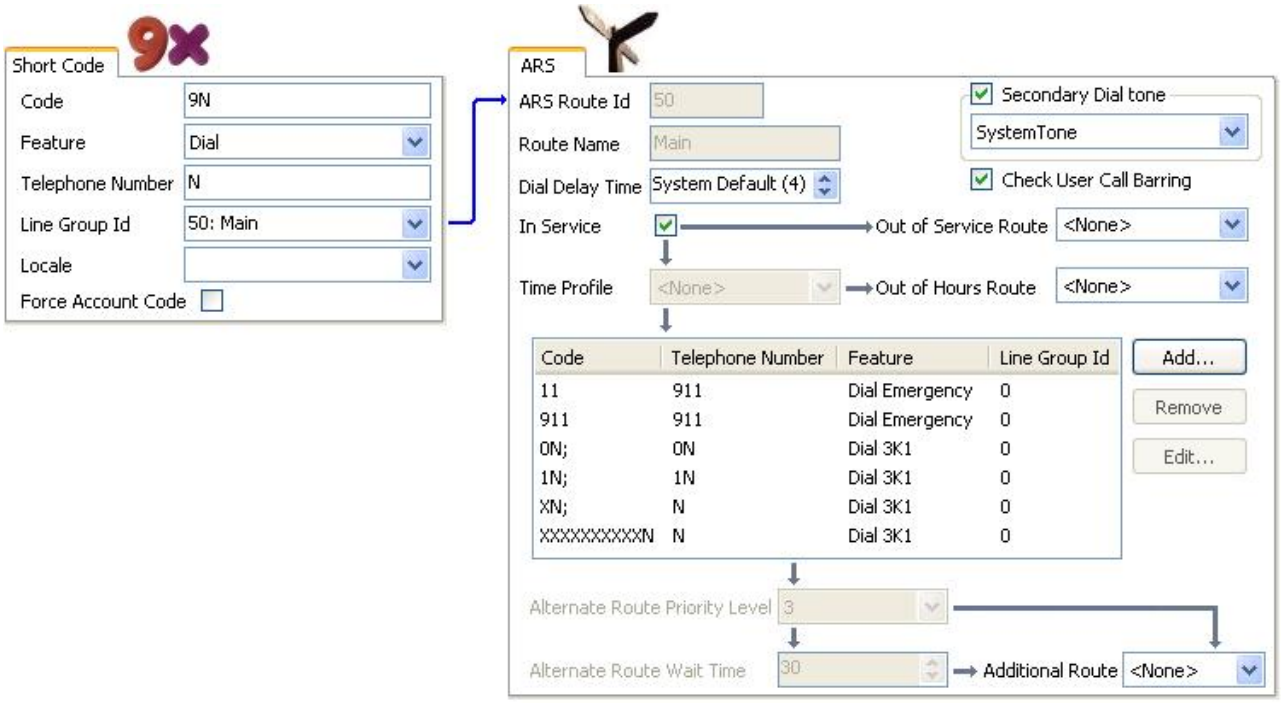
Related links

Configuring ARS on page 552

ARS Operation

The diagram below illustrates the default ARS routing applied to systems defaulted to the **United States** system locale. In summary:

- Any dialing prefixed with 9 will match the default system short code **9N**.
- That short code routes calls to the default ARS form **50:Main**.
- The short codes in that ARS form route all calls to an available line that has its **Outgoing Group ID** set to **0**.



The table describes in more detail the process that the system has applied to the user's dialing, in this example 91555707392200.

The user dials...	
9	The **Dial Delay Count** is zero, so the system begins looking for short code matches in the system and user's short codes immediately. Since there is only one match, the **9N** system short code, it is used immediately. The **9N** short code is set to route the call to the ARS form **Main**. It only passes those digits that match the N part of the dialing, ie. the 9 is not passed to the ARS, only any further digits dialed by the user. **Secondary Dial Tone** is selected in the ARS form. Since no digits for ARS short code matching have been received, secondary dial tone is played to the user.

Table continues…

1	Having received some digits, the secondary dial tone stops. The ARS form short codes are assessed for matches. The **11** and **1N;** short codes are possible matches. The **911** and **0N;** short codes are not possible matches. The **XN;** and **XXXXXXXXXXN;** short codes are also not matches because the **1N;** short code is already a more exact match. Since there is more than one possible match, the system waits for further digits to be dialed.
555	The **11** short code is no longer a possible match. The only match is left is the **1N;** short code. The **;** in the short code tells the system to wait for the **Dial Delay Time** to expire after the last digit it received before assuming that dialing has been completed. This is necessary for line providers that expect to receive all the routing digits for a call 'en bloc'. The user can also indicate they have completed dialing by pressing **#**.
707392200	When the dialing is completed, a line that has its **Outgoing Group ID** set to 0 (the default for any line) is seized. If no line is available, the alternate route settings would applied if they had been configured.

Related links

Configuring ARS on page 552
ARS Short Codes on page 556
Simple Alternate Line Example on page 558
Simple Call Barring on page 558
User Priority Escalation on page 559
Time Based Routing on page 560
Account Code Restriction on page 561
Tiered ARS Forms on page 562
Planning ARS on page 563

ARS Short Codes

The short codes in the default ARS form have the following roles:

Code	Feature	Telephone Number	Line Group ID	Description

Table continues…

11	**Dial Emergency**	**911**	**0**	These two short codes are used to route emergency calls. A **Dial Emergency** call is never blocked. If the required line is not available, the system will use the first available line. Similarly, calls using **Dial Emergency** ignore any outgoing call bar settings that would be normally applied to the user.
911	**Dial Emergency**	**911**	**0**	
0N;	**Dial 3K1**	**0N**	**0**	Matches international numbers.
1N;	**Dial 3K1**	**1N**	**0**	Matches national numbers.
XN;	**Dial 3K1**	**N**	**0**	Matches 7 digit local numbers.
XXXXXXXXXN;	**Dial 3K1**	**N**	**0**	Matches 10 digit local numbers.

ARS Short Code Settings

Code The digits used for matching to the user dialing.

Feature ARS short codes can use any of the **Dial** short code features or the **Barred** feature. When a **Barred** short code is matched, the call will not proceed any further.

Telephone Number The number that will be output to the line as the result of the short code being used as the match for the user dialing. Short code characters can be used such as N to match any digits dialed for N or X in the **Code**.

Line Group ID The line group from which a line should be seized once short code matching is completed. Another ARS form can also be specified as the destination.

Locale Not used for outgoing external calls.

Forced Account Code If enabled, the user will be prompted to enter a valid account code before the call can continue. The account code must match one set in the system configuration.

Related links

ARS Operation on page 554

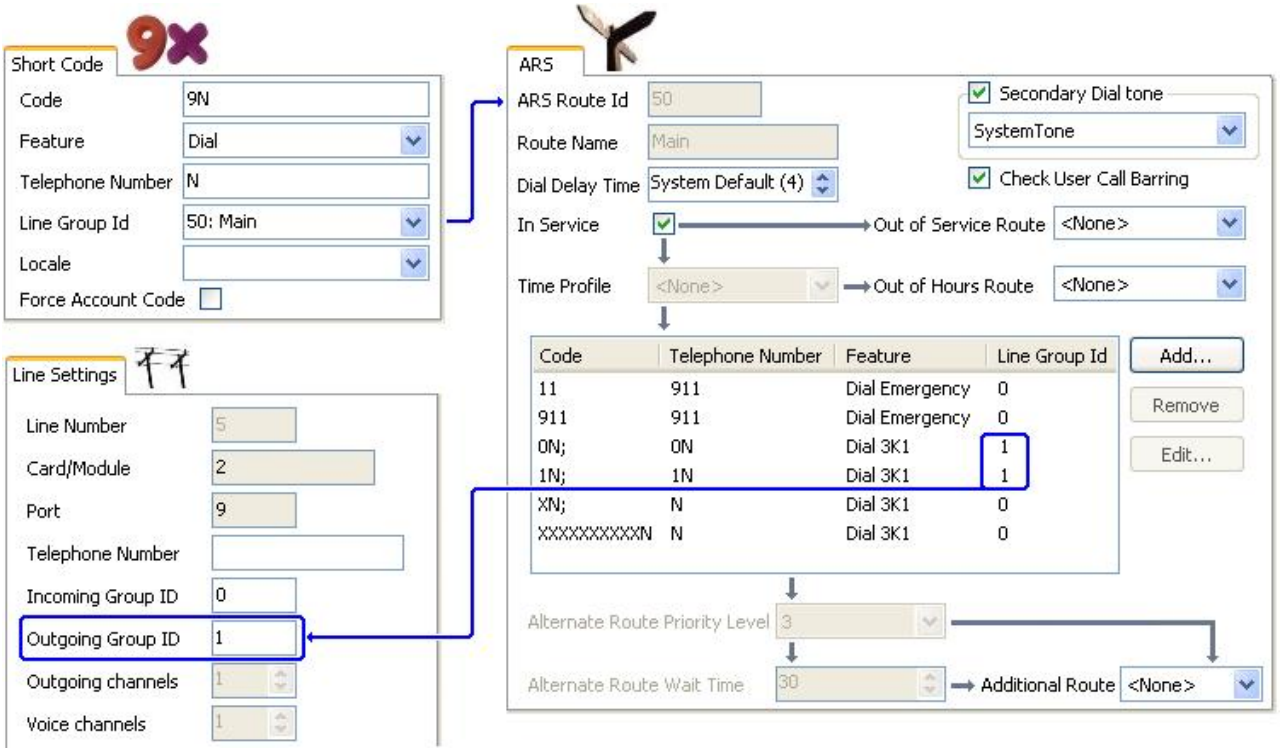
Simple Alternate Line Example

Using the default ARS settings, despite having several short codes in the ARS form, all outgoing calls are actually routed the same way using the same trunks. However, by having separate short codes for different call types present, it is easy to change the routing of each call type if required.

For this example, the customer has separate sets of lines for local calls and for national/ international calls. These have been configured as follows:

- The lines for local and emergency calls have been left with the default **Outgoing Group ID** of **0**.
- The lines for national and international calls have been set with the **Outgoing Group ID** of **1**.

The default ARS can be configured to match this by just changing the **Line Group ID** settings of the default ARS short codes to match.



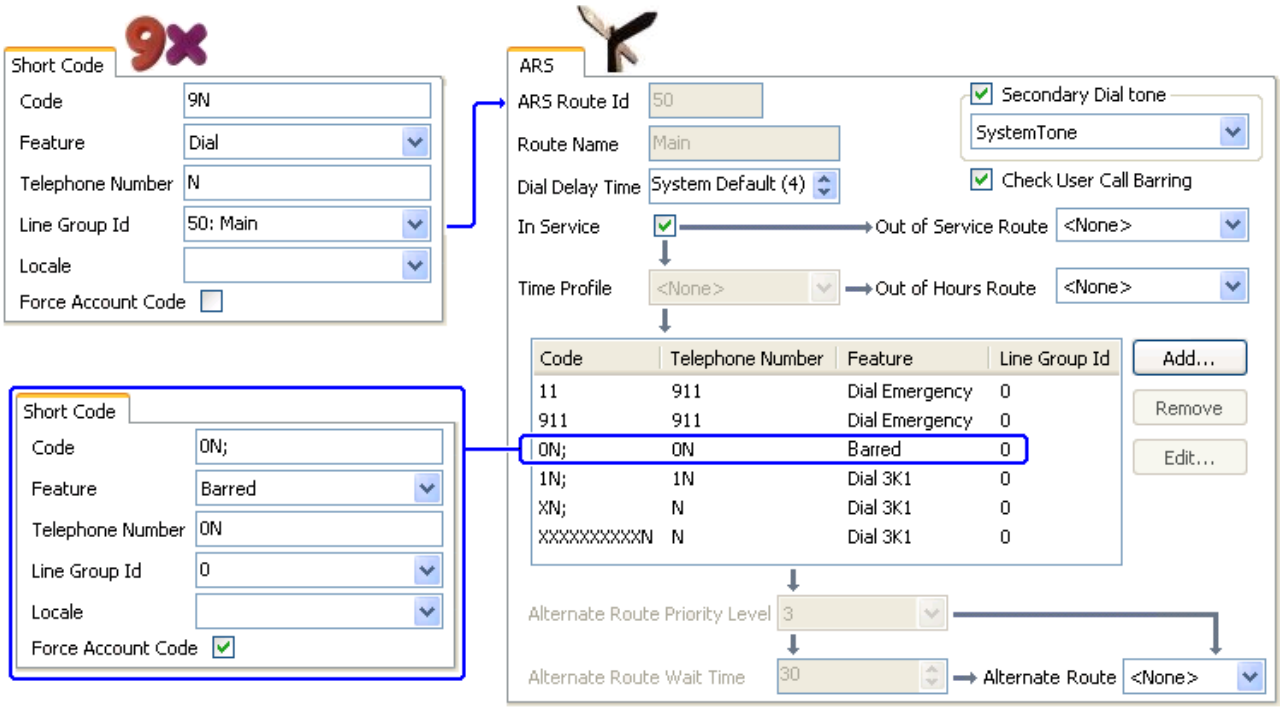
Related links

ARS Operation on page 554

Simple Call Barring

All ARS short codes use one of the **Dial** short code features. The exception is the **Barred** short code feature. This can be selected for ARS short codes that match dialing that is not allowed.

In the example below, any user dialing an international number will be routed to the **Barred** short code. This prevents the dialing of external numbers prefixed with 0.



To restrict a user from making any outgoing external calls, use the user's Outgoing Call Bar option.

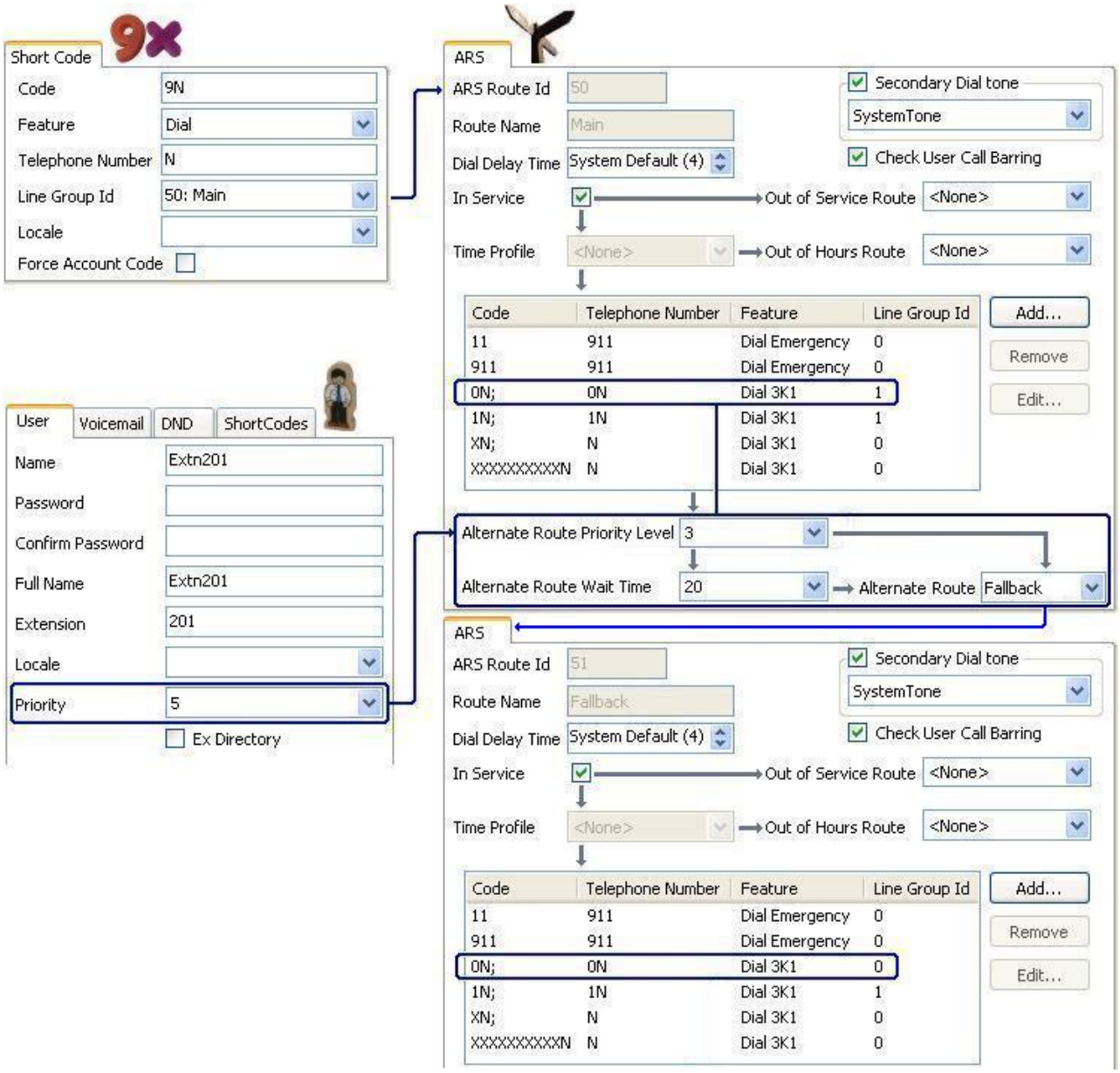
Related links

ARS Operation on page 554

User Priority Escalation

User priority can be used to alter call routing when the required route is not available.

In this example, international calls are initially targeted to seize a line in outgoing line group 1. However an alternate route has been defined which will be used if no line in line group 1 is available. The fallback ARS form allows international calls to seize a line from line group 0. Whether this is done immediately or after a delay is set by whether the users priority is high enough.



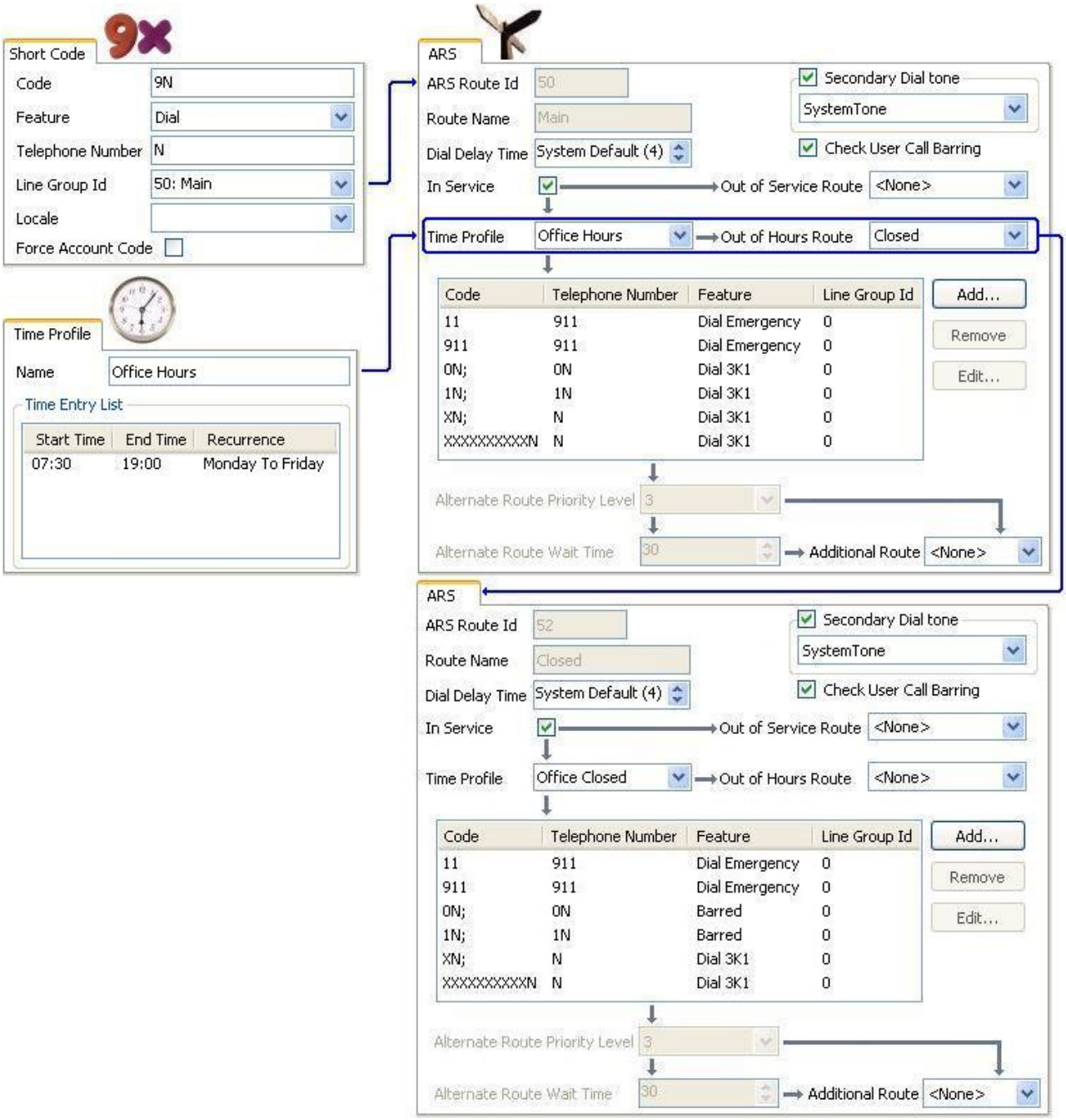
Related links

ARS Operation on page 554

Time Based Routing

Time profiles can be used to switch call routing from one ARS form to another.

In the example below, a time profile has been define that sets the hours for normal operation. Outside the times set in the time profile, the other ARS form is used. This other ARS form only allows local and emergency calls.



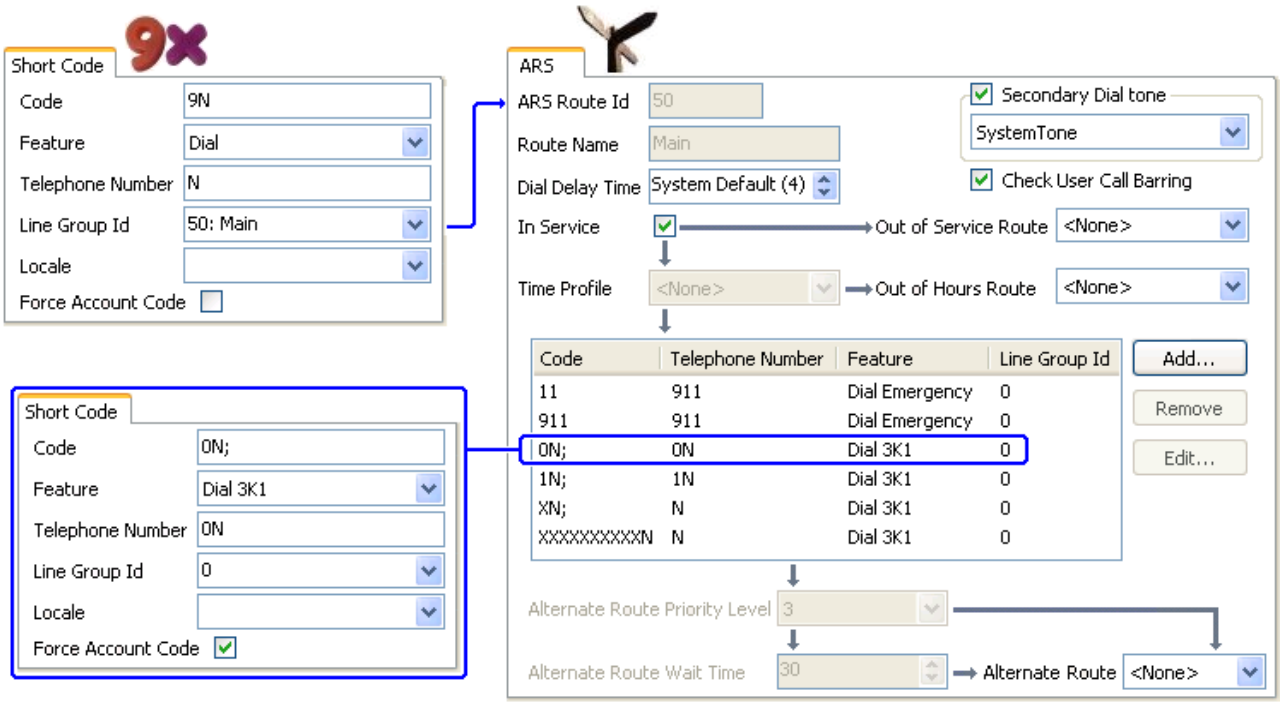
Related links

ARS Operation on page 554

Account Code Restriction

The short codes within an ARS form can be individually set to require an account code before allowing any call that matches it to proceed.

In the example below, the short code for international calls has been set to require the user to enter an account code. A valid account code must be dialed to continue with the call.



If a user should always enter an account code to make any external call, the user option Force Account Code should be used.

Related links

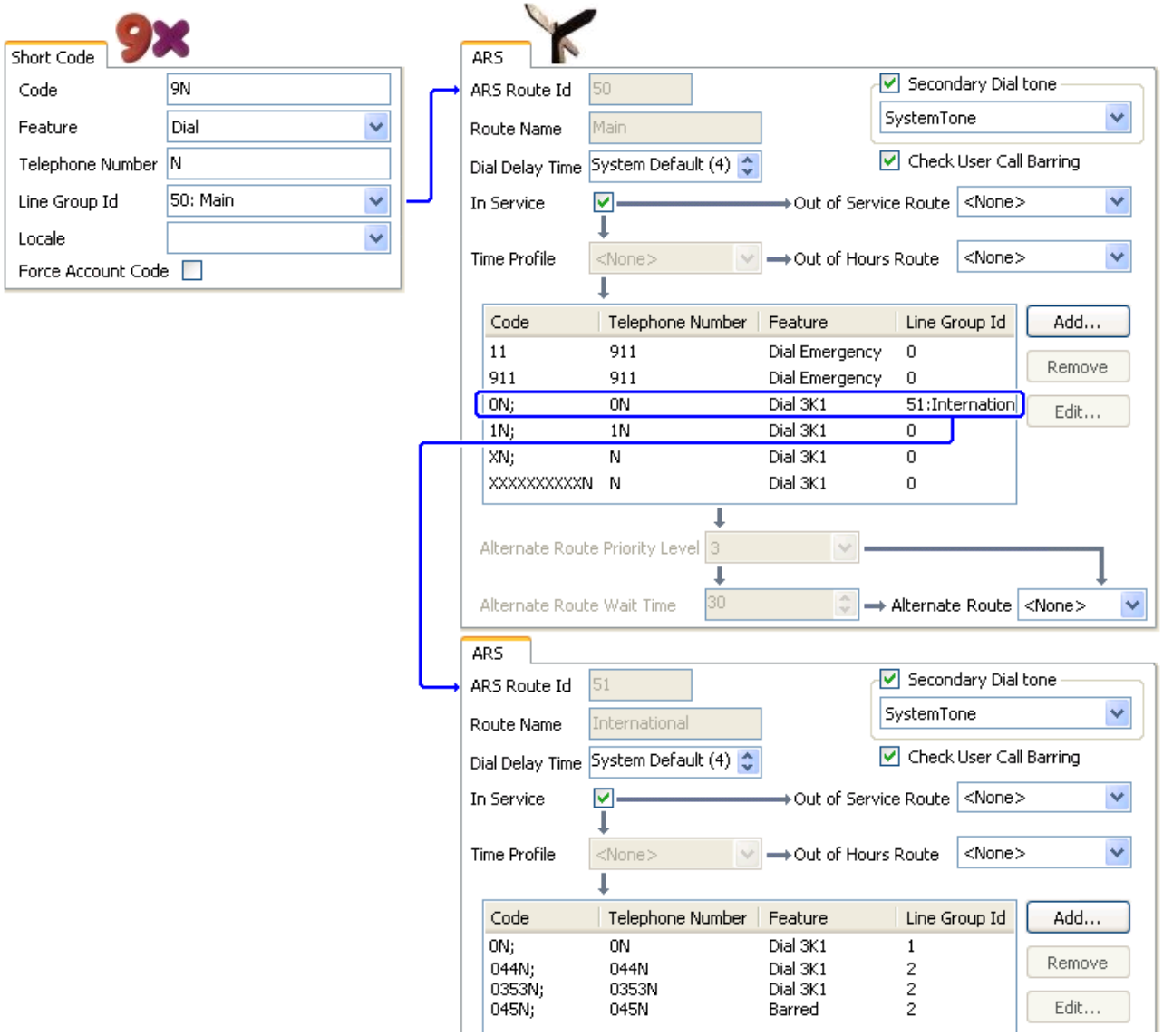
ARS Operation on page 554

Tiered ARS Forms

It is possible for an ARS short code in one form to have another ARS form as its destination. Dialing that matches the short code is then subject to further matching against the short codes in the other ARS form.

In the example below, the user wants different routing applied to international calls based on the country code dialed. To do that in the default ARS form would introduce a large number of short codes in the one form, making maintenance difficult.

So the short code matching calls with the international dialing prefix 0 has been set to route matching calls to another ARS form. That form contains short codes for the different country dialing codes of interest plus a default for any others.



Related links

ARS Operation on page 554

Planning ARS

Using the methods shown in the previous examples, it is possible to achieve ARS that meets most requirements. However the key to a good ARS implementation is planning.

A number of questions need to be assessed and answered to match the system's call routing to the customer's dialing.

What What numbers will be dialed and what needs to be output by the system. What are the different call tariffs and the dialing codes.

Where Where should calls be routed.

Who Which users should be allowed to use the call routes determined by the previous questions.

When When should outgoing external calls be allowed. Should barring be applied at any particular times? Does the routing of calls need to be adjusted for reasons such as time dependant call tariffs.

Related links

ARS Operation on page 554

Configuring IP Routes

The system acts as the default gateway for its DHCP clients. It can also be specified as the default gateway for devices with static IP addresses on the same subnet as the system. When devices want to send data to IP addresses on different subnets, they will send that data to the system as their default gateway for onward routing.

The IP Route table is used by the system to determine where data traffic should be forwarded. This is done by matching details of the destination IP address to IP Route records and then using the Destination specified by the matching IP route. These are referred to as 'static routes'.

Automatic Routing (RIP): The system can support RIP (Routing Information Protocol) on LAN1 and or LAN2. This is a method through which the system can automatically learn routes for data traffic from other routers that also support matching RIP options, see RIP. These are referred to as 'dynamic routes'. This option is not supported on Linux based servers.

Dynamic versus Static Routes: By default, static routes entered into the system override any dynamic routes it learns by the use of RIP. This behavior is controlled by the Favor RIP Routes over static routes option on the **System | System** tab.

Static IP Route Destinations: The system allows the following to be used as the destinations for IP routes:

- **LAN1** Direct the traffic to the system's LAN1.
- **LAN2** Traffic can be directed to LAN2.
- **Service** Traffic can be directed to a service. The service defines the details necessary to connect to a remote data service.
- **Tunnel** Traffic can be directed to an IPSec or L2TP tunnel.

Default Route: The system provides two methods of defining a default route for IP traffic that does not match any other specified routes. Use either of the following methods:

- **Default Service** Within the settings for services, one service can be set as the **Default Route** (**Service | Service**).
- **Default IP Route** Create an IP Route record with a blank IP Address and blank IP Mask set to the required destination for default traffic.

RIP Dynamic Routing common

Routing Information Protocol (RIP) is a protocol which allows routers within a network to exchange routes of which they are aware approximately every 30 seconds. Through this process, each router adds devices and routes in the network to its routing table.

Each router to router link is called a 'hop' and routes of up to 15 hops are created in the routing tables. When more than one route to a destination exists, the route with the lowest metric (number of hops) is added to the routing table.

When an existing route becomes unavailable, after 5 minutes it is marked as requiring 'infinite' (16 hops). It is then advertised as such to other routers for the next few updates before being removed from the routing table. The system also uses 'split horizon' and 'poison reverse'.

RIP is a simple method for automatic route sharing and updating within small homogeneous networks. It allows alternate routes to be advertised when an existing route fails. Within a large network the exchange of routing information every 30 seconds can create excessive traffic. In addition the routing table held by each system is limited to 100 routes (including static and internal routes).

It can be enabled on LAN1, LAN2 and individual services. The normal default is for RIP to be disabled.

- **Listen Only (Passive)**: The system listens to RIP1 and RIP2 messages and uses these to update its routing table. However the system does not respond.
- **RIP1:** The system listens to RIP1 and RIP2 messages. It advertises its own routes in a RIP1 sub-network broadcast.
- **RIP2 Broadcast (RIP1 Compatibility)**: The system listens to RIP1 and RIP2 messages. It advertises its own routes in a RIP2 sub-network broadcast. This method is compatible with RIP1 routers.
- **RIP2 Multicast**: The system listens to RIP1 and RIP2 messages. It advertises its own routes to the RIP2 multicast address (249.0.0.0). This method is not compatible with RIP1 routers.

Broadcast and multicast routes (those with addresses such as 255.255.255.255 and 224.0.0.0) are not included in RIP broadcasts. Static routes (those in the IP Route table) take precedence over a RIP route when the two routes have the same metric.

Creating a Virtual WAN Port

Procedure

1. Select  **WAN Port**.
2. Click  and select **PPP**.
3. In the **Name** field, enter either **LINEx.y** where:
   - **LINE** must be in uppercase.
   - **x** is the line number. For a PRI/T1 module in Slot A, this will be 1. For a PRI/T1 module in Slot B, this will be 5.
   - **y** is the lowest numbered channel number to be used by the WAN link minus 1. For example, if the lowest channel to be used is channel 1 then y = 1 - 1 = 0.
4. In the **Speed** field, enter the total combined speed of the maximum number of channels sets in the Service.

In this example, 12 channels x 64000 bits = 76800.

Note:

The maximum number of channels that can be used will be limited by the number of data channels supported by the system Control Unit and not already in use.

5. In the **RAS Name** field, select the RAS name created when the new Service of that name was created.
6. Click **OK**.

System Events

The system supports a number of methods by which events occurring on the system can be reported. These are in addition to the real-time and historical reports available through the System Status Application (SSA).

SNMP Reporting

Simple Network Management Protocol (SNMP) allows SNMP clients and servers to exchange information. SNMP clients are built into devices such as network routers, server PC's, etc. SNMP servers are typically PC application which receive and/or request SNMP information. The system SNMP client allows the system to respond to SNMP polling and to send alarm information to SNMP servers.

In order for an SNMP server application to interact with a system, the MIB files provided with the Manager installation software must be compiled into the SNMP server's applications database.

Note:

The process of 'on-boarding' (refer to the IP Office Installation manual and the IP Office SSL VPN Solutions Guide) may automatically configure SNMP and create a number of SNMP alarm traps. These will override any existing SNMP configuration settings.

SMTP Email Reporting

The system can send alarms to an SMTP email server. Using SMTP requires details of a valid SMTP email account user name and password and server address. If SMTP email alarms are configured but for some reason the system cannot connect with the SMTP server, only the last 10 alarms are stored for sending when connection is successful. Use of SMTP alarms requires the SMTP server details to be entered in the SMTP tab.

Syslog Reporting

The system can also send alarms to a Syslog server (RFC 3164) without needing to configure an SNMP server. In addition Syslog output can include audit trail events.

Multiple event destinations can be created, each specifying which events and alarms to include, the method of reporting to use (SNMP, Syslog or Email) and where to send the events. Up to 2 alarm destinations can be configured for SNMP, 2 for Syslog and 3 for SMTP email.

Related links

Configuring Alarm Destinations on page 567

Configuring Alarm Destinations

About this task

The Alarms section of the System Events tab displays the currently created alarm traps. It shows the event destinations and the types of alarms that will trigger the send of event reports. Up to 2 alarm destinations can be configured for SNMP, 2 for Syslog and 3 for SMTP email.

Procedure

1. In the navigation pane, select **System**.
2. In the details pane, select **System Events** and then select the **Alarms** sub-tab.
3. Use the **Add**, **Remove** and **Edit** controls to alter the traps.
4. Click **Add** or select the alarm to alter and then click **Edit**.
5. For a new alarm, set the **Destination** to either **Trap (SNMP)** or **Syslog** or **Email (SMTP)**.

   Note that once a destination has been saved by clicking **OK** it cannot be changed to another sending mode.
6. The remaining details will indicate the required destination information and allow selection of the alarm events to include.
7. When completed, click **OK**.
8. Click **OK**again.

Related links

System Events on page 566

Configuring authorization codes

Note:

In release 9.1, authorization codes can no longer be associated with User Rights. If an authorization code was configured in relationship with User Rights in an earlier release configuration, this authorization code will be lost during upgrade. The administrator must re-configure the authorization code, after upgrade. The authorization code must be associated with a user.

Authorization codes are enabled by default.

A user dials a number that matches a short code set to **Force Authorization Code**. The user is prompted to enter an authorization code.

They dial their authorization code. If a matching entry is found in **Authorization Codes** records the system checks the corresponding user. Note that the user checked does not necessarily need to be connected with the user dialing or the user whose extension is being used to make the call.

The dial string is checked against the short codes with the matching user. If it matches a dial short code or no short code the call is allowed, otherwise it is blocked. Note that the short code is not processed, it is just checked for a match. If multi-tier authorization codes are required there must be blocking (busy) short codes (or a wild card '?')

Example:

A restaurant has a number of phones in publicly accessible areas and want to control what calls can be made by staff. Staff must not be able to dial long distance numbers. staff should be able to dial local and cell phone numbers.

ARS Table
In the Main (50) ARS table, add the following short codes: • 044XXXXXXXXX/Dial/044N/ • 01XXXXXXXXX/Dial/01N/Force Auth Code checked
Authorization Codes
Configure an authorization code for each staff member that is allowed to make long distance calls. For example, for staff members Alice and Bob: AuthCode: **2008 - Alice** AuthCode: **1983 - Bob**

It is recommended to use short codes that use X characters to match the full number of characters to be dialed. That ensures that authorization code entry is not triggered until the full number has been dialed rather than mid-dialing. For example 09 numbers are premium rate in the UK, so you would create a **09XXXXXXXX/Dial/N** short code set to Forced Authorization. In the associated user or user right short code it is recommended to use 09N type short codes.

System short codes that route to ARS will not have their **Force Authorization Code** setting used. However short codes within an ARS table will have their **Force Authorization** Code setting used.

Forcing Authorization Codes

There are two methods to force a user to enter an authorization code in order to complete dialing an external call.

- **To Force Authorization Codes on All External Calls** A user can be required to enter an authorization code for all external calls. This is done by selecting Force Authorization Code (**User | Telephony | Supervisor Settings**).
- **To Force Authorization Codes on Specific Calls** To require entry of an authorization code on a particular call or call type, the Force Authorization Code option should be selected in the short code settings. This can be used in user or system short codes in order to apply its effect to a user or all users respectively. You need to ensure that the user cannot dial the same number by any other method that would by pass the short code, for example with a different prefix.

Related links

Entering an Authorization Code on page 569

Entering an Authorization Code

Where possible, when an authorization code is required, the user can enter it through their phones display. However, this is not possible for all type of phone, for example it is not possible with analog phones and Avaya XX01 or XX02 phones. The users of these device must either enter the authorization code using a short code set to the Set Authorization Code feature immediately before making the call.

When entry of an authorization code is triggered, the user can enter any authorization code with which they are directly associated.

Note the following.

- If authorization code entry is setup for a particular number, calls forwarded or transferred to that number will also trigger authorization code entry.
- On systems using line appearances to BRI trunk channels to make outgoing calls, authorization code entry may not be triggered. This can be resolved by adding a short code such as [9]XN;/Dial/XN/0 (adjust the prefix and line group as necessary).

Related links

Configuring authorization codes on page 567

Preventing Toll Bypass

Use this procedure to prevent toll bypass in Enterprise Branch and Small Community Network (SCN) deployments. Toll bypass is prevented by only allowing PSTN calls where the originating location and terminating location are the same.

The location of non-IP lines is the same as the system location. If an IP address is not resolved to any location, then that device is assumed to be in the system location. The location of public IP lines must be configured to same as PSTN termination location.

The **Location** field for extensions with simultaneous login must be automatic and the location tab must be properly configured for the IP range.

Enterprise Branch deployments: All the distributed users must be in the same location as system location. Users registering from a location different from the system location are not supported.

Procedure

1. In the navigation pane on the left, select **System**.
2. In the details pane, click the **Telephony** tab.
3. Under **Telephony**, click the **Telephony** tab.

4. On the **Telephony** tab:
   a. Click the check box to turn **Restrict Network Interconnect** on.
   b. Click the check box to turn **Include location specific information** on.

      Setting the two configuration setting on the **Telephony** tab adds a **Network Type** field to the configuration settings for each trunk.
5. For Enterprise Branch deployments, open the **SM Line | Session Manager** tab. For SCN deployments, open the **IP Office Line | Line** tab.
6. If the line is a PSTN trunk (includes SIP), set **Network Type** to **Public**. If the line is an enterprise trunk, set the **Network Type** to **Private**.
7. If the **Network Type** is **Private**, the **Include location specific information** field is available.

   If the line is connected to an Avaya Aura® system release 7.0 or higher, or an IP Office release 9.1 or higher, set **Include location specific information** to **On**.

Configuring unknown locations

Use this procedure to configure extensions where the location is unknown.

Procedure

1. In the navigation pane, select **Location**.
2. Enter **a Location Name**.
3. Set **Parent Location for CAC** to **Cloud**.
4. In the **Extension | Extn** tab, set the **Location** field to the location defined in step 2.

Call Barring

Related links

Applying Call Barring on page 570
Overriding call barring on page 571

Applying Call Barring

Call barring can be applied in a number of ways.

Barring a User From Receiving Any External Calls:

For each user, the **Incoming Call Bar** setting (**User | Telephony | Supervisor Settings**) can be selected to stop that user from receiving any external calls.

Barring a User From Making Any External Calls:

For each user, the **Outgoing Call Bar** setting (**User | Telephony | Supervisor Settings**) can be selected to stop that user from making any external calls.

Barring Particular Numbers/Number Types:

System short codes are used to match user dialing and then perform a specified action. Typically the action would be to dial the number to an external line. However, short codes that match the dialing of particular numbers or types of numbers can be added and set to another function such as Busy. Those short codes can be added to a particular user, to a User Rights associated with several users or to the system short codes used by all users.

The system allows short codes to be set at user, user rights, system and least cost route. These have a hierarchy of operation which can be used to achieve various results. For example a system short code for a particular number can be set to busy to bar dialing of that number. For a specific user, a user short code match to the same number but set to Dial will allow that user to override the system short code barring.

Using Account Codes:

The system configuration can include a list of account codes. These can be used to restrict external dialing only to users who have entered a valid account code.

- **Forcing Account Code Entry for a User**: A user can be required to enter an account code before the system will return dialing tone. The account code that they enter must match a valid account code stored in the system configuration. The setting for this is **Force Account Code** (**User | Telephony | Supervisor Settings**)
- **Forcing Account Code Entry for Particular Numbers**: Each system short code has a Force Account Code option. Again the account code entered must match a valid account code stored in the system configuration. for the call to continue.

Barring External Transfers and Forwards:

A user cannot forward or transfer calls to a number which they cannot normally dial. In addition there are controls which restrict the forwarding or transferring of external calls back off-switch. See Off-Switch Transfer Restrictions on page 643.

Related links

Call Barring on page 570

Overriding call barring

When a system or user short code is configured to bar outgoing calls, you can override call barring. Typically, this configuration is used for a phone in a shared or public area. By default, the phone has outgoing calls barred. The administrator can override call barring for specific dialed numbers by entering numbers with a record in the external directory. When the dialed number exists in the external directory and the **Directory Overrides Call Barring** setting is enabled, call barring is overridden.

The System Directory entries must use the format (shortcode)number. For example, if the number to dial is 61234, where 6 is the shortcode used to dial externally and 1234 is the number, the System Directory entry must be (6)1234. If the dial shortcode contains a name string rather than digits, then **Directory Overrides Call Barring** will not work.

The **Directory Overrides Barring** setting is located on the **System | Telephony | Telephony** tab.

For information on the directory, see the description for the **System | Directory Services** tab.

Server Edition configuration

For Server Edition deployments, the **Directory Overrides Barring** must be enabled on each node. It is not a system wide setting.

For example, if the Primary Server uses an IP500 V2 expansion system as an ISDN gateway, **Directory Overrides Barring** must be enabled on the Primary Sever for Primary Server users dialing on external ISDN lines. For the IP500 V2 expansion users, **Directory Overrides Barring** must be enabled on the IP500 V2 expansion system.

It is recommend that the short code configured to dial externally on ISDN lines be the same on all nodes. For example, if Primary Server users and IP500 V2 expansion users want to reach PSTN number 123456789 on ISDN lines, configure the dial codes as follows.

- Primary Server: 6N/Dial/6N/XX (XX is the line group ID for the SCN line)
- IP500 V2 expansion: 6N/Dial/N/YY (YY is the line group ID for ISDN line)
- Directory Entry number defined on Primary Server: (6)123456789

Related links

Call Barring on page 570

Chapter 11: Configure User Settings

Related links

User Management Overview

Users are the people who use the system. They do not necessary have to be an extension user, for example users are used for RAS dial in data access. In addition, more users can be created than there are extensions, with users logging in to an extension when they want to receive calls.

By default, a user is automatically created to match each extension. They are numbered from 201 upwards and the first 16 are placed in the hunt group Main (200), which is the default destination for incoming calls.

Terminology

Standard User: A standard user.

Centralized User: Centralized users can be provisioned for enterprise branch deployments.

No User: Used to apply settings for extensions which currently have no associated user. The **SourceNumbers** settings of the **NoUser** user is used to configure a number of special options. These are then applied to all users on the system.

Remote Manager: Used as the default settings for dial in user connections.

Hot Desking User: Users with a Login Code can move between extensions by logging in and off.

Deleting a User

When a user is deleted, any calls in progress continue until completed. The ownership of the call is shown as the NoUser user. Merging the deletion of a user causes all references to that deleted user to be removed from the system.

Changing a User's Extension

Changing a user's extension number automatically logs the user in on the matching base extension if available and the user doesn't have Forced Login enabled. If **Forced Login** is enabled, then the user remains on the current extension being used until they log out and log in at the new extension.

Note that changing a user's extension number affects the user's ability to collect Voicemail messages from their own extension. Each user's extension is set up as a "trusted location" under the Source Numbers tab of the User configuration form. This "trusted location" allows the user to dial *17 to collect Voicemail from his own extension. Therefore if the extension number is changed so must the "trusted location".

The following related configuration items are automatically updated when a user extension is changed:

- User, Coverage and Bridged Appearance buttons associated with the user.
- Hunt group membership (disabled membership state is maintained).
- Forwards and Follow Me's set to the user as the destination.
- Incoming call routes to this destination.
- Dial in source numbers for access to the user's own voicemail.
- Direct call pickup buttons are updated.
- The extension number of an associated extension is updated.

Server Edition User Management

In a Server Edition network, individual users are still added to the configuration of a particular server. Typically they are added to the configuration of the server that hosts the user's physical extension or supports their main place of work. That server is treated as the host system for the user. However, once a user is added to the configuration of a particular system, you can use Manager and Web Manager to manage all users in the Server Edition solution.

Centralized User Management

Centralized Users are provisioned for enterprise branch deployments. **Centralized Users** are registered with Session Manager and are able to utilize telephony features provided by Communication Manager. The **Centralized User** profile is applicable to both SIP and analogue extensions. For more information, see *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*. The following requirements must be met when provisioning a centralized user:

- An SM line must be configured on the system.
- The user must be provisioned with an existing extension.
- The extension **Base Extension** value must match the centralized extension value.
- Centralized users must be configured with a password for SIP registration on Session Manager. The password is set in User | Telephony | Supervisor Settings | Login Code field.

Related links

Configure User Settings on page 573

Configuring User Rights

For most settings in a user rights template, the adjacent drop down list is used to indicate whether the setting is part of the template or not. The drop down options are:

- **Apply User Rights Value** Apply the value set in the user rights template to all users associated with the template.
  - The matching user setting is grayed out and displays a lock symbol.
  - Users attempting to change the settings using short codes receive inaccessible tone.
- **Not Part of User Rights** Ignore the user rights template setting.

Default User Rights

For defaulted systems, the following user rights are created as a part of the default configuration. Fields not listed are not part of the user rights.

Note:

When a user logs in as a Outbound Contact Express agent, the Outdialer user rights are automatically applied. When the agent logs out, the previous user rights are applied.

✓ = Set to On. ✗ = Set to Off. – = Not part of the user rights.

User Rights	Call Center Agent	Boss	Application	Default	IP Hard Phone	Mailbox	Paging	T3	Outdialer
Priority	✓ 5	✓ 5	✓ 5	✓ 5	✓ 5	✓ 5	✓ 5	✓ 5	✓ 5
Voicemail	–	–	–	–	–	✓	–	–	✗

Table continues…

User Rights	Call Center Agent	Boss	Application	Default	IP Hard Phone	Mailbox	Paging	T3	Outdialer
Voicemail Ringback	✗	✗	✗	✗	✗	✗	–	✗	✗
Outgoing Call Bar	✗	✗	✗	✗	✗	✗	✗	✗	✓
No Answer Time	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	0
Transfer Return Time	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	0
Individual Coverage Time	✓ 10	✓ 10	✓ 10	✓ 10	✓ 10	✓ 10	✓ 10	✓ 10	10
Busy on Held	✗	✗	✗	✗	✗	–	–	✗	✓
Call Waiting	✗	✗	✓	✗	✗	✗	✗	✓	✗
Can Intrude	✗	✗	✗	✗	✗	✗	✗	✗	✗
Cannot be Intruded	✗	✗	✓	✓	✓	✗	✗	✗	✗
Deny Auto Intercom Calls	–	–	–	–	–	–	–	–	✗
Enable Inhibit Off-Switch Forward / Transfer	–	–	–	–	–	–	–	–	✓
Enable Outgoing Call Bar	–	–	–	–	–	–	–	–	✓

Table continues…

User Rights	Call Center Agent	Boss	Application	Default	IP Hard Phone	Mailbox	Paging	T3	Outdialer
Centralized Logging	-	-	-	-	-	-	-	-	✗
Force Login	✓	-	-	-	-	-	-	-	
Force Account Code	✗	✗	✗	✗	✗	✗	✗	✗	
Button Programming	1: a= 2: b= 4: HGEna 5: DNDOn 6: Busy	1: a= 2: b= 3: c= 6: DNDOn 7: Dial *17	✓	1: a= 2: b= 3: c=	1: a= 2: b= 3: c= 6: Dial *17	✓	-	✓	1: a= 2: b= 3: Supervisor 4: Extn Logout

Related links

Configure User Settings on page 573
Adding User Rights on page 577
Creating a User Right Based on an Existing User on page 578
Associating User Rights to a User on page 578
Copy User Rights Settings over a User's Settings on page 578

Adding User Rights

About this task

Procedure

1. Select  **User Rights**.
2. Click  and select **User Rights**.
3. Enter a name.
4. Configure the user rights as required.
5. Click **OK**.

Related links

Configuring User Rights on page 575

Creating a User Right Based on an Existing User

About this task

Procedure

1. Select  **User Rights**.
2. In the group pane, right-click and select **New User Rights from a User**.
3. Select the user and click **OK**.

Related links

Configuring User Rights on page 575

Associating User Rights to a User

About this task

Procedure

1. Select  **User Rights** or  **User**.
2. In the group pane, right-click and select **Apply User Rights to Users**.
3. Select the user rights to be applied.
4. On the **Members of this User Rights** sub tab select the users to which the user rights should be applied as their Working Hours User Rights.
5. On the **Members when out of hours** sub tab select which users should use the selected user rights as their out of hours user rights.
6. Click **OK**.

Related links

Configuring User Rights on page 575

Copy User Rights Settings over a User's Settings

About this task

This process replaces a user's current settings with those that are part of the selected user rights. It does not associate the user with the user rights.

Procedure

1. Select  **User Rights**.
2. In the group pane, right-click and select **Copy user rights values to users**.

3. Select the user rights to be applied.
4. Click **OK**.

Related links

Configuring User Rights on page 575

Managing Users with LDAP

Lightweight Directory Access Protocol (LDAP) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the internet or on a corporate intranet. IP Office supports LDAP v2 compliant directory services servers.

LDAP synchronization allows an administrator to quickly configure the IP Office system with users and extensions for the users based on an organization's LDAP directory. An LDAP directory is organized in a simple tree consisting of the following hierarchy of levels:

1. The root directory (the starting place or the source of the tree)
2. Countries
3. Organizations
4. Organizational units (divisions, departments, etc.)
5. Individuals (which includes people, files, and shared resources, for example printers)

An LDAP directory can be distributed among many servers. Each server can have a replicated version of the total directory that is synchronized periodically. An LDAP server is called a Directory System Agent (DSA). An LDAP server that receives a request from a user takes responsibility for the request, passing it to other DSA's as necessary, but ensuring a single coordinated response for the user.

Related links

Configure User Settings on page 573
LDAP Synchronization on page 579

LDAP Synchronization

LDAP directory synchronization allows the IP Office telephone number directory to be synchronized with the information on an LDAP server. IP Office interoperate with any server that supports LDAP Version 2.

This feature is only supported by Server Edition Select systems. LDAP synchronization is performed using Web Manager.

Swapping of extensions between Users is not supported through Web Manager. The IP Office system displays an error message `Extension conflicts` in the LDAP User Sync Summary report if you try to swap extension numbers between Users on the LDAP server and perform synchronization through Web Manager.

Related links

Managing Users with LDAP on page 579
Performing LDAP Synchronization on page 580
Creating a User Provisioning Rule for LDAP Synchronization on page 580

Performing LDAP Synchronization

Procedure

1. In Web Manager, navigate to the page **Solution** > **Solution Settings** > **User Synchronization Using LDAP** > **Connect to Directory Service**.
2. Define the connection to the LDAP server and to define the parameters for searching the LDAP directory. All fields are mandatory.
3. Click **Test Connection**.

   Web Manager attempts to connect to the LDAP server with the specified credentials.
4. Click **Synchronize User Fields**.
5. Map the IP Office user fields to the LDAP fields. Not all fields are mandatory.

   Note:

   You must click **Test Connection** on the **Connect to Directory Service** page to populate the LDAP fields on the **Synchronize User Fields** page.
6. Click **Preview Results** and review the list in the Preview Results window.
7. Click **Synchronize**.

   The User Synchronization window opens. Click the information icon to open a detailed report.

Related links

LDAP Synchronization on page 579

Creating a User Provisioning Rule for LDAP Synchronization

A user provisioning rule (UPR) provides a way to manage the users to be imported. A UPR can provide the following properties for importing users.

- the IP Office system where the users are created
- starting extension
- extension template
- extension type
- user template

Procedure

1. In Web Manager, navigate to the page **Solution** > **Solution Settings** > **User Synchronization Using LDAP** > **Manage User Provisioning Rules**.

2. In the **User Provisioning Rule Name** field, enter a name for the rule.
3. Optional. Select an **IP Office Name** from the list.

   If an IP Office system is selected, the users are created on this system.
4. Optional. Enter a **Start Extension**.

   If a start extension is provided, users are assigned starting from this extension. If an extension number is in use, the extension number is skipped and the next available number is assigned.

   Note:

   Start Extension is a mandatory field if a value is provided for **Extension Template** or **Extension Type**.
5. Optional. Select an **Extension Template** from the **Select Extension Template** list.

   The extension template is applied to all users imported with this UPR.
6. Optional. Select an **Extension Type** to define the extension type created for each user.

   If both **Select Extension Template** and **Extension Type** are selected, the **Extension Template** is used.
7. Optional. Select a **User Template** from the **Select User Template** list.

   The user template is applied to all users imported with this UPR.
8. In the LDAP directory, enter the name of the UPR created in IP Office in the User column.
9. In IP Office, navigate to the page **Solution** > **Solution Settings** > **User Synchronization Using LDAP** > **Synchronize User Fields**.
10. Map the IP Office fields defined in the user provisioning rule to **User Provisioning Rule**.

Related links

LDAP Synchronization on page 579

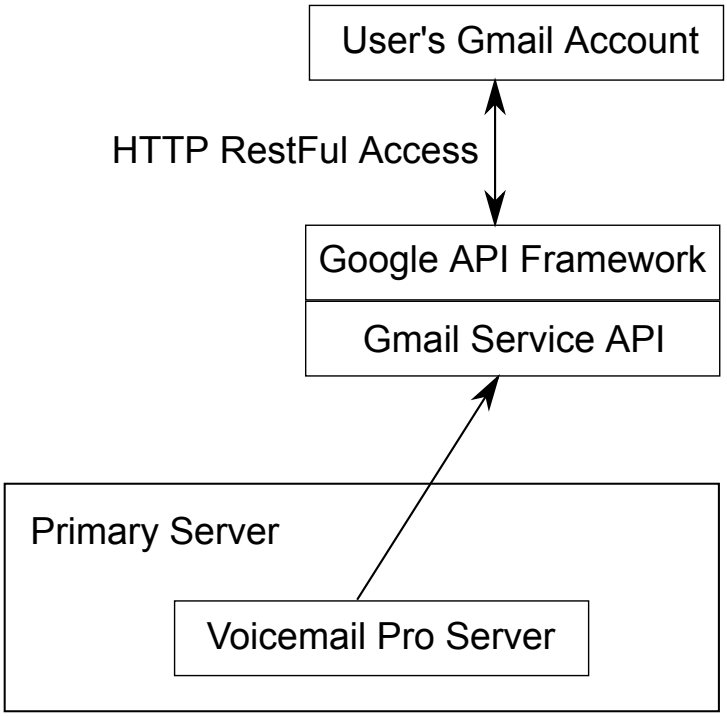
Configuring Gmail Integration

You can integrate the Google Gmail application into Voicemail Pro in order to use a Gmail account for voicemail to email functions. The supported functions are:

- **Forward**: Voicemail messages are sent as email to the Gmail account of a user. Users can use Gmail to retrieve and manage emails.
- **Copy**: Copies of voicemail messages are sent as email to the Gmail account of a user. The message is also stored locally on the Voicemail Pro server.
- **Alert**: An email is sent to the Gmail account of a user indicating the arrival of a new voicemail.

For the forwarding function:

- Up to 250 users are supported.
- The maximum message length is 7 minutes or 14 minutes when using companded.
- Messages can be accessed using Visual Voice but not one-X Communicator.



Related links

Configure User Settings on page 573

Call Intrusion

The system supports several different methods for call intrusion. The method used affects which parties can hear and be heard by other parties following the intrusion. Intrusion features are supported across a multi-site network

In the scenarios below, user A is on a call with B who may be internal or external. User C invokes one of the call intrusion methods targeting user A.

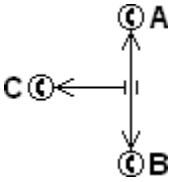
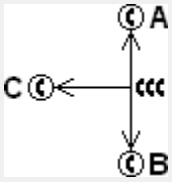
Feature	Description	Privacy Settings		
		User	Target	
		Can Intrude	Cannot Be Intruded	Private Call
Call Listen 	This feature allows you to monitor another user's call without being heard. Monitoring can be accompanied by a tone heard by all parties. Use of the tone is controlled by the Beep on Listen setting on the System | Telephony | Tones & Music tab. The default for this setting is on. If enabled, this is the only indication of monitoring given to the monitored user. There is no phone display indication of monitoring.	Used	Used	Used
Call Intrude 	This feature allows you to intrude on the existing connected call of the specified target user. All call parties are put into a conference and can talk to and hear each other. A **Call Intrude** attempt to a user who is idle becomes a Priority Call.	Used	Used	Used

Table continues…

Feature	Description	Privacy Settings		
		User	Target	
		Can Intrude	Cannot Be Intruded	Private Call
Call Steal	This function can be used with or without a specified user target. If the target has alerting calls, the function will connect to the longest waiting call. If the target has no alerting calls but does have a connected call, the function will take over the connected call, disconnecting the original user. This usage is subject to the **Can Intrude** setting of the **Call Steal** user and the **Cannot Be Intruded** setting of the target. If no target is specified, the function attempts to reclaim the user's last ringing or transferred call if it has not been answered or has been answered by voicemail.	Used	Used	Used

Table continues…

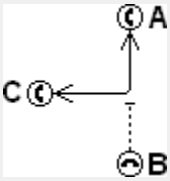
Feature	Description	Privacy Settings		
		User	Target	
		Can Intrude	Cannot Be Intruded	Private Call
Dial Inclusion 	This feature allows you to intrude on another user's call to talk to them. Their current call is put on hold while you talk and automatically reconnected when you end the intrusion. The intruder and the target extension can then talk but cannot be heard by the other party. This can include intruding into a conference call, where the conference will continue without the intrusion target. During the intrusion all parties hear a repeated intrusion tone. When the intruder hangs-up the original call parties are reconnected. Attempting to hold a dial inclusion call simply ends the intrusion. The inclusion cannot be parked.	Used	Used	Used

Table continues…

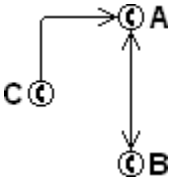
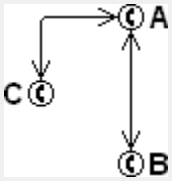
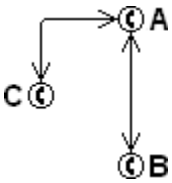
Feature	Description	Privacy Settings		
		User	Target	
		Can Intrude	Cannot Be Intruded	Private Call
Whisper Page 	This feature allows you to intrude on another user and be heard by them without being able to hear the user's existing call which is not interrupted. For example: User A is on a call with user B. When user C intrudes on user A, they can be heard by user A but not by user B who can still hear user A. Whisper page can be used to talk to a user who has enabled private call.	Used	Used	Not Used
Coaching Intrusion 	This feature allows the you to intrude on another user's call and to talk to them without being heard by the other call parties to which they can still talk. For example: User A is on a call with user B. When user C intrudes on user A, they can hear users A and B but can only be heard by user A.	Used	Used	Used

Table continues…

Feature	Description	Privacy Settings		
		User	Target	
		Can Intrude	Cannot Be Intruded	Private Call
Request Coaching Intrusion 	This feature allows you to request a call intrusion. While on a call, user A indicates to user C a request for coaching support. When user C intrudes on user A, they can hear users A and B but can only be heard by user A.	Used	Used	Used
Call Appearance	In addition to making and answering calls, appearance buttons that indicate 'in use elsewhere' can be pressed in order to join that call. The **Can Intrude** setting of the user is not used. The **Cannot Be Intruded** setting of the longest present internal party in the call is used.	Not Used	Used	Used
Bridged Appearance		Not Used	Used	Used
Line Appearance		Not Used	Used	Used

Warning:

The use of features to listen to a call without the other call parties being aware of that monitoring may be subject to local laws and regulations. Before enabling the feature you must ensure that you have complied with all applicable local laws and regulations. Failure to do so may result in severe penalties.

Intrusion Privacy Controls

The ability to intrude and be intruded is controlled by two configuration settings, the Can Intrude (User | Telephony | Supervisor Settings) setting of the user intruding and the Cannot Be Intruded (User | Telephony | Supervisor Settings) setting of target being intruded on. The setting of any other internal party is ignored. By default, no users can intrude and all users are set to cannot be intruded.

For intrusion using appearance buttons, the user's **Can Intrude** setting is not used. The **Cannot Be Intruded** setting of the longest present internal party in the call is used.

A user who can normally be intruded on can indicate that a call is a private call by using a Private Call short code or programmable button. While private call status is enabled, no intrusion is allowed except for **Whisper Page** intrusion.

In addition to the options above, **Call Listen** can only be used to intrude on calls by users in the user's Monitor Group (User | Telephony | Supervisor Settings).

For the **Call Steal** function, the **Can Be Intruded** setting is used if the call is connected.

Related links

Configure User Settings on page 573

Call Tagging

Call tagging associates a text string with a call. That string remains with the call during transfers and forwards. That includes calls across a multi-site network.

On Avaya display phones, the text is shown whilst a call is alerting and is then replace by the calling name and number when the call is connected. On analog phones with a caller ID display, the tag text replace the normal caller information.

Applications such as SoftConsole display any call tag associated with a call. If the call is parked, the tag is shown on the call park slot button used. A call tag can be added when making a call using SoftConsole or one-X Portal. A tag can be added to a call by an Incoming Call Route or by an Voicemail Pro Assisted Transfer action.

Related links

Configure User Settings on page 573

Call Waiting

Call waiting allows a user who is already on a call to be made aware of a second call waiting to be answered.

User Call Waiting

Call waiting is primarily a feature for analog extension users. The user hears a call waiting tone and depending on the phone type, information about the new caller may be displayed. The call waiting tone varies according to locale.

For Avaya feature phones with multiple call appearance buttons, call waiting settings are ignored as additional calls are indicated on a call appearance button if available.

To answer a call waiting, either end the current call or put the current call on hold, and then answer the new call. Hold can then be used to move between the calls.

Call waiting for a user can be enabled through the system configuration (User | Telephony | Call Settings | Call Waiting On) and through programmable phone buttons.

Call waiting can also be controlled using short codes. The following default short codes are available when using Call Waiting.

***15 - Call Waiting On** Enables call waiting for the user.

***16 - Call Waiting Off** Disables call waiting for the user.

***26 - Clear Call and Answer Call Waiting** Clear the current call and pick up the waiting call.

Hunt Group Call Waiting

Call waiting can also be provided for hunt group calls. The hunt group **Ring Mode** must be **Collective Call Waiting**.

On phones with call appearance buttons, the call waiting indication takes the form of an alert on the next available call appearance button. On other phones, call waiting indication is given by a tone in the speech path (the tone is locale specific).

The user's own **Call Waiting** setting is overridden when they are using a phone with call appearances. Otherwise the user's own **Call Waiting** setting is used in conjunction with the hunt group setting.

Related links

Configure User Settings on page 573

Call Restriction

Call barring can be applied in a range of ways.

Barring a User From Receiving Any External Calls For each user, Incoming Call Bar (User | Telephony | Supervisor Settings) can be selected to stop that user from receiving any external calls.

Barring a User From Making Any External Calls For each user, Outgoing Call Bar (User | Telephony | Supervisor Settings) can be selected to stop that user from making any external calls.

Barring Particular Numbers/Number Types System short codes are used to match user dialing and then perform a specified action. Typically the action would be to dial the number to an external line. However, short codes that match the dialing of particular numbers or types of numbers can be added and set to another function such as Busy. Those short codes can be added to a particular user, to a User Rights associated with several users or to the system short codes used by all users.

The system allows short codes to be set at user, user rights, system and least cost route. These have a hierarchy of operation which can be used to achieve various results. For example a system

short code for a particular number can be set to busy to bar dialing of that number. For a specific user, a user short code match to the same number but set to Dial will allow that user to override the system short code barring.

Using Account Codes The system configuration can include a list of account codes. These can be used to restrict external dialing only to users who have entered a valid account code.

- **Forcing Account Code Entry for a User** A user can be required to enter an account code before the system will return dialing tone. The account code that they enter must match a valid account code stored in the system configuration. The setting for this is Force Account Code (User | Telephony | Supervisor Settings).
- **Forcing Account Code Entry for Particular Numbers** Each system short code has a Force Account Code option. Again the account code entered must match a valid account code stored in the system configuration. for the call to continue.

Barring External Transfers and Forwards A user cannot forward or transfer calls to a number which they cannot normally dial. In addition there are controls which restrict the forwarding or transferring of external calls back off-switch. See Off-Switch Transfer Restrictions.

Related links

Configure User Settings on page 573

Centralized Call Log

The system can store a centralized call log for users. Each users' centralized call log can contain up to 60 call records for user calls (30 on IP500 V2). When this limit is reached, each new call records replaces the oldest previous record.

On Avaya phones with a fixed **Call Log** or **History** button (1400, 1600, 9500 and 9600 Series), that button can be used to display the user's centralized call log. The centralized call log is also used for M-Series and T-Series phone. The user can use the call log to make calls or to store as a personal speed dial. They can also edit the call log to remove records. The same call log is also used if the user logs into one-X Portal.

The centralized call log moves with the user if they log on and off from different phones. This includes if they hot desk within a network.

Call Log Information

The following information is included in each centralized call log record:

Information	Description

Table continues…

Name	The name, of the caller or the party called, if available. Up to 31 characters. This text is similar to that shown on the phone display of phones when they receive the call. For example, on forwarded call details of the original target and the caller name are included, eg. Bob > Sue.
Number	The number associated with the call. Up to 31 digits.
Tag	A text tag can be associated with calls by several different methods. See Call Tagging. Up to 31 characters. The tag is not shown within the call log display on phones.
Time and Date	The time and date of the call using the system time.
Duration	The call duration. For outgoing and answered calls this is the call connection time. For missed calls this is the call ringing time.

Table continues…

Record Type	Call log records can be **Incoming**, **Outgoing** or **Missed**. Note that these are calls to or from the user, not the phone, so it can include calls handled through a twinned device such as when using mobile call control. **Incoming** Calls to the user that the user then answered. This includes calls that the user answers on a twinned device. This also includes outgoing calls that are transferred to and answered by the user. **Outgoing** Calls made by the user. **Missed** Calls to the user that they did not answer. This includes calls while the user is logged off or in Do Not Disturb state. • Missed call records include an indication of what happened to the missed call. Options are **Answered by Another**, **Answered by Voicemail** or **Lost** (not answered on the system). • Missed call records are also marked as either acknowledged or unacknowledged. If the user's call log contains any unacknowledged call log records, the **Call Log** lamp is lit when using a 1608 or 1616 phone. From the phone, viewing an unacknowledged record changes it to acknowledged. • If the user has also be configured to included missed hunt group calls in their call log, those are also marked as acknowledged or unacknowledged.
Count	The number of times a matching call has been logged. A matching call is one with the same name, number and type. Only one record is kept for matching calls, with the count increased by 1 and using the time and date of the most recent matching call.

If missed hunt group calls are also being logged, the system stores up to 10 call records for each hunt group. When this limit is reached, new call records replace the oldest record.

Controlling Centralized Call Logging

The following controls exist for which users have their calls included in the centralized call log and which calls are included.

User Setting

The user centralized call log settings can be set through the user configuration (User | Telephony | Call Log) or through their associated user rights (User Rights | Telephony | Call Log).

Centralized Call Log: Default = System Default (On) This setting allows the use of centralized call logging to be enabled or disabled on a per user basis. The default is to match the system setting Default Centralized Call Log On (System | Telephony | Call Log). The other options are **On** or **Off** for the individual user. If off is selected, the call log shown on the users phone is the local call log stored by the phone.

System Settings (System | Telephony | Call Log)

Default Centralized Call Log On: Default = On. When selected, each user is defaulted to have the system store a call log of their calls. This call log is accessible on the phone when the user is using a phone with a **Call Log** or **History** button. The use of centralized call logging can be enabled/disabled on a per user basis using the Centralized Call Log user setting (User | Telephony | Call Log).

Log Missed Calls Answered at Coverage: Default = Off. This setting controls how calls to a user, that are answered by a covering user should be logged in the centralized call log. This option applies for calls answered elsewhere (covered) by pickup, call coverage (call coverage buttons or coverage group), bridged appearance button, user BLF, voicemail, etc.

Setting	Targeted User	Covering User
Off (Default)	Nothing	Answered Call
On	Missed Call	Answered Call

Log Missed Hunt Group Calls: Default = Off. By default, hunt group calls are not included in any user's centralized call log unless answered by the user. If this option is selected, a separate call log is kept for each hunt group of calls that are not answered by anyone. It includes hunt group calls that go to voicemail.

If missed hunt group calls are also being logged, the system stores up to 10 call records for each hunt group. When this limit is reached, new call records replace the oldest record.

Within the user call log setting (User | Telephony | Call Log), the list of hunt groups allows selection of which hunt groups' missed call records should be displayed as part of the user's centralized call log.

Call Scenarios

This is not a comprehensive list. However it summarizes how the user call log is used in some common call scenarios.

Scenarios	User Call Log Notes
Authorization/Account Codes	Account and authorization codes used as part of a call are not included in user call logs.
Automatic Callback	If answered, they will show as an outgoing call to the target.
Application Calls	Calls made and answered using applications (including CTI interfaces) are logged as if the user made or answered the call using an extension.

Table continues…

Scenarios	User Call Log Notes
Conference Calls	Conference calls are not included in the user call log.
Hold	When a user holds and then un-holds a call, the call duration includes the time the call was on hold.
Follow-Me	Calls to the user still appear in their user call log. The follow me calls do not appear in the user call log of the user who was the follow me destination.
Forward on Busy **Forward on No Answer**	If the forwarded call is answered, the forwarding user will have a **Missed - Answered by Other** call log record. If the forwarded call times out to voicemail, the user will have a **Missed - Answered by Voicemail** call log record.
Forward Unconditional	When forwarding to another number, there will be no record of forwarded calls in the forwarding users call log. When using the To Voicemail option, the forwarded call will by logged as a Missed - Answered by Voicemail call record.
Page Calls	Page calls are not included in any user call logs unless the page is answered (by pressing Conference). When answered the page is logged as a normal call between the two users involved.
Park	Retrieving a call from Park (even if the user is the one who parked the call) is logged as a incoming call.
Short Codes	Calls are only logged if they result in a call being made or a call being answered. Calls made using Break Out are not included.
Suppressed Digits	Calls made with digit suppression enabled (AD Suppress button) are not included in the users call log.
Transfers	If the user answers and accepts a supervised transfer, they will have a incoming calls records. One for the transfer enquiry call and one for the transferred call. If the user is the target of an unsupervised transfer, they will have an Incoming or Missed call log. Note that even if the call being transferred was originally an outgoing call, for the user answering the transfer it is logged as a incoming call.

Table continues…

Scenarios	User Call Log Notes
Twinning and Mobility	When a user has a twinned device (either internal twinning or mobile twinning), the user's call log operates regardless of which device the user uses to make or answer calls. Calls between the twinned devices, ie. the user transferring a call between devices, are not included in their call log. This includes calls made using mobile call control or a one-X Mobile client.

Multi-Site Network

The user's call log records are stored by the system that is their home system, ie. the one on which they are configured. When the user is logged in on another system, new call log records are sent to the user's home system, but using the time and date on the system where the user is logged in.

Hunt group call log records are stored on the system on which the hunt group is configured.

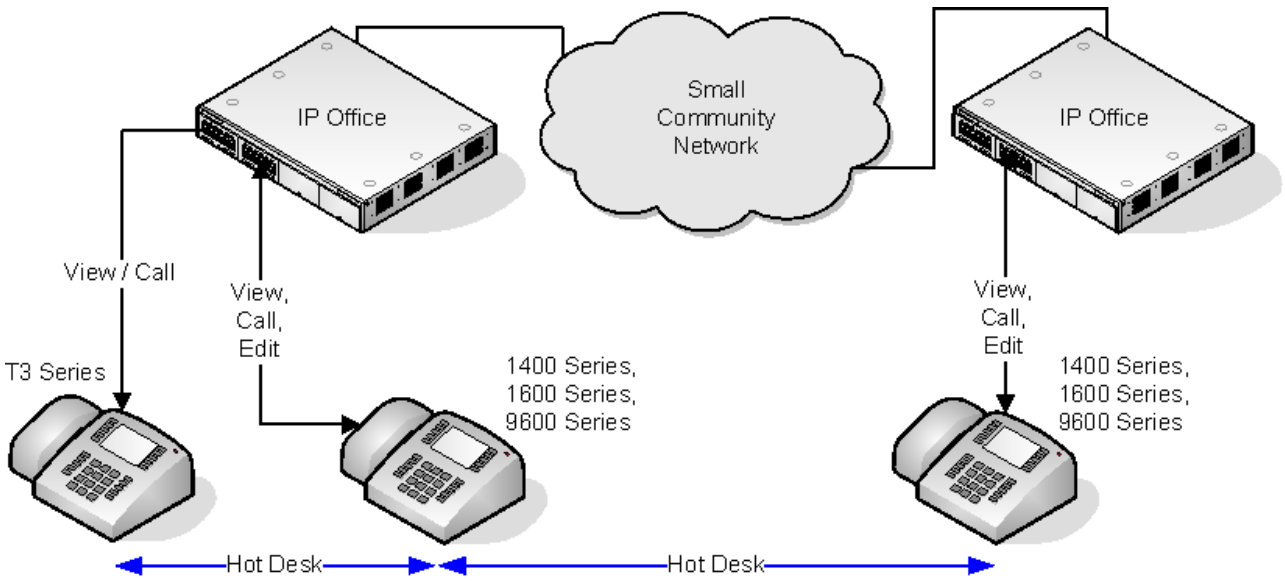
Related links

Configure User Settings on page 573

Centralized Personal Directory

Each system user is able to have up to 250 personal directory records stored by the system. A user's personal directory is also usable with 1400, 1600, 9500 and 9600 Series phones with a **CONTACTS** button. The user can view these records and use them to make calls.

1400, 1600, 9500 and 9600 Series phone users can edit their personal directory records through the phone. The user personal directory records can be edited using the Manager User | Personal Directory menu.



When the user hot desks to another phone that supports the centralized personal directory, their personal directory records become accessible through that phone. That also includes hot desking to another system in the network.

Users can also use and edit their personal directory records using one-X Portal for IP Office. Note that using one-X Portal for IP Office, users can have more personal directory records, with excess records stored by the one-X Portal server.

Related links

Configure User Settings on page 573

Account Code Configuration

Forcing Account Code Entry for Specific Numbers

Account code can be set a being required for any dialing that matches a particular short code. This is done by ticking the Force Account Code option found in the short code settings. Note that the account code request happens when the short code match occurs. Potentially this can be in the middle of dialing the external number, therefore the use of **X** wildcards in the short code to ensure full number dialing is recommended.

Entering Account Codes

The method for entering account codes depends on the type of phone being used. Refer to the relevant telephone User's Guide for details.

Account Code Button:

The Account Code Entry action (**User | Button Programming | Emulation | Account Code Entry**) and Set Account Code action (**User | Button Programming | Advanced | Set | Set Account Code**) can be assigned to a programmable button on some phones. They both operate

the same. The button can be preset with a specific account code or left blank to request account code entry when pressed. The button can then be used to specify an account code before a call or during a call.

Setting an Account Code using Short Codes:

The **Set Account Code** feature allows short codes to be created that specify an account code before making a call.

Show Account Code Setting :

This setting on the **System | Telephony | Telephony** tab controls the display and listing of system account codes.

When on and entering account codes through a phone, the account code digits are shown while being dialed.

When off and eentering account codes through a phone, the account code digits are replaced by **s** characters on the display.

Server Edition Account Code Management

Accounts codes configured on Server Edition are shared by all systems in the network.

Related links

Configure User Settings on page 573
Setting a User to Forced Account Code on page 597

Setting a User to Forced Account Code

Procedure

1. Receive the system configuration if one is not opened.
2. In the left-hand panel, click **User**. The list of existing user is shown in the right-hand panel.
3. Double-click the required user.
4. Select the **Telephony** tab.
5. Tick the Force Account Code option.
6. Click **OK**.
7. Merge the configuration.

Related links

Account Code Configuration on page 596

Coverage Groups

For users with a **Coverage Group** selected, coverage group operation is applied to all external calls that are targeted to the user.

For external calls:

In scenarios where an external call would normally have gone to voicemail, it instead continues ringing and also starts alerting the members of the coverage group.

- The follow me settings of Coverage Group members are used, the forwarding settings are not.
- If the user is not available, for example if they have logged off or set to do not disturb, coverage group operation is applied immediately.
- If the user is configured for call forward on busy, coverage operation is applied to the user's calls forwarded to the forward on busy destination.

Coverage group operation is not applied to the following types of call:

Hunt group calls.

Recall calls such as transfer return, hold recall, park recall, automatic callback.

The Coverage Group is set through the user's User | Telephony | Supervisor Settings or through their associated User Rights | Telephony | Supervisor Settings. The only group settings used are:

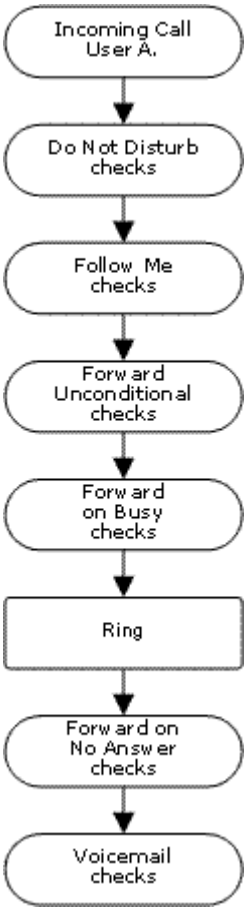
- The list of group members. They are treated as a collective group regardless of the group's configuration.
- If the group has **Night Server Fallback Group** and or **Out of Service Fallback Group** set, the members of those groups are used if the coverage group is set to night service mode or out of service mode respectively.

Related links

Configure User Settings on page 573

DND, Follow Me and Forwarding

This section contains topics looking at how users can have their calls automatically redirected. As illustrated, there is an order of priority in which the redirect methods are used.



Redirect priority

1. **Do Not Disturb (DND)** Redirect all calls to voicemail if available, otherwise return busy tone. DND overrides all the redirect method below unless the calling number is in the user's DND Exception Numbers List.
2. **Follow Me** Redirect all calls to another extension that the users is temporarily sharing. Follow Me overrides Forward Unconditional. The Follow Me destination is busy or does not answer, the user's Forward on Busy or Forward on No Answer options can be used if set.
3. **Forward Unconditional** Redirect the user's external calls to another number. That number can be any number the user can normally dial including external numbers. Forwarding of hunt group and internal calls is optional. Forward Unconditional overrides Forward on Busy and Forward on No Answer.

   If the destination is an internal user on the same system, they are able to transfer calls back to the user, overriding the Forward Unconditional.
4. **Forward on Busy** Redirects the user's external calls when the system sees the user as being busy. Uses the same number as Forward Unconditional unless a separate Forward on Busy Number is set. Forwarding internal calls is optional. Forward on Busy overrides Forward on No Answer.
5. **Forward on No Answer** Redirects the user's external calls when they ring for longer than the user's No Answer Time. Uses the same number as Forward Unconditional unless a separate Forward on Busy Number is set. Forwarding internal calls is optional.

Retrieving Externally Forwarded Calls:

Where a call is forwarded to an external destination and receives busy or is not answered within the forwarding user's **No Answer Time**, the system will attempt to retrieve the call. If forwarded on a trunk that does not indicate its state the call is assumed to have been answered, for example analog loop start trunks.

Off-Switch Forwarding Restrictions:

User forwarding is subject to the same restrictions as transferring calls. To bar a user from forwarding calls to an external number, the **Inhibit Off-Switch Forward/Transfers (User | Telephony | Supervisor Settings)** option. To bar all users from forwarding calls to external numbers the Inhibit **Off-Switch Forward/Transfers** option can be used.

When transferring a call to another extension that has forwarding enabled, the type of call being transferred is used. For example, if transferring an external call, if the transfer target has forwarding of external calls enabled then the forward is used.

Block Forwarding:

The Block Forwarding setting is used for enforcing predictable call routing, where the call should always go to the same destination. This setting was implemented for contact center applications.

Block Forwarding can be set for a user on the **User | Forwarding** page or as a user rights setting on the **User Rights | Forwarding** page.

Related links

Configure User Settings on page 573
Do Not Disturb (DND) on page 600
Follow Me on page 602
Forward Unconditional on page 604
Forward on Busy on page 606
Forward on No Answer on page 608
Determining a User's Busy Status on page 610
Chaining on page 611

Do Not Disturb (DND)

Summary: Redirect all calls to busy tone or to voicemail if available except those in your DND exceptions list.

Do Not Disturb (DND) is intended for use when the user is present but for some reason does not want to be interrupted. Instead calls are sent to voicemail if available, otherwise they receive busy tone.

Exceptions Specific numbers can be added to the user's Do Not Disturb Exception List. Calls from those numbers override DND. N and X wildcards can be used at the end of exception numbers to match a range of numbers. For external numbers, this uses the incoming caller line ID (ICLID) received with the call.

Priority Enabling DND overrides any Follow Me or forwarding set for the user, except for calls in the user's Do Not Disturb Exception List.

Phone When enabled, the phone can still be used to make calls. An **N** is displayed on many Avaya phones. When a user has do not disturb in use, their normal extension will give alternate dialtone when off hook.

Applied to

Call Types Blocked		Call Treatment
Internal	✓	Voicemail if available, otherwise busy tone.
External	✓	Voicemail if available, otherwise busy tone.
Hunt Group	✓	Call not presented (DND exceptions are not used).
Page	✓	Call not presented.
Follow Me	✗	Rings.
Forwarded	✓	Busy.
VM Ringback	✗	Rings
Automatic Callback	✗	Rings
Transfer Return	✗	Rings.
Hold Return	✗	Rings.
Park Return	✗	Rings.
Twinning	✓	Voicemail if available, otherwise busy tone.

Do Not Disturb and Twinning

Mobile Twinning Selecting DND disables mobile twinning.

Internal Twinning

- Logging out or setting do not disturb at the primary stops twinned calls alerting at the secondary also.
- Logging out or setting do not disturb at the secondary only affects the secondary.

Do Not Disturb Exceptions List For both types of twinning, when DND is selected, calls from numbers entered in the user's Do Not Disturb Exception List are presented to both the primary and secondary phones.

Do Not Disturb Controls

Do Not Disturb	
Manager	A user's DND settings can be viewed and changed through the User | DND tab within the system configuration settings.

Table continues…

Controls	The following short code features/button programming actions can be used:
Voicemail	If voicemail is available, it is used instead of busy tone for callers not in the users exceptions list. For Voicemail Pro, the Play Configuration Menu action can be used to let callers switch DND on or off.
SoftConsole	A SoftConsole user can view and edit a user's DND settings except exception numbers. Through the directory, select the required user. Their current status including DND is shown. Double-click on the details to adjust DND on or off.

Feature/Action	Short Code	Default	Button
Do Not Disturb On	✓	*08	✓ - Toggles.
Do Not Disturb Off	✓	*09	✓
Do Not Disturb Exception Add	✓	*10*N#	✓
Do Not Disturb Exception Delete	✓	*11*N#	✓
Cancel All Forwarding	✓	*00	✓

Related links

DND, Follow Me and Forwarding on page 598

Follow Me

Summary: Have your calls redirected to another user's extension, but use your coverage, forwarding and voicemail settings if the call receives busy tone or is not answered.

Follow Me is intended for use when a user is present to answer calls but for some reason is working at another extension such as temporarily sitting at a colleague's desk or in another office or meeting room. Typically you would use Follow Me if you don't have a Hot Desking log in code or if you don't want to interrupt your colleague from also receiving their own calls, ie. multiple users at one phone.

Priority Follow Me is overridden by DND except for callers in the user's DND Exception Numbers List. Follow Me overrides Forward Unconditional but can be followed by the user's Forward on Busy or Forward on No Answer based on the status of the Follow Me destination.

Destination The destination must be an internal user extension number. It cannot be a hunt group extension number or an external number.

Duration The Follow Me user's no answer timeout is used. If this expires, the call either follows their Forward on No Answer setting if applicable, or goes to voicemail is available. Otherwise the call continues to ring at the destination.

Phone When enabled, the phone can still be used to make calls. When a user has follow me in use, their normal extension will give alternate dialtone when off hook.

Exceptions

- The Follow Me destination extension can make and transfer calls to the follow me source.
- The call coverage settings of the user are applied to their Follow Me calls. The call coverage settings of the destination are not applied to Follow Me calls it receives.

Calls Forwarded

Call Types Redirected		
Internal	✓	Redirected.
External	✓	Redirected.
Hunt Group	✓	Redirected*.
Page	✓	Redirected.
Follow Me	✗	Not redirected.
Forwarded	✓	Redirected.
VM Ringback	✗	Not redirected.
Automatic Callback	✗	Not redirected.
Transfer Return	✗	Not redirected.
Hold Return	✗	Not redirected.
Park Return	✗	Not redirected.

*Except calls for "Longest Waiting" type hunt groups.

Follow Me Controls

Follow Me	
Manager	A user's Follow Me settings can be viewed and changed through the User | Forwarding tab within the system configuration settings. Note that on this tab, entering a Follow Me Number also enables Follow Me.
Controls	The following short code features/button programming actions can be used:

Table continues…

Voicemail	For calls initially targeted to the user but then redirected, when voicemail is invoked the mailbox of the user is used and not the mailbox of the destination. For Voicemail Pro, the Play Configuration Menu action can be used to let callers alter or set their current Follow Me destination.
SoftConsole	A SoftConsole user can view and edit a user's Follow Me settings. Through the directory, select the required user. Their current status including Follow Me is shown. Double-click on the details and select Forwarding to alter their forwarding settings including Follow Me.

Feature/Action	Short Code	Default	Button
Follow Me Here	✓	*12*N#	✓
Follow Me Here Cancel	✓	*13*N#	✓
Follow Me To	✓	*14*N#	✓
Cancel All Forwarding	✓	*00	✓

Related links

DND, Follow Me and Forwarding on page 598

Forward Unconditional

Summary: Have your calls redirected immediately to another number including any external number that you can dial.

Priority This function is overridden by DND and or Follow Me if applied. **Forward Unconditional** overrides **Forward on Busy**.

Destination The destination can be any number that the user can dial. If external and Inhibit Off-Switch Transfers is applied, the caller is directed to voicemail if available, otherwise they receive busy tone. If the destination is an internal user on the same system, they are able to transfer calls back to the user, overriding the Forward Unconditional.

Duration After being forwarded for the user's no answer time, if still unanswered, the system can apply additional options. It does this if the user has forward on no answer set for the call type or if the user has voicemail enabled.

- If the user has forward on no answer set for the call type, the call is recalled and then forwarded to the forward on no answer destination.
- If the user has voicemail enabled, the call is redirected to voicemail.
- If the user has both options set, the call is recalled and then forwarded to the forward on no answer destination for their no answer time and then if still unanswered, redirected to voicemail.

- If the user has neither option set, the call remains redirected by the forward unconditional settings.

Note that for calls redirected via external trunks, detecting if the call is still unanswered requires call progress indication. For example, analog lines do not provide call progress signalling and therefore calls forwarded via an analog lines are treated as answered and not recalled.

Phone When enabled, the phone can still be used to make calls. An **D** is displayed on DS phones. When a user has forward unconditional in use, their normal extension will give alternate dialtone when off hook.

Calls Forwarded Once a call has been forwarded to an internal destination, it will ignore any further **Forward No Answer** or **Forward on Busy** settings of the destination but may follow additional **Forward Unconditional** settings unless that creates a loop.

Call Types Forwarded		
Internal	✓	Optional.
External	✓	Forwarded.
Hunt Group	✓	Optional.*
Page	✗	Not presented.
Follow Me	✗	Rings.
Forwarded	✓	Forwarded.
VM Ringback	✗	Rings.
Automatic Callback	✗	Rings.
Transfer Return	✗	Rings.
Hold Return	✗	Ring/hold cycle.
Park Return	✗	Rings.

*Optional only for calls targeting sequential and rotary type groups. Includes internal call to a hunt group regardless of the forward internal setting.

To Voicemail: Default = Off. If selected and forward unconditional is enabled, calls are forwarded to the user's voicemail mailbox. The **Forward Number** and **Forward Hunt Group Calls** settings are not used. This option is not available if the system's **Voicemail Type** is set to **None**. 1400, 1600, 9500 and 9600 Series phone users can select this setting through the phone menu. Note that if the user disables forward unconditional the **To Voicemail** setting is cleared.

Forward Unconditional Controls

Forward Unconditional	
Manager	A user's forwarding settings can be viewed and changed through the User | Forwarding tab within the system configuration settings.
Controls	The following short code features/button programming actions can be used:

Table continues…

Voicemail	For calls initially targeted to the user but then redirected, when voicemail is invoked the mailbox of the user is used and not the mailbox of the destination. For Voicemail Pro, the Play Configuration Menu action can be used to let callers set their current forwarding destination and switch Forwarding Unconditional on/off.
SoftConsole	A SoftConsole user can view and edit a user's forwarding settings. Through the directory, select the required user. Their current forwarding status is shown. Double-click on the details and select Forwarding to alter their forwarding settings.

Feature/Action	Short Code	Default	Button
Forward Number	✓	*07*N#	✓
Forward Unconditional On	✓	*01	✓ - Toggles.
Forward Unconditional Off	✓	*02	✓
Forward Hunt Group Calls On	✓	✗	✓ - Toggles.
Forward Hunt Group Calls Off	✓	✗	✓
Disable Internal Forwards	✓	✗	✗
Enable Internal Forwards	✓	✗	✗
Disable Internal Forwards Unconditional	✓	✗	✗
Enable Internal Forwards Unconditional	✓	✗	✗
Set No Answer Time	✓	✗	✓
Cancel All Forwarding	✓	*00	✓

Related links

DND, Follow Me and Forwarding on page 598

Forward on Busy

Summary: Have your calls redirected when you are busy to another number including any external number that you can dial.

The method by which the system determines if a user is 'busy' to calls depends on factors such as whether they have multiple calls appearance buttons or Call Waiting and or Busy on Held set. See Busy.

Priority This function is overridden by DND and or Forward Unconditional if applied. It can be applied after a Follow Me attempt. It overrides Forward on No Answer.

Destination The destination can be any number that the user can dial. The Forward Unconditional destination number is used unless a separate number Forward on Busy Number is set. If Inhibit Off-Switch Transfers is applied, the caller is directed to voicemail if available, otherwise they receive busy tone.

Duration The destination is rung using the forwarding user's No Answer Time. If this expires, the call goes to voicemail is available. Calls to an external destination sent on trunks that do not signal their state are assumed to have been answered, for example analog loop start trunks.

Phone Forward on Busy is not indicated and normal dial tone is used.

Calls Forwarded Once a call has been forwarded to an internal destination, it will ignore any further **Forward No Answer** or **Forward on Busy** settings but may follow additional **Forward Unconditional** settings.

Call Types Forwarded		
Internal	✓	Optional.
External	✓	Forwarded.
Hunt Group	✗	Not presented.
Page	✗	Not presented.
Follow Me	✗	Rings.
Forwarded	✓	Forwarded.
VM Ringback	✗	Rings.
Automatic Callback	✗	Rings.
Transfer Return	✗	Rings.
Hold Return	✗	Ring/hold cycle.
Park Return	✗	Rings.

Forward on Busy Controls

Forward on Busy	
Software Level	A user's forwarding settings can be viewed and changed through the User | Forwarding tab within the system configuration settings.
Controls	The following short code features/button programming actions can be used:

Table continues…

Voicemail	For calls initially targeted to the user but then redirected, when voicemail is invoked the mailbox of the user is used and not the mailbox of the destination. For Voicemail Pro, the Play Configuration Menu action can be used to let callers set the forward destination.
SoftConsole	A SoftConsole user can view and edit a user's forwarding settings. Through the directory, select the required user. Their current forwarding status is shown. Double-click on the details and select Forwarding to alter their forwarding settings.

Feature/Action	Short Code	Default	Button
Forward Number	✓	*07*N#	✓
Forward on Busy Number	✓	*57*N#	✓
Forward on Busy On	✓	*03	✓ - Toggles.
Forward on Busy Off	✓	*04	✓
Disable Internal Forwards	✓	✗	✗
Enable Internal Forwards	✓	✗	✗
Disable Internal Forwards Busy or No Answer	✓	✗	✗
Enable Internal Forwards Busy or No Answer	✓	✗	✗
Set No Answer Time	✓	✗	✓
Cancel All Forwarding	✓	*00	✓

Related links

DND, Follow Me and Forwarding on page 598

Forward on No Answer

Summary: Have your calls redirected another number if it rings without being answered.

Priority This function is overridden by DND and Forward on Busy if applied. It can be applied after a Follow Me attempt. Forward Unconditional overrides Forward on Busy and Forward on No Answer.

Destination The destination can be any number that the user can dial. The Forward Unconditional destination number is used unless a separate number Forward on Busy Number is set. If Inhibit Off-Switch Transfers is applied, the caller is directed to voicemail if available, otherwise they receive busy tone.

Duration The destination is rung using the forwarding user's No Answer Time. If this expires, the call goes to voicemail is available. Otherwise the call continues to ring at the destination. Calls to an external destination sent on trunks that do not signal their state are assumed to have been answered, for example analog loop start trunks.

Phone Forward on No Answer is not indicated and normal dial tone is used.

Calls Forwarded Once a call has been forwarded to an internal destination, it will ignore any further **Forward No Answer** or **Forward on Busy** settings but may follow additional **Forward Unconditional** settings.

Call Types Forwarded		
Internal	✓	Optional.
External	✓	Forwarded.
Hunt Group	✗	Not applicable.
Page	✗	Not applicable.
Follow Me	✗	Rings.
Forwarded	✓	Forwarded.
VM Ringback	✗	Rings.
Automatic Callback	✗	Rings.
Transfer Return	✗	Rings.
Hold Return	✗	Ring/hold cycle.
Park Return	✗	Rings.

Forward on No Answer Controls

Forward on No Answer	
Manager	A user's forwarding settings can be viewed and changed through the User | Forwarding tab within the system configuration settings.
Controls	The following short code features/button programming actions can be used:

Table continues…

Voicemail	For calls initially targeted to the user but then redirected, when voicemail is invoked the mailbox of the user is used and not the mailbox of the destination. For Voicemail Pro, the Play Configuration Menu action can be used to let callers set the forward destination. It cannot however be used to enable Forward on Busy or set a separate Forward on Busy number.
SoftConsole	A SoftConsole user can view and edit a user's forwarding settings. Through the directory, select the required user. Their current forwarding status is shown. Double-click on the details and select Forwarding to alter their forwarding settings.

Feature/Action	Short Code	Default	Button
Forward Number	✓	*07*N#	✓
Forward on Busy Number	✓	*57*N#	✓
Forward on No Answer On	✓	*05	✓ - Toggles.
Forward on No Answer Off	✓	*06	✓
Enable Internal Forwards	✓	✗	✗
Disable Internal Forwards	✓	✗	✗
Enable Internal Forwards Busy or No Answer	✓	✗	✗
Disable Internal Forwards Busy or No Answer	✓	✗	✗
Set No Answer Time	✓	✗	✓
Cancel All Forwarding	✓	*00	✓

Related links

DND, Follow Me and Forwarding on page 598

Determining a User's Busy Status

Various system features allow users to handle more than one call at a time. Therefore the term "busy" has different meanings. To other users it means whether the user is indicated as being busy. To the system it means whether the user is not able to receive any further calls. The latter is

used to trigger 'busy treatment', either using a user's **Forward on Busy** settings or redirecting calls to voicemail or just returning busy tone.

Busy Indication - In Use The user busy indication provided to programmable buttons and to user applications, is based on the monitored user's hook switch status. Whenever the user is off-hook, they will be indicated as being busy regardless of call waiting or call appearance settings.

Busy to Further Calls Whether a user can receive further calls is based on a number of factors as described below.

- **Logged In and Present** Is the user logged into an extension and is that extension physically connected to the system.
- **Busy on Held** If a user enables their Busy on Held setting, whenever they have a call on hold, they are no longer available to any further incoming calls.
- **Appearance Buttons** A user's call appearance button are used to receive incoming calls. Normally, whilst the user has any free call appearance buttons, they are available to receive further calls. Exceptions are:
  - **Reserve Last Appearance** Users with appearance buttons require a free call appearance button to initiate transfers or conferences. Therefore it is possible through the user's configuration settings to reserve their last call appearance button for outgoing calls only.
  - **Other Appearance Buttons** Calls may also be indicated on line, call coverage and bridged appearance buttons.

Call Waiting Users of phones without appearance buttons can use call waiting. This adds an audio tone, based on the system locale, when an additional call is waiting to be answered. Only one waiting call is supported, any further calls receive busy treatment.

Hunt Group Calls A user's availability to receive hunt group calls is subject to a range of other factors. See Member Availability.

Related links

DND, Follow Me and Forwarding on page 598

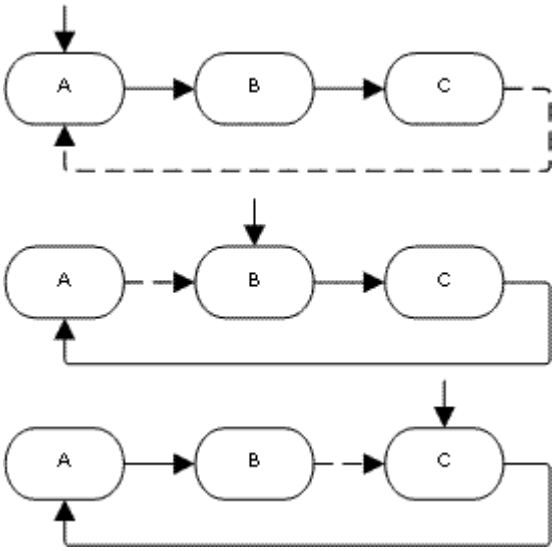
Chaining

Chaining is the process where a call forward to an internal user destination is further forwarded by that user's own forwarding settings.

Follow Me Calls Follow Me calls are not chained. They ignore the forwarding, Follow Me and Do Not Disturb settings of the Follow Me destination.

Voicemail If the call goes to voicemail, the mailbox of the initial call destination before forwarding is used.

Looping When a loop would be created by a forwarding chain, the last forward is not applied. For example the following are scenarios where A forwards to B, B forwards to C and C forwards to A. In each case the final forward is not used as the destination is already in the forwarding chain.



Hunt Group Loop If a user forwards a call to a hunt group of which they are a member, the group call is not presented to them but is presented to other members of the hunt group.

Maximum Number of Forwards A maximum of 10 forwarding hops are supported for any call.

Calls Forwarded Once a call has been forwarded to an internal destination, it will ignore any further **Forward No Answer** or **Forward on Busy** settings but may follow additional **Forward Unconditional** settings.

Related links

DND, Follow Me and Forwarding on page 598

Hot Desking

Hot desking allows users to log in at another phone. Their incoming calls are rerouted to that phone and their user settings are applied to that phone. There are a number of setting and features which affect logging in and out of system phones.

In order to hot desk, a user must be assigned a Login Code (User | Telephony | Supervisor Settings) in the system configuration.

By default, each system extension has an **Base Extension** setting. This associates the extension with the user who has the matching **Extension** settings as being that extension's default associated user.

- By leaving the **Base Extension** setting for an extension blank, it is possible to have an extension with no default associated user. This is only supported for non-IP/CTI extensions. Extensions in this state use the settings of a special user named **NoUser**. On suitable phones the display may show **NoUser**.
- You can create users whose Extension directory number is not associated with any physical extension. These users must have a log in code in order to log in at a phone when they need

to make or receive calls. In this way the system can support more users than it has physical extensions.

When another user logs in at an extension, they take control of that phone. Any existing user, including the default associated user, is logged out that phone.

- Any user settings not applicable to the type of phone on which the user has logged in become inaccessible. For example some programmable button features will become inaccessible if the phone at which a user logs in does not have a sufficient number of programmable buttons.
- Note that settings that are stored by the phone rather than by the system remain with the phone and do not move when a user hot desks.

1400 Series, 1600 Series, 9500 Series, 9600 Series, M-Series and T-Series telephones all use the centralized call log and centralized personal directory features that move those settings with the user as they hot desk.

Other Avaya H.323 IP telephones can be configured to backup and restore user settings to a file server when a user hot desks between phones. The range of settings supported depends on the particular phone model. Refer to the IP Office H.323 IP Telephone Installation Manual.

For all other features and phone types, it must be assumed that any settings and data shown by the phone is stored by the phone and are still accessible after logging off.

When a user logs off or is logged out by someone else logging in, they are automatically logged back in at the extension for which they are the default associated user if no one else is logged in at that extension. However this does not happen for users set to **Forced Login** (User | Telephony | Supervisor Settings).

For each user, you can configure how long the extension at which they are logged in can remain idle before they are automatically logged out. This is done using the Login Idle Period option. This option should only be used in conjunction with Force Login.

Logged in users who are members of a hunt group can be automatically logged out if they do not answer hunt group calls presented to them. This is done by selecting **Logged Off** as the user's **Status on No Answer** (User | Telephony | Supervisor Settings) setting.

Calls to a logged out user are treated as if the user is busy until the user logs in.

Logging in and out at a phone can be done either using system short codes or programmable buttons.

- The default system short code for logging in, is ***35*N#** where the user replaces N with their extension number and then log in code separated by a *. This uses the short code feature ExtnLogin. If the user dials just a log in code as N, it is checked against the user with the same extension number as the extension's base extension number.
- The default system short code for logging out is ***36**. This uses the short code feature ExtLogout.
- The ExtnLogin and ExtnLogout features can be assigned to programmable buttons on suitable Avaya phones. The **ExtnLogin** button will then prompt the user to enter their details.

Related links

Configure User Settings on page 573
Remote Hot Desking on page 614
Call Center Agents on page 615
Hot Desking Examples on page 615
Automatic Log Out on page 617

Remote Hot Desking

The system supports hot desking between systems within a network.

In the descriptions below, the system on which the user is configured is termed their 'home' system, all other systems are 'remote' systems.

When a user logs in to a remote system:

- The user's incoming calls are rerouted to that system.
- The user's outgoing calls uses the settings of the remote system.
- The user's license privileges move with them, for example their user profile setting is retained. The host system does not need to be licensed for the user.
- The user's own settings are transferred. However, some settings may become unusable or may operate differently.
- User rights are not transferred to the remote system but the name of any user rights associated with the user are transferred. If user rights with the same name exist on the remote system, then they will be used. The same applies for user rights applied by time profiles, if time profiles with the same name exist on the remote system .
- Appearance buttons configured for users on the home system will no longer operate.
- Various other settings may either no longer work or may work differently depending on the configuration of the remote system at which the user has logged in. For example: For T3 phones, the personal directory is not transferred with the user.
- The rights granted to the user by their **Profile** settings are retained by the user. There is no requirement for the remote system to have the appropriate licenses for the **Profile**.

If the user's home system is disconnected while the user is remotely hot desked, the user will remain remotely hot desked. They can remain in that state unless the current host system is restarted. They retain their license privileges as if they were on their home system. Note however that when the user's home system is reconnected, the user may be automatically logged back onto that system.

Break Out Dialing 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 multi-site network but is of most use to remote hot deskers.

Related links

Hot Desking on page 612

Call Center Agents

On systems with a call center application such as Compact Contact Center (CCC) or Compact Business Center (CBC), logging in and logging out is a key part of tracking and reporting on call center agents. It also controls call distribution as, until the agent logs in, their hunt group membership is seen as disabled.

For CCC, CBC and Delta Server, an agent is defined as being a user with a Login Code and set to Forced Login. Those users consume a CCC agent license.

Related links

Hot Desking on page 612

Hot Desking Examples

The following are example of different ways that the hot desking settings can be used.

Related links

Hot Desking on page 612

Scenario 1: Occasional Hot Desking

About this task

In this scenario, a particular user, for this example extension 204, needs to occasionally work at other locations within the building.

Procedure

1. A **Login Code** is added to the user's configuration settings, for this example **1234**.
2. The user can now log in when needed at any other phone by dialing ***35*204*1234#**.

   The phone's default associated user is logged out by this and their calls get busy treatment. User 204 is also logged out their normal phone and their calls now rerouted to the phone at which they have logged in.
3. When finished, the user can dial ***36** to log out.
4. This logs the phone's normal default user back on.

   Its also logs the hot desking user back on at their normal extension.

Scenario 2: Regular Hot Desking

About this task

This scenario is very similar to the one above. However, the user doesn't want to be automatically logged back in on their normal phone until they return to its location.

Procedure

1. A **Login Code** is added to the user's configuration settings, for this example **1234**.
2. The Forced Login option is selected.
3. When the user logs out of the phone that they are currently using, they are no longer automatically logged in on their normal extension.

   When they return to it they must dial ***35*204*1234#** to log in.
4. Whilst not logged in anywhere, calls to the user receive busy treatment.

Scenario 3: Full Hot Desking

About this task

Similar to the scenarios above but this time the user doesn't have a regular phone extension that they use. In order to make and receive calls they must find a phone at which they can log in.

Procedure

1. The user is given an Extension directory number that is not matched by the extension directory number setting of any existing extension.
2. They are also given a **Login Code** and a **Login Idle Period** is set, for this example 3600 seconds (an hour).

   Forced Login isn't required as the user has no default extension at which they might be automatically logged in by the system.
3. The user can now log in at any available phone when needed.
4. If at the end of the business day they forget to log out, the Login Idle Period will eventually log them off automatically.

Scenario 4: Call Center Hot Desking

About this task

In this scenario, the phone extensions have no default extension number. Several phones set like this might be used in a call center where the agents use whichever desk is available at the start of their shift. Alternatively a set of desks with such phones might be provided for staff that are normally on the road but occasionally return to the office and need a temporary desk area to complete paper work.

Procedure

1. For the extensions, the Extension setting is left blank.

This means that those phones will be associated with the NoUser user's settings and display **NOT LOGGED ON**.

2. The call center agents or road-warrior users are configured with Extension directory numbers that also don't match any existing physical extensions.

   They are all given Login Code numbers.

3. The users can log in at any of the extensions when required.

   When they log out or log in elsewhere, the extensions return to the NoUser setting.

Automatic Log Out

Normally a user can either log themselves out or be logged out by another user logging in. The following methods can be used by the system to automatically log out a user. A remote hot desking user whose home system can no longer be seen by the remote system at which they are logged in is automatically logged out after 24 hours.

The following methods only apply to users with a **Login Code** and set to **Forced Login**.

Idle Timeout

The user Login Idle Period (User | Telephony | Supervisor Settings) can be used to automatically log out the user after a set period of phone inactivity. The period can be set between 1 to 99999 seconds and is based on call inactivity other than ringing calls.

Unanswered Calls

Users who are members of hunt groups are presented with hunt group calls when they are logged in and not already on a call. If the user is logged in but not actually present they will continue to be presented with hunt group calls. In this scenario it can be useful to log the user off.

For the hunt group On the Hunt Group | Hunt Group tab, use the Agent's Status on No Answer Applies to setting to select which types of unanswered hunt group calls should change the user's status. The options are:

None.

Any Calls.

External Inbound Calls Only.

For the user The Status on No Answer (User | Telephony | Supervisor Settings) can be used. This sets what the user's status should be changed to if they do not answer a hunt group call. The options are:

Logged In If this option is selected, the user's status is not changed.

Busy Wrap-Up If this option is selected the user's membership status of the hunt group triggering the action is changed to disabled. The user can still make and receive calls and will still continue to receive calls from other hunt groups to which they belong.

Busy Not Available If this option is selected the user's status is changed to do not disturb. This is the equivalent of DND and will affect all calls to the user.

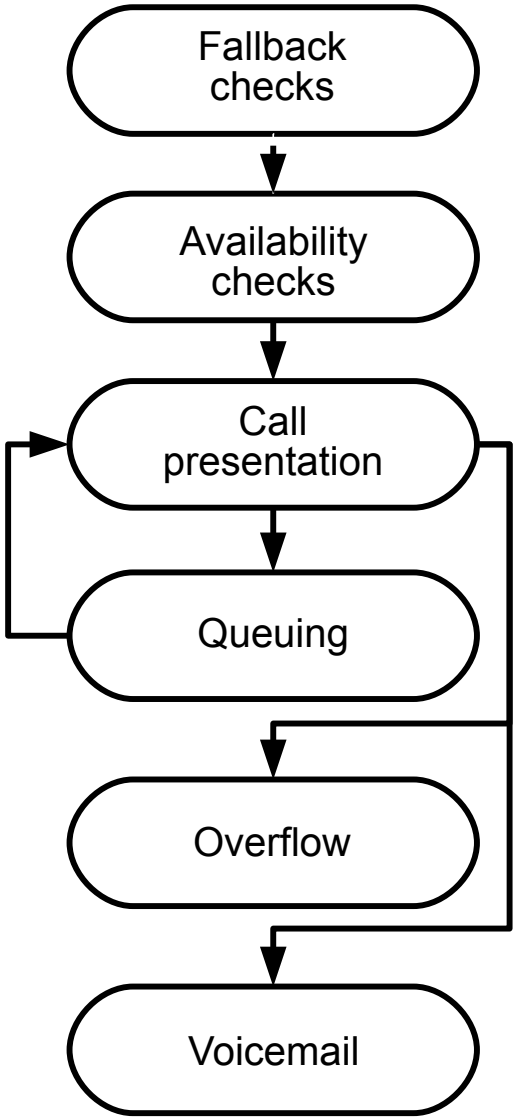
Logged Off If this option is selected the users status is changed to logged out. In that state the cannot make calls and cannot receive calls. Hunt group calls go to the next available agent and personal calls treat the user as being busy.

Related links

Hot Desking on page 612

Group Operation

A group is a collection of users accessible through a single directory number. Calls to that group can be answered by any available member of the group. The order in which calls are presented can be adjusted by selecting different group types and adjusting the order in which group members are listed.



- **Call Presentation**: The order in which the available members of the group are used for call

presentation is selectable.

- **Availability**: There are a range of factors which control whether group calls are presented to a user in addition to that user being a member of the group.
- **Queuing**: This optional feature allows calls to be queued when the number of calls to be presented exceeds the number of available group members to which call can be presented.
- **Announcements**: On systems with a voicemail server (Voicemail Pro or Embedded Voicemail), announcements can be played to callers waiting to be answered. That includes calls that are ringing and calls that are queued.
- **Overflow**: This optional feature can be used to include additional agents from an overflow group or groups when a call is not answered.
- **Fallback**: A group can be taken out of operation manually or using a time profile. During fallback, calls can be redirected to a fallback group or sent to voicemail or just receive busy tone. Two types of fallback are supported; night service and out of service.
- **Voicemail**: Calls can be redirected to voicemail. The system allows selection of whether group calls remain in the group mailbox or are copied (broadcast) to the individual mailboxes of the group members. When messages are stored in the group's own mailbox, selection of who receives message waiting indication is possible.

Group Editing

Changing the name of a group has the following effects:

- A new empty mailbox is created on voicemail with the new group name.
- Records in other groups' Overflow lists will be updated.
- Out-of-Service and Night-Service fallback references are updated.

Modifying the extension number of a group updates the following:

- Group buttons.
- Overflow, Out of Service Fallback and Night Service Fallback group records.
- Incoming call route records.

When a group is deleted, all references to the deleted group will be removed including:

- Records in Incoming call routing tables.
- Transfer target in internal auto-attendant.
- Overflow, Night-Service or Fallback-Service on other groups.
- DSS keys monitoring group status.

Server Edition Group Management

Groups can be stored in the configuration of any system in the network. Groups created at the solution level on Manager and Web Manager are stored on the Primary Server. All groups can include users from anywhere in the network and are automatically advertised to and diallable on any of the systems in the network.

Groups configured on the Server Edition Primary by default fail over to the Server Edition Secondary. Groups configured on a Server Edition Expansion System can be configured to fail over to the Server Edition Primary, the Server Edition Secondary, or another Server Edition Expansion System.

Groups in a Multi-Site Network

In a multi-site network, the extension numbers of users are automatically shared between systems and become diallable from other systems without any further programming.

The following features are available for groups.

Advertised Groups:

Each group can be set as being 'advertised'. The group can then be dialed from other systems within the multi-site network. The groups extension number and name must be unique within the network. Non-advertised group numbers remain local only to system hosting the group.

Distributed Groups:

Groups on a system can include users located on other systems within the network. Distributed groups are automatically advertised to other systems within the network. Note that distributed groups can only be edited on the system on which they were created.

Related links

[Configure User Settings](#) on page 573
[Group Types](#) on page 621
[Call Presentation](#) on page 622
[Group Member Availability](#) on page 623
[Example Hunt Group](#) on page 625
[CBC/CCC Agents and Hunt Groups](#) on page 627

Group Types

At its most basic, a group's settings consist of a group name, an extension number, a list of group members and a hunt type selection. It is the last two settings which determine the order in which incoming calls are presented to hunt group members.

The available group types are; Collective, Sequential, Rotary and Longest Waiting. These work are follows:

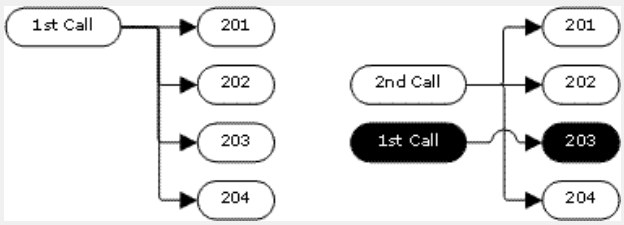
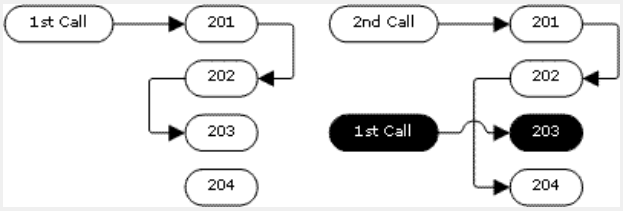
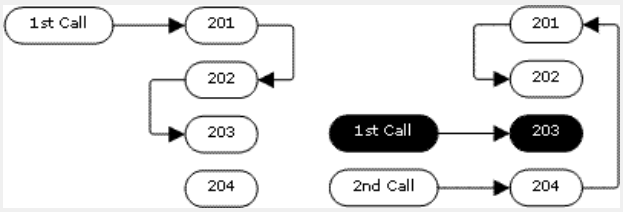
Collective Group (formerly Group Group)	
An incoming call is presented simultaneously to all the available group members.	
Sequential Group (formerly Hunt or Linear Group)	

Table continues…

An incoming call is presented to the first available member in the list. If unanswered, it is presented to the next available member in the list. The next incoming call uses the same order. It is presented to the available members starting again from the top of the list.	
Rotary Hunt Type (formerly Circular Group)	
This hunt type operates similarly to Sequential. However the starting point for call presentation is the first available member after the last member to answer a call.	
Longest Waiting Hunt Type (formerly Idle or Most Idle)	
This hunt type does not present calls to hunt group members in the order that they are listed. It presents calls using the order of how long the available hunt group members have been idle. An incoming call is first presented to the available member who has been idle the longest. If unanswered it is presented to the next longest idle member. Where hunt group calls are being presented to a twinned extension, the longest waiting status of the user can be reset by calls answered at either their master or twinned extension.	

Related links

Group Operation on page 618

Call Presentation

Summary: Calls are presented to each available hunt group member in turn. If having been presented to all the available members, none answers, the call is redirected to voicemail if available, otherwise it continues to be presented to the next available member.

In addition to the summary, options exist to have calls queued or to have calls also presented to agents in an overflow group or groups.

First and Next Available Members The first available member to which a call is presented and the order of the next available members to which a call is presented are determined by the hunt group's Hunt Type setting.

Additional Calls When additional calls are waiting to be presented, additional available hunt group members are alerted using the hunt group type. When any member answers a call it will be the first waiting call that is answered.

No Available Members If the number of incoming calls exceeds the number of available members to which calls can be presented, the following actions are usable in order of precedence.

Queuing If queuing has been enabled for the hunt, it is applied to the excess calls up to the limits specified for the number of queued calls or length of time queued.

Voicemail If voicemail has been enabled for the hunt group, excess calls are directed to voicemail.

Busy Tone Busy tone is returned to the excess calls .

No Answer Time This value is used to determine how long a call should ring at a hunt group member before being presented to the next available hunt group member. The **System | Telephony | Telephony | No Answer Time** setting is used unless a specific **Hunt | Hunt Group | No Answer Time** is set.

Voicemail If voicemail is being used, if having been presented to all the available group members the call is still not answered then it goes to voicemail.

The call will also go to voicemail when the hunt group's **Voicemail Answer Time** is exceeded. the mailbox of the originally targeted hunt group is used even if the call has overflowed or gone to a night server hunt group.

Calls Not Being Answered Quick Enough - Overflow In addition to ringing at each available member for the No Answer Time, a separate **Overflow Time** can be set. When a calls total ring time against the group exceeds this, the call can be redirected to an overflow group or groups.

No Available Member Answers If a call has been presented unanswered to all the available members, either of two actions can be applied. If voicemail is available, the call is redirected to voicemail. If otherwise, the call will continue being presented to hunt group members until answered or, if set, overflow is used.

Call Waiting For hunt groups using the Group hunt type, call waiting can be used.

Related links

Group Operation on page 618

Group Member Availability

Summary: Details when a hunt group member is seen as being available to be presented a hunt group call.

The Hunt Group settings within Manager list those users who are members of the hunt group and therefore may receive calls directed to that hunt group. However there are a range of factors that can affect whether a particular hunt group member is available to take hunt group calls at any time.

Existing Connected Call Users with an existing connected call are not available to further hunt group calls. This is regardless of the type of connected call, whether the user has available call appearance buttons or is using call waiting.

Hunt Group Call Waiting For Collective hunt groups call waiting can be enabled using the **Ring Type** of **Collective Call Waiting**.

Logged In/Logged Out The system allows user's to log in and out extensions, a process known as 'hot desking'. Whilst a user is logged out they are not available to receive hunt group calls.

Mobile Twinning users with both **Hunt group calls eligible for mobile twinning** and **Twin when logged out** selected will still receive hunt group calls unless they switch off twinning.

Membership Enabled/Disabled The system provides controls to temporarily disable a users' membership of a hunt group. Whilst disabled, the user is not available to receive calls directed to that hunt group.

Do Not Disturb This function is used by users to indicate that they do not want to receive any calls. This includes hunt group calls. In call center environments this state is also known as 'Busy Not Available'. See Do Not Disturb.

Busy on Held When a user has a held call, they can receive other calls including hunt group calls. The Busy on Held settings can be used to indicate that the user is not available to further calls when they have a held call.

Forward Unconditional Users set to Forward Unconditional are by default not available to hunt group calls. The system allows the forwarding of hunt group calls to be selected as an option.

Idle /Off Hook The hunt group member must be idle in order to receive hunt group call ringing.

No Available Members If queuing has been enabled, calls will be queued. If queuing has not been enabled, calls will go to the overflow group if set, even if the overflow time is not set or is set to 0. If queuing is not enabled and no overflow is set, calls will go to voicemail. If voicemail is not available, external calls go to the incoming call routes fallback destination while internal calls receive busy indication.

Hunt Group Member Availability Settings	
Manager	Forwarding and do not disturb controls for a user are found on the User | Forwarding and User | DND tabs. Enabling and disabling a users hunt group membership is done by ticking or unticking the user entry in the hunt group's extensions list on the Hunt Group | Hunt Group tab.
Controls	The following short code features/button programming actions can be used:
SoftConsole	A SoftConsole user can view and edit a user's settings. Through the directory, select the required user. Their current status including DND, Logged In and hunt group membership states are shown and can be changed. Forwarding settings can be accessed by then selecting Forwarding.

Feature/Action	Short Code	Default	Button
Hunt Group Enable	✓	✗	✓HGEna - Toggles.
Hunt Group Disable	✓	✗	✓HGDis
Forward Hunt Group On	✓	✓-*50	✓FwDH+ - Toggles

Table continues…

Feature/Action	Short Code	Default	Button
Forward Hunt Group Off	✓	✓-*51	✓FwDH-
Busy on Held	✓	✗	✓BusyH
Do Not Disturb On	✓	✓-*08	✓DNDOn - Toggles
Do Not Disturb Off	✓	✓-*09	✓DNDOf
Extn Login	✓	✓-*35*N#	✓Login
Extn Logout	✓	✓-*36	✓Logof

Related links

Group Operation on page 618

Example Hunt Group

The follow are simple examples of how a department might use the facilities of a hunt group.

1. Basic Hunt Group

Scenario	The Sales department want all sales related calls to be presented first to Jane, then Peter and finally Anne.
Actions	1. Create a hunt group named Sales and assign it an extension number. 2. Set the **Hunt Type** to **Sequential**. 3. Add Jane, Peter and Ann to the **User L** ist in that order. 4. Turn off queuing on the Queuing tab and voicemail on the Voicemail tab. 5. Route relevant calls to the Sales group by selecting it as the destination in the appropriate Incoming Call Routes.
Results	Any call received by the Sales hunt group is first presented to Jane if she is available. If Jane is not available or does not answer within 15 seconds the call is presented to Peter. If Peter is not available or does not answer within 15 seconds the call goes Anne. Since voicemail is not on, the call will continue to be presented around the group members in that order until it is answered or the callers hangs up.

2. Adding Voicemail Support

Scenario	A voicemail server has now been added to the system. The Sales department wants to use it to take messages from unanswered callers. When messages are left, they want Jane to receive message waiting indication.
Actions	1. Open the Sales hunt group settings and select **Voicemail On** on the Voicemail tab. 2. Select the User settings for Jane. On the **Source Numbers** tab, add the entry **HSales**.
Results	Once a call to the Sales group has been presented to all the available members, if it is still unanswered then the call will be redirected to the group's voicemail mailbox to leave a message. When a message has been left, the message waiting indication lamp on Jane's phone is lit.

3. Using the Queuing Facility

Scenario	The Sales department now wants calls queued when no one is available to answer. However if the number of queued calls exceeds 3 they then want any further callers directed to voicemail.
Actions	1. Open the Sales hunt group settings and select **Queuing On** on the **Queuing** tab. 2. Set the **Queue Limit** to **3**.
Results	When the Sales group are all on calls or ringing, any further calls to the group are queued and receive queuing announcements from the voicemail server. When the number of queued calls exceeds 3, any further calls are routed to the group's voicemail mailbox.

4. Using Out of Service Fallback

Scenario	During team meetings, the Sales department want their calls redirected to another group, for this example Support.
Actions	1. Open the Sales hunt group settings and select the **Fallback** tab. In the **Out of Service Fallback Group** field select the **Support** group. 2. Create a system short code ***88/Set Hunt Group Out of Service/300**. 3. Create a system short code ***89/Clear Hunt Group Out of Service/300**.

Table continues…

Results	Prior to team meetings, dialing *88 puts the Sales group into out of service mode. Its calls are then redirected to the Support group. Following the meeting, dialing *89 puts the Sales group back In Service.

5. Using a Night Service Time Profile

Scenario	Outside their normal business hours, the Sales department want their group calls automatically sent to voicemail. This can be done using a time profile and leaving the Night Service Fallback Group setting blank.
Actions	1. Create a Time Profile called **Sales Hours** and in it enter the times during which the Sales department are normally available. 2. Open the Sales hunt group settings and select the **Fallback** tab. 3. In the **Time Profile** field select **Sales Hours**.
Results	Outside the normal business hours set in the time profile, the Sales hunt group is automatically put into Night Service mode. Since no Night Service Fallback Group has been set, calls are redirected to voicemail.

Related links

Group Operation on page 618

CBC/CCC Agents and Hunt Groups

The use of and reporting on hunt groups is a key feature of call center operation. For IP Office, reporting is provided through the Compact Business Center (CBC) or Compact Contact Center (CCC) applications.

In order for these applications to provide hunt group and hunt group user (agent) reports, the following rules apply:

- The hunt group names must be restricted to a maximum of 12 characters.
- The hunt group and user extension numbers should be a maximum of 4 digits.
- Hunt group members should be given a Login Code and set to Force Login.
- The agent state Busy Not Available is equivalent to Do Not Disturb. The agent state Busy Wrap Up is equivalent to hunt group disable.

Related links

Group Operation on page 618

Malicious Call Tracing (MCID)

MCID (Malicious Caller ID) is an ISDN feature. It is supported on BRI and PRI trunks to ISDN service provider who provide MCID.

When used, it instructs the ISDN exchange to perform a call trace on the user's current call and to keep a record of the call trace at the exchange for the legal authorities. Trace information is not provided to or displayed by the system or system phones.

The use of MCID is subject to local and national legal requirements that will vary. The feature may also not be enabled until specifically requested from the service provider. You should consult with your ISDN service provider and with appropriate legal authorities before attempting to use MCID.

Note:

Currently, in Server Edition network, MCID is only supported for users using an MCID button and registered on the same IP500 V2 Expansion system as the MCID trunks.

Activating MCID

1. **Liaise with the ISDN Service Provider** MCID should not be used without first confirming its usage with the ISDN service provider.
2. **Enabling MCID Call Tracing on a Line** BRI and PRI lines include a **Support Call Tracing Option** which by default is off.
3. **Enabling MCID Call Tracing for a User** Each user has a **Can Trace Calls** (**User | Telephony | Supervisor Settings**) option. This option is off by default.
4. **Providing an Active MCID Control** The user needs to be provided with a mechanism to trigger the MCID call trace at the exchange. This can be done using either a short code or a programmable button.

- **MCID Activate Button** The action **MCID Activate** (**Advanced | Miscellaneous | MCID Activate**) can be assigned to a programmable buttons. It allows a malicious call trace to be triggered during a call.
- **MCID Activate Short Codes** The feature **MCID Activate** can be used to create a short code to triggering a malicious call trace.

Related links

Configure User Settings on page 573

Message Waiting Indication

Message waiting indication (MWI) or a message lamp is supported for a wide variety of phones. It is used to provide the user with indication of when their voicemail mailbox contains new messages. It can also be configured to provide them with indication when selected hunt group mailboxes contain new messages.

Avaya digital and IP phones all have in-built message waiting lamps. Also for all phone users, the one-X Portal for IP Office application provides message waiting indication.

Related links

Configure User Settings on page 573
Message Waiting Indication for Analog Phones on page 629
Message Waiting Indication for Analog Trunks on page 630

Message Waiting Indication for Analog Phones

For analog phones, the system supports a variety of analog message waiting indication (MWI) methods. The method used for an individual analog extension is set for the **Extn | Analog | Message Waiting Lamp Indication Type** field. Those methods are

- **101V**
- **51V Stepped**
- **81V**
- **Bellcore FSK**
- **Line Reversal A**
- **Line Reversal B**
- **None**
- **On**

The 101V method is only supported when using a Phone V2 expansion module.

81V is typically used in European countries. 51V Stepped is used in most other countries. However the actual method used for a particular model of analog phone should be confirmed with the phone manufacturer's documentation.

The **Message Waiting Lamp Indication Type** field also provides options for **None** (no MWI operation) and **On**. **On** selects a default message waiting indication method based on the system locale.

'On' Method	Locale
81V	Belgium, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Netherlands, Norway, Poland, Portugal, Russia, Saudi Arabia, Sweden, Switzerland, United Kingdom.
51V Stepped	Argentina, Australia, Brazil, Canada, Chile, China, Colombia, Japan, Korea, Mexico, New Zealand, Peru, South Africa, Spain, United States.

For the United Kingdom system locale (eng), the default Caller Display Type (UK) allows updates of an analog phone's ICLID display whilst the phone is idle. The system uses this facilities to display the number of new messages and total number of messages in the users own mailbox. This feature is not supported with other Caller Display Types.

Hunt Group Message Waiting Indication

By default no message waiting indication is provided for hunt group voicemail mailboxes. Message waiting indication can be configured by adding an **H** entry followed by the hunt groups name to the Source Numbers tab of the user requiring message waiting indication for that hunt group. For example, for the hunt group Sales, add **HSales**. Hunt group message waiting indication does not require the user to be a member of the hunt group.

Related links

Message Waiting Indication on page 628

Message Waiting Indication for Analog Trunks

IP Office can provide a MWI for analog trunks from the PSTN network that terminate on an ATM4U-V2 card. Multiple users can be configured to receive a MWI from a single analog line. Users can receive an MWI from multiple lines. Configuring a user for MWI includes configuraton of a button for automatically dialing the message center.

Note the following conditions.

- Only supported for analog trunks terminating on the ATM4U-V2 card.
- When Analog Trunk MWI is selected as the Voicemail Type, no other voicemail system is active. As a result, hunt group queue announcements are not supported, since they require Embedded Voice Mail or Voicemail Pro.
- All analog trunks configured for MWI must use the same message center number. Multiple message centers are not supported.
- Not supported in One-X Portal.
- No TAPI is provided for analog trunk MWI status.
- Not supported across multiple IP Office systems. If the analog line is on a different node than the user's phone, that phone cannot receive an MWI for the line.
- Mobile twinning is not supported. Analog trunk MWI is displayed only on the master set.
- Internal twinning is not supported automatically. However, the twinned set can be configured to receive the same analog trunk MWI as the master set.

Configuring MWI for an Analog Trunk

1. Go to **System | Voicemail**. In the **Voicemail** field, select **Analog Trunk MWI**.
2. In the **Destination** field, enter the message center telephone number.
3. Select the **Line** you want to configure for Analog MWI, and then select the **Analog Options** tab.
4. In the **MWI Standard field**, select **Bellcore FSK**.
5. Select the **User** you want to configure for MWI and then select the **Button Programming** tab.
6. Select the button you want to configure and then click **Edit**.
7. In the **Action** field click the browse (...) button and select **Advanced > Voicemail > Monitor Analog Trunk MWI**.

8. In the **Action Data** field, enter the line appearance ID of the analog line.

Related links

Message Waiting Indication on page 628

Mobile Call Control

Mobile call control is only supported on digital trunks, including SIP trunks. It allows a user receiving a call on their twinned device to access system dial tone and then perform dialing action including making calls and activating short codes.

After answering a twinned call, the Mobile Call Control user can dial ** (within 1 second of each other) to place that call on hold and instead get dial tone from the system. Any dialing is now interpreted as if the user is logged into a basic single line extension on the system using their user settings. That also include user BLF status indication.

To use these features the user must be configured to support mobile call control.

Warning:

This feature allows external callers to use features on your phone system and to make calls from the phone system for which you may be charged. The only security available to the system is to check whether the incoming caller ID matches a configured users' **Twinned Mobile Number** setting. The system cannot prevent use of these features by caller's who present a false caller ID that matching that of a user configured for access to this feature.

Trunk Restrictions:

Mobile call control is only supported on systems with trunk types that can give information on whether the call is answered. Therefore, mobile call control is not supported on analog or T1 analog trunks. All other trunk types are supported (ISDN PRI and BRI, SIP (RFC2388), H323).

Routing via trunks that do not support clearing supervision (disconnect detection) should not be used.

DTMF detection is applied to twinned calls to a user configured for this feature. This will have the following effects:

DTMF dialing is muted though short chirps may be heard at the start of any DTMF dialing.

DTMF dialed by the user will not be passed through to other connected equipment such as IVR or Voicemail.

Mobile Call Control Features and FNE Services:

Mobile call control uses a short code set to invoke an FNE service. The codes relevant to mobile call control are summarized below.

- **FNE 31 = Mobile Call Control** This code allows a user called or calling the system to invoke mobile call control and to then handle and make calls as if they were at their system extension.

- **FNE 32 = Mobile Direct Access** Mobile direct access FNE32 immediately redials on switch the DDI digits received with the call rather than returning dial tone and waiting for DTMF digits as with FNE31 .
- **FNE 33 = Mobile Callback** Mobile callback allows the user to call the system and then hang up. The system will then make a call to the user's CLI and when answered, provide them with dial tone from the system to make calls.
- **FNE 35 = Simplified Mobile Call Control**: In addition to the Mobile Call Control feature that enables your mobile to make and handle calls as if your are using your extension, this Simplified Mobile Call Control FNE 35 clears the dial tone when the call recipient ends the call. The dial tone is provided on the mobile phone for fresh calls after the current call is cleared.
- **FNE 36 = Simplified Mobile Direct Access**: In addition to the Mobile Direct Access feature, the Simplified Mobile Direct Access FNE36 clears the dial tone when the call recipient ends the call.
- **FNE 37 = Simplified Mobile Callback**: In addition to the Mobile Callback feature that enables your mobile to get call back from the system and lets you use the dial tone for making and handling calls, this Simplified Mobile Callback FNE 37 clears the dial tone when the call recipient ends the call. The dial tone is provided on the mobile phone for fresh calls after the current call is cleared.

Using Mobile Call Control:

In addition to using ** to access mobile call control, the user has access to the following additional controls:

- **Clearing a Call: *52** It may be necessary to clear a connected call, for example after attempting a transfer and hearing voicemail or ringing instead. To do this dial **** for dial tone and then ***52** (this is a default system short code and can be changed if required).
- **Return to Dial Tone: ##** Return to dial tone after getting busy, number unobtainable or short code confirmation tones from the system.

Enabling Outgoing Mobile Call Control:

1. **Configure the user for Mobile Twinning and Mobile Call Control** On the User | Mobility tab do the following:

- Enable **Mobility Features** for the user.
- Set the **Twinned Mobile Number** for the user's twinned calls destination.

1. Digits are matched from right to left.
2. The match must be at least 6 digits. If either the CLI or the Mobile Twinned Number is less than 6 digits no match will occur.
3. Matching is done for up to 10 digits. Further digits are ignored. If either the CLI or Mobile Twinned Number is less than 10 digits, matching stops at that shorter length.

4. If multiple matches occur the first user in the configuration is used. Manager will warn against configuration where such a conflict may exist.

- Select **Can do Mobile Call Control**.

On systems with some unsupported trunk types, further changes such as Outgoing Group ID, system shorts codes and ARS may be necessary to ensure that calls to the mobile twinned numbers are only routed via trunks that support mobile call control.

Incoming Mobile Call Control:

The system can be configured to allow Mobile Call Control users to use this function when making an incoming call to the system. This requires the user to make the incoming call from the same CLI as their Mobile Twinning Number (even if they do not actually use Mobile Twinning).

The call will be rejected:

- If the caller ID is blank or withheld.
- If the caller ID does not match a Twinned Mobile Number of a user with **Can do Mobile Call Control** enabled.
- If the call is received on a trunk type that does not support Mobile Call Control.

Enabling Incoming Mobile Call Control:

On the **User | Mobility** tab do the following:

1. Enable **Mobility Features** for the user.
2. Set the **Twinned Mobile Number** to match the CLI of the device from which the user will be making calls.
3. Select **Can do Mobile Call Control**.

Add a FNE Short Code In the system short codes section of the configuration add a short code similar to the following. Key points are the use of the **FNE Service** feature and the **Telephone Number** value **31**.

- **Short Code**: *89
- **Feature**: FNE Service
- **Telephone Number**: 31

Add an Incoming Call Route for the user Create an incoming call route that matches the user's CLI and with the FNE short code created above as its destination.

On systems with some unsupported trunk types, further changes such as Incoming Group ID changes may be necessary to ensure that only calls received on trunks that support Mobile Call Control are routed to this short code.

Related links

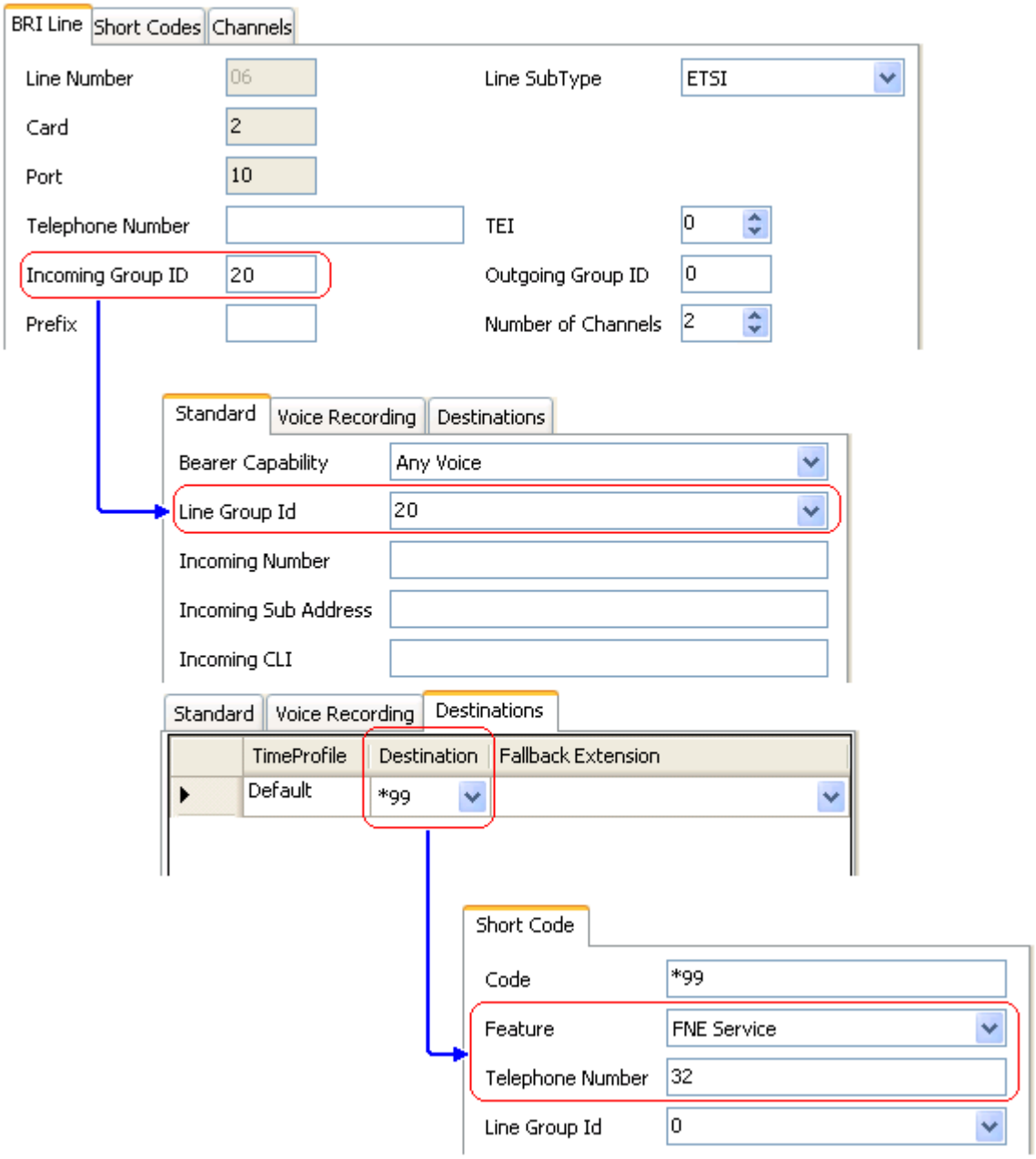
Configure User Settings on page 573
Mobile Direct Access (MDA) on page 634
Mobile Callback on page 635

Mobile Direct Access (MDA)

For a Mobile Call Control or one-X Mobile client user, FNE32 immediately redials on switch the DDI digits received with the call rather than returning dial tone and waiting for DTMF digits as with FNE31. This is called Mobile Direct Access (MDA).

MDA requires the user's external telephony provider to provide a direct trunk with DDI to the system (ie. an ISDN or SIP trunk). By assigning a specific incoming line group ID to the trunk, an incoming call route can be created for the same line group ID with blanks incoming number and incoming CLI fields. The destination is a short code set to FNE32.

User validation is performed using the CLI in the same way as for normal Mobile Call Control. In addition the call will be rejected no DDI digits are provided. Once connected the user can use the other Mobile Call Control features such as **.



Related links

Mobile Call Control on page 631

Mobile Callback

Mobile callback allows the user to call the system and then hang up. The system will then make a call to the user's CLI and when answered, provide them with dial tone from the system to make calls.

Mobile callback is subject to all the normal trunk type and user licensing restrictions of mobile call control. In addition the user must have the **Mobile Callback** (**User | Mobility**)setting enabled in the system configuration.

When the user makes a call using a DDI that is routed to an FNE33 short code, the system will not connect (answer) the call but will provide ringing while it waits for the user to hang up (after 30 seconds the system will disconnect the call).

- The system will reject the call if the CLI does not match a user configured for Mobile Callback or does not meet any of the other requirements for mobile call control.
- The system will reject calls using FNE33 if the user already has a mobile twinning or mobile call control call connected or in the process of being connected. This includes a mobile callback call in the process of being made from the system to the user.

If the CLI matches a user configured for mobile callback and they hang up within the 30 seconds, the system will within 5 seconds initiate a callback to that user's CLI.

- If the call is answered after the user's **Mobile Answer Guard** time and within the user's **No Answer Time**, the user will hear dial tone from the system and can begin dialling as if at their system extension.
- If the call is not answered within the conditions above it is cleared and is not reattempted.

Related links

Mobile Call Control on page 631

Twinning

Twinning allows a user's calls to be presented to both their current extension and to another number. The system supports two modes of twinning:

	Internal	Mobile
Twinning Destination	Internal extensions only	External numbers only.
Supported in	All locales.	All locales.
License Required	No	No

User BLF indicators and application speed dials set to the primary user will indicate busy when they are connected to a twinned call including twinned calls answered at the mobile twinning destination.

Do Not Disturb and Twinning

Mobile Twinning

Selecting DND disables mobile twinning.

Internal Twinning

- Logging out or setting do not disturb at the primary stops twinned calls alerting at the secondary also.

- Logging out or setting do not disturb at the secondary only affects the secondary.

Do Not Disturb Exceptions List

For both types of twinning, when DND is selected, calls from numbers entered in the user's Do Not Disturb Exception List are presented to both the primary and secondary phones.

Internal Twinning

Internal twinning can be used to link two system extensions to act as a single extension. Typically this would be used to link a users desk phone with some form of wireless extension such as a DECT or WiFi handset.

Internal twinning is an exclusive arrangement, only one phone may be twinned with another. When twinned, one acts as the primary phone and the other as the secondary phone. With internal twinning in operation, calls to the user's primary phone are also presented to their twinned secondary phone. Other users cannot dial the secondary phone directly.

- If the primary or secondary phones have call appearance buttons, they are used for call alerting. If otherwise, call waiting tone is used, regardless of the users call waiting settings. In either case, the **Maximum Number of Calls** setting applies.
-
- Calls to and from the secondary phone are presented with the name and number settings of the primary.
- The twinning user can transfer calls between the primary and secondary phones.
- Logging out or setting do not disturb at the primary stops twinned calls alerting at the secondary also.
- Logging out or setting do not disturb at the secondary only affects the secondary.
- User buttons set to monitor the status of the primary also reflect the status of the secondary.
- Depending on the secondary phone type, calls alerting at the secondary but then answered at the primary may still be logged in the secondary's call log. This occurs if the call log is a function of the phone rather than the system.
- Call alerting at the secondary phone ignoring any **Ring Delay** settings applied to the appearance button being used at the primary phone. The only exception is buttons set to No Ring, in which case calls are not twinned.

The following applies to internal twinned extensions:

If using a T3, 1400, 1600, 9500 or 9600 Series phone as the secondary extension:

- The secondary extension's directory/contacts functions access the primary user's Centralized Personal Directory records in addition to the Centralized System Directory.
- The secondary extension's call Log/call List functions access the primary user's Centralized Call Log.
- The secondary extension's redial function uses the primary users Centralized Call Log. Note that the list mode or single number mode setting is local to the phone.

It is also shown on 3700 Series phones on a DECT R4 system installed using system provisioning .

For all phone types, changing the following settings from either the primary or secondary extension, will apply the setting to the primary user. This applies whether using a short code,

programmable button or phone menu. The status of the function will be indicated on both extensions if supported by the extension type.

- Forwarding settings.
- Group membership status and group service status.
- Voicemail on/off.
- Do Not Disturb on/off and DND Exceptions Add/Delete.

Mobile Twinning

This method of twinning can be used with external numbers. Calls routed to the secondary remain under control of the system and can be pulled back to the primary if required. If either leg of an alerting twinned call is answered, the other leg is ended.

Mobile twinning is only applied to normal calls. It is not applied to:

- Intercom, dial direct and page calls.
- Calls alerting on line appearance, bridged appearance and call coverage buttons.
- Returning held, returning parked, returning transferred and automatic callback calls.
- Follow me calls.
- Forwarded calls except if the user's **Forwarded Calls Eligible for Mobile Twinning** setting is enabled.
- Hunt group calls except if the user's **Hunt Group Calls Eligible for Mobile Twinning** setting is enabled.
- Additional calls when the primary extension is active on a call or the twinning destination has a connected twinned call.

A number of controls are available in addition to those on this tab.

Button Programming Actions:

The **Emulation | Twinning** action can be used to control use of mobile twinning. Set on the primary extension, when that extension is idle the button can be used to set the twinning destination and to switch twinning usage on/off. When a twinned call has been answered at the twinned destination, the button can be used to retrieve the call at the primary extension.

Mobile Twinning Handover:

When on a call on the primary extension, pressing the **Twinning** button will make an unassisted transfer to the twinning destination. This feature can be used even if the user's **Mobile Twinning** setting was not enabled.

- During the transfer process the button will wink.
- Pressing the twinning button again will halt the transfer attempt and reconnect the call at the primary extension.
- The transfer may return if it cannot connect to the twinning destination or is unanswered within the user's configured **Transfer Return Time** (if the user has no **Transfer Return Time** configured, a enforced time of 15 seconds is used).

Short Code Features:

The following short code actions are available for use with mobile twinning.

- **Set Mobile Twinning Number**.
- **Set Mobile Twinning On**.
- **Set Mobile Twinning Off**.
- **Mobile Twinned Call Pickup**.

Related links

Configure User Settings on page 573

Private Calls

This feature allows users to mark a call as being private.

When on, any subsequent calls cannot be intruded on until the user's private call status is switched off. The exception is Whisper Page which can be used to talk to a user on a private call.

Note that use of private calls is separate from the user's intrusion settings. If the user's **Cannot be Intruded** (User | Telephony | Supervisor Settings) setting is enabled, switching private calls off does not affect that status. To allow private calls to be used to fully control the user status, **Cannot be Intruded** (User | Telephony | Supervisor Settings) should be disabled for the user.

Use of private calls can be changed during a call. Enabling privacy during a call will stop any current recording, intrusion or monitoring. Privacy only applies to the speech part of the call. Call details are still recorded in the SMDR output and other system call status displays.

Button Programming The button programming action **Advanced | Call | Private Call** can be used to switch privacy on/off. Unlike the short code features it can be used during a call to apply or remove privacy from current calls rather than just subsequent calls. On suitable phones the button indicates the current status of the setting.

Short Codes A number of short code features are available for privacy.

- **Private Call** Short codes using this feature toggle private status on/off for the user's subsequent calls.
- **Private Call On** Short codes using this feature enable privacy for all the user's subsequent calls until privacy is turn off.
- **Private Call Off** Short codes using this feature switch off the user's privacy if on.

Related links

Configure User Settings on page 573

System Phone Features

The user option **System Phone Rights** (User | User) can be used to designate a user as being a system phone user. System phone users can access a number of additional function not available

to other phone users. Note that if the user has a login code set, they will be prompted to enter that code in order to access these features..

- **None** The user cannot access any system phone options.
- **Level 1** The user can access all system phone options supported on the type of phone they are using except system management and memory card commands.
- **Level 2** The user can access all system phone options supported on the type of phone they are using including system management and memory card commands. Due to the nature of the additional commands a login code should be set for the user to restrict access.

..

The following functions are supported:

- **MENU to set date/time** Restricted to 4412, 4424, 4612, 4624, 6408, 6416 and 6424 phones where supported by the system. Note 4612 and 4624 not support for 4.1+. On these phones, a system phone user can manually set the system date and time by pressing **Menu | Menu | Func | Setup**.
- **SoftConsole Send Message** If the system phone user is using SoftConsole, they can access the SoftConsole function **Send Message** to send a short text message (up to 16 characters) to a display phone. Refer to the SoftConsole documentation for details. Note that this is no longer required for 4.0+.

Change Login Code of Other Users Using a short code with the Change Login Code feature, system phone users can change the login code of other users on the system.

Outgoing Call Bar Off Using a short code with the Outgoing Call Bar Off feature, system phone users can switch off the outgoing call bar status of other users on the system. .

Edit System Directory Records ..Using a 1400, 1600, 9500 or 9600 Series phone, a system phone user can edit system directory records stored in the configuration of the system on which they are hosted. .They cannot edit LDAP and/or HTTP imported records.

The following commands are only supported using 1400, 1600, 9500 and 9600 Series phones. Due to the nature of the commands a login code should be set for the user to restrict access. The commands are accessed through the **Features | Phone User | System Administration** menu. For full details refer to the appropriate phone user guide or the IP Office Installation manual.

System Management (IP500 V2 only) Allows the user to invoke a system shutdown command.

Memory Card Management Allows the user to shutdown, startup memory cards and to perform actions to move files on and between memory cards.

System Alarms (IP500 V2 only) For certain events the system can display an **S** on the user's phone to indicate that there is a system alarm. The user can then view the full alarm text in the phone's Status menu. The possible alarms in order of priority from the highest first are:

1. Memory Card Failure.
2. Expansion Failure.
3. Voicemail Failure.

4. Voicemail Full.
5. Voicemail Almost Full.
6. License Key Failure.
7. System Boot Error.
8. Corrupt Date/Time.

The following functions are not supported on analog, T3, T3 IP and wireless phones.

Date/Time Programmable Button: Allows system phone users to manually set the system date and time through a programmable button (see Self Administer and Date and Time).

Related links

Configure User Settings on page 573

The 'No User' User

It is possible to have an extension which has no default associated user. This can occur for a number of reasons:

- The extension has no **Base Extension** setting associating it with a user who has the same setting as their **Extension** to indicate that they are the extension's default associated user.
- The extension's default associated user has logged in at another extension. Typically they will be automatically logged back in at their normal extension when they log out the other phone.
- The extension's default associated user cannot be automatically logged in as they are set to **Forced Login**.

Phones with no current user logged in are associated with the setting of the **NoUser** user in the system configuration. This user cannot be deleted and their Name and Extension setting cannot be edited. However their other settings can be edited to configure what functions are available at extensions with no currently associated user.

By default the **NoUser** user has **Outgoing Call Bar** enabled so that the extension cannot be used for external calls. The users first programmable button is set to the **Login** action.

Avaya 1100 Series, 1200 Series, M-Series and T-Series phones, when logged out as **No User**, the phones are restricted to logging in and dial emergency calls only.

NoUser Source Numbers

The **SourceNumbers** tab of the **NoUser** user is used to configure a number of special options. These are then applied to all users on the system. For details refer to the **User | Source Numbers** section.

Related links

Configure User Settings on page 573
Suppressing the NoCallerId alarm on page 642

Suppressing the NoCallerId alarm

Use this procedure to suppress the NoCallerId alarm for all users on the system. Once the task is completed, the NoCallerID alarm is not raised in SysMonitor, SNMP traps, email notifications, SysLog or System Status.

Procedure

1. In Manager, in the navigation pane on the left, select **User**.
2. In the list of users, select **NoUser**.
3. In the details pane, select the **Source Numbers** tab.
4. Click **Add**.
5. In the **Source Number** field, enter **SUPPRESS_ALARM=1**.
6. Click **OK**.

Related links

The 'No User' User on page 641

Transferring Calls

The following are some of the methods usable to transfer calls.

Supervised Transfer This is a transfer where the user waits for the transfer destination to answer and talks to that party before completing the transfer, this is referred to as a consultation call. They then either complete the transfer or drop the call and return to the held for transfer call. The call details, display, ringing and forwarding applied are appropriate to the type of call (internal or external) being transferred.

Unsupervised Transfer This is a transfer completed whilst the destination is still ringing.

Automatic Transfer - Forwarding The system allows users to automatically transfer calls using forwarding options such as Forward on Busy, Forward on No Answer and Forward Unconditional. For full details see DND, Follow Me and Forwarding.

Transfers to a Forwarded Extension When transferring a call to another extension that has forwarding enabled, the type of call being transferred is used. For example, if transferring an external call, if the transfer target has forwarding of external calls enabled then the forward is used.

Transfer Return Time (secs): Default = Blank (Off), Range 1 to 99999 seconds. Sets the delay after which any call transferred by the user, which remains unanswered, should return to the user. A return call will continue ringing and does not follow any forwards or go to voicemail.

Transfer return will occur if the user has an available call appearance button.

Transfer return is not applied if the transfer is to a hunt group that has queuing enabled.

Tool	Unsupervised Transfer	Supervised Transfer	Reclaim
Analog Phone/ Single Line Phones	1. Press R. Note that broken dial tone is heard while a call is on hold. 2. Dial the transfer destination number. 3. Hang-up.	1. Press R. 2. Dial the transfer destination number. 3. If the destination answers and accepts the call, hang-up. 4. If the called party does not answer or does not want to accept the call, press Ragain. 5. To return to the original caller press R.	*46
Avaya DS Phone	1. Press **Transfer**. 2. Dial the transfer destination number. 3. Press **Transfer** again to complete the transfer.	1. Press **Transfer**. 2. Dial the transfer destination number. 3. If the destination answers and accepts the call, press **Transfer** again to complete the transfer. 4. If the called party does not answer or does not want to accept the call, press **Drop**. 5. To return to the original caller press it's call appearance button.	*46

Related links

Configure User Settings on page 573

Off-Switch Transfer Restrictions

Users cannot transfer calls to a destination that they cannot normally dial. This applies to manual transfers and also to automatic transfers (forwarding). In addition to call barring applied through short codes, the following system settings may restrict a users ability to transfer calls.

User Specific Controls

Outgoing Call Bar: Default = Off (**Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Supervisor Settings**) When enabled, this setting stops a user from making any external calls. It therefore stops them making any external transfers or forwards.

Inhibit Off-Switch Forward/Transfer: Default = Off (**Call Management** > **Users** > **Add/Edit Users** > **Telephony** > **Supervisor Settings**). When enabled, this setting stops the specific user from transferring or forwarding calls externally. This does not stop another user transferring the restricted users calls off-switch on their behalf.

When either system or user **Inhibit Off-Switch Forward/Transfer** is enabled, it affects the operation of the user's phone and applications. User attempts to set an external forward destination via a short code will receive error tone. User attempt to set an external forward destination via a programmable button on their phone will not have a Next option allowing the number to be saved.

Line Specific Control

Analog Trunk to Trunk Connection: Default = Off (**System Settings** > **Line** > **Add/Edit Trunk Line** > **Analog Line** > **Analog Options**) When not enabled, users cannot transfer or forward calls on one analog trunk back off-switch using another analog trunk.

System Wide Controls

Inhibit Off-Switch Forward/Transfer: Default = Off (**System Settings** > **System** > **Telephony**) When enabled, this setting stops any user from transferring or forwarding calls externally.

Restrict Network Interconnect: Default = Off (**System Settings** > **System** > **Telephony**). When this option is enabled, each trunk is provided with a Network Type option that can be configured as either **Public** or **Private**. The system will not allow calls on a Public trunk to be connected to a Private trunk and vice versa, returning busy indication instead.

Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.

Conference Control

Users can use conference controls to effectively transfer calls. This includes transferring an external call to another external number. The use of conferencing to effect off-switch transfers can be restricted using the **Inhibit External Only Impromptu Conference** setting (**System Settings** > **System** > **Telephony**).

Context Sensitive Transfer

Calls and Button Status Indication The status indication for a call on hold pending transfer has changed to differentiate such calls from standard held calls:

- On phones with both dual lamp buttons, both the green and red lamps fast flash (flutter) when the button represents a call on hold pending transfer.
- On phones with single lamp buttons or status icons, **Xfer**: is now shown in front of the caller ID information rather than the button name. For example **Xfer:Extn299** is shown rather than **a = Extn299**.
- The call status information shown when the button of a call on hold pending transfer is the currently highlight line is now prefixed with **On-Hold-Xfer** rather than **On-Hold**.

Switching Between Calls Switching from a connected call to an existing call on hold pending transfer puts the connected call on hold pending transfer. The following table is an example of the resulting operation .

Call or answer A	Connected to A
Press `Transfer`	A on hold pending transfer
Call or answer B	A on hold pending transfer. Connected to B.
Reconnect to A	Connected to A. B on hold pending transfer
Press `Transfer`or **Complete***.	A transferred to B.

Requirement for a Free Call Appearance Before Starting a Transfer When the user already has a call or calls on hold, they can now put their current call on hold pending transfer even if there are no free call appearances available. Previously an available call appearance was required in order to then make a consultation call to the potential transfer destination.

Conferencing Calls For these phone there have also been changes to which calls are conferenced in different scenarios including when there is a call on hold pending transfer. See Context Sensitive Conferencing.

Dial Tone Transfer

A user who is not able to make external calls to any or some external numbers, can be transferred to dial tone by a user who is able to make external calls.

- The restricted user wanting to make the external call, dials the unrestricted user and requests dial tone.
- The unrestricted user initiates a transfer and dials the prefix for an ARS form configured to provide secondary dial tone.

The prefix is a short code set up to access the required ARS form. While this can be a system short code, using a user or user rights short code will allow control over who can provide dial tone transfer for restricted users.

- When they hear the secondary dial tone, the unrestricted user completes the transfer.
- The restricted user now hears the secondary dial tone and is now able to make an external call.
- The restricted user is now able to make calls as permitted by the short codes in the ARS form.
- The restricted user is not able to transfer the dial tone to another user.

The ARS form being used can still contain short codes that restrict the dialing that can be attempted after the restricted user hears secondary dial tone. Other ARS features can also be used such as alternate routing or time profiles to provide out of hours routing. The ARS form timers are run from when the unrestricted caller dials the ARS form. They are not reset when the restricted user is transferred to the ARS form.

Multiple prefixes and ARS forms can be used if required to create more complex scenarios. For example, one where the unrestricted user can transfer the restricted users to an ARS forms that allows international calls or to an ARS form that only allows national dialing.

Example Configuration

The example below is a simple configuration that allows the unrestricted user to use 8 as a transfer destination that provides secondary dial tone.

Create an ARS Form for Secondary Dial Tone The ARS form needs to be created before short codes can be added to route callers to it.

- Enter a **Route Name** to identify the ARS form, for example **Dial Tone Trans**.
- Select **Secondary Dial Tone**.
- Select either **System Tone** (this matches locale specific normal dial tone) or **Network Tone** (this matches locale specific secondary dial tone). For some locales both tones are the same.
- Enter short codes that will take any digits dialed by the restricted user and process them for external dialing to an outgoing line group. For this example we will allow any digits dialed to be presented to the first trunk seized in outgoing line group 0.

Code	N
Telephone Number	N
Feature	Dial
Line Group ID	0

- Other short codes can be used to allow or bar the dialing of specific numbers or types of numbers.
- Configure the rest of the ARS form as required. For full details on ARS form configuration see ARS.

Create a Short Code for Dial Tone Transfer For this example we will allow the prefix 8 to be used to access an ARS form created above.

In the user short codes of the unrestricted user, create a short code that invokes the ARS form created above. For example:

Code	8
Telephone Number	
Feature	Dial
Line Group ID	51 Dial Tone Trans

- It is important that the short code does not pass any digits to the ARS form. Once the ARS form receives any digits, it starts short code matching and ends secondary dial tone.
- The short code could also be setup as a system or user rights short code.

The unrestricted user is now able to provide secondary dial tone to other users by on request by pressing **Transfer**, dialing **8** and then pressing **Transfer** again.

Account and Authorization Codes

If the restricted user enters an account or authorization code while calling the unrestricted user to request dial tone, that value is not carried forward with their external call once they have been provided with secondary dial tone.

If the unrestricted user enters an account or authorization code while dialing the ARS form, that value remains associated with the call made by the restricted user.

If the ARS form short code used to route the restricted users call requires an account or authorization code, the value already entered is used, otherwise the restricted user is prompted to enter a value.

Call Logging

The restricted user's outgoing call log will include the call to the unrestricted user and the outgoing external call they subsequently make. The outgoing external call record will include the prefix dialed by the unrestricted user to access the ARS form.

The unrestricted users call log will include just an incoming call from the restricted user.

Within the SMDR output, the calls by the restricted user are included. The call by the unrestricted user is not included.

Handsfree Announced Transfers

This feature allows the enquiry call part of a supervised transfer to be answered handsfree. In addition the system can be optionally configured to allow both the enquiry call and completed transfer call to be auto-answered.

Example

1. User 201 answers a call that they then want to transfer to user 203.
2. They press `TRANSFER`to put the call on hold pending transfer.
3. They then press a **Dial Direct** button and dial 203.
4. The transfer enquiry call is auto answered by User 203's phone. User 201 is able to announce the pending transfer and hear if User 203 wants to accept the call.

The auto-answer only occurs if the target user's extension is idle. If the target is already connected to a call, the transfer enquiry will be presented as normal call.

If the transfer is accepted, User 201 can press `TRANSFER`again to complete the transfer process.

The transferred call will then ring at the target. However, if required the system can be configured to also auto-answer the completed transfer.

Configuration

Handsfree announced transfers are supported when using one of the following features after having pressed **TRANSFER**.

Button Features	Short Code Features
Dial Direct Automatic Intercom Dial Intercom	Dial Direct

User Button Usability

Following the use of any of the buttons above, if the button has not been programmed with a specific target, a User button can be used to indicate the target for the enquiry call. This gives the advantage of being able to see the target user's status before attempting the transfer.

- For **Automatic Intercom** and **Dial Intercom** buttons without a pre-specified target, the **User** button must be on a button module.
- For **Dial Direct** buttons without a pre-specified target, the **User** button can be on the phone or button module. Due to this and the support for **Dial Direct** across a network of systems, we recommend that a **Dial Direct** button is used for handsfree announced transfers.

Phone Support

Handsfree announced transfer is supported for calls being transferred to the following phones:

Full Support	Partial Support	Not Supported
The following system phones support full announced transfer operation. **1603, 1608, 1616, 2410, 2420, 5410, 5420, 4610, 4621, 4625, 5610, 5620, 5621.** **Analog Off-Hook Stations** (See notes below).	The following phone can auto-answer announced transfers but require the user to use the handset to respond. **2402, 4601, 4602, 5402, 5601, 5602**.	Announced transfer is not supported for any phones not listed in the other column. On unsupported phones the transfer eqnuiry consultation call will be presented as a normal call.

Notes

On supported phones, if the target user's phone is not idle when the enquiry call attempt is made, the enquiry call is turned into a normal transfer attempt, eg. alerting on an available call appearance.

Enabling the extension specific setting Disable Speakerphone will turn all auto-answer calls, including handsfree announced transfers to the extension, into normal calls.

Off-Hook Station Analog Phones Analog phone extensions configured as Off-Hook Station can auto-answer transfers when off-hook and idle.

Headset Users The following applies to users on supported phones with a dedicated **HEADSET** button. These users, when in headset mode and idle will auto-answer the announced transfer enquiry call through the headset after hearing 3 beeps. The transfer completion will require them to press the appropriate call appearance unless they are set to Headset Force Feed.

Twinning Handsfree announced transfer calls to users with twinning enabled will be turned into normal calls.

Multi-site network Support Dial Direct is supported to targets across a multi-site network, therefore allowing handsfree announced transfers to remote users.

Full Handsfree Transfer Operation

If required the system can be configured to allow the full handsfree announced transfer process, ie. both the enquiry call and the transfer, to be auto-answered on supported phones. This is done

by entering **FORCE_HANDSFREE_TRANSFER** into the Source Numbers of the NoUser user and rebooting the system

One Touch Transferring

This feature allows selected users to transfer calls to each other using a reduced number of key presses.

With this option, a call can be transferred by simply selecting the transfer destination and then hanging up (or pressing **Transfer** if working handsfree).

Without this option the normal sequence is to press `Transfer`, dial the destination and then hanging up (or pressing **Transfer** if working handsfree).

For one touch transfer the transfer destination number must be selected using a button programmed to one of the following features:

- **User**
- **Dial**
- **Abbreviated Dial**
- **Automatic Intercom**
- **Dial Intercom**
- **Dial Direct**

This feature is enabled on a per user basis by adding **Enable_OTT** to the user's Source Number settings. This feature is supported on all Avaya phones that support the programmable button features above except T3 phones.

Centrex Transfer

Centrex Transfer is a feature provided by some line providers on external analog lines. It allows the recipient of a calls on such a line to transferred that call to another external number. The transfer is then performed by the line provider and the line is freed. Without Centrex Transfer, transferring an external call to another external number would occupy both a incoming and outgoing line for the duration of the call.

The following are the supported controls and usages for Centrex Transfer:

- **Centrex Transfer Button Operation** The action **Flash Hook** (**Advanced | Miscellaneous | Flash Hook**) can be assigned to programmable buttons on DS and IP phones. This button can be configured with or without a telephone number for an automatic or manual transfer respectively.
  - **Manual Transfer** If the programmable button is setup as a Flash Hook button without a target telephone number, pressing the button returns dial tone to the user. They can then dial the required transfer number and when they hear ringing or an answer, hang up to complete the Centrex Transfer.

- **Automatic Transfer** If the programmable button is setup as a Flash Hook button with a target telephone number, pressing the button performs the Centrex Transfer to the numbers as a single action.

- **Centrex Transfer Short Code Operation** The short code feature Flash Hook can be used with system short codes. It can be setup with or without a telephone number in the same way as a Flash Hook programmable button detailed above. The line group must be the group of analog lines from the Centrex service line provider.
  - **Centrex Transfer Operation for Analog Extensions** Most analog phones have a button that performs the action of sending a hook flash signal. The marking of the button will vary and for example may be any of R, H, Recall or Hold. For system analog extensions, pressing this button sends a hook flash to the system to hold any current call and return dial tone.
    - To perform a Centrex Transfer, pressing the analog extension's hook flash button should be followed by the dialing of a Flash Hook short code.
    - For analog extension users with Call Waiting enabled, pressing the hook flash button during a call will hold the current call and connect any call waiting. Therefore it is recommend that analog extension users wanting to use Centrex Transfer should not also have Call Waiting enabled.
  - **Transfer from Voicemail/Auto-Attendant** This operation is only supported through Voicemail Pro using an Assisted Transfer action with the destination set to a Flash Hook short code.

Additional Notes

Addition Prefix Dialing In some cases the Centrex service provider may require a prefix for the transfer number. If that is the case, that prefix must be inserted in the button programming or the short code used for the Centrex Transfer.

Application Transfers Centrex Transfer is not supported for calls being held and transferred through applications such as SoftConsole.

Conference Calls Centrex Transfer is not supported with conference calls.

Chapter 12: Configure Server Edition system settings

Synchronizing Server Edition passwords in Web Manager

In order to open IP Office Manager for a Server Edition solution, all IP Office systems in the solution must have a service user with common credentials. If the security settings on any system are reset, service user passwords are reset to the default value. In this case, when a system does not have a service user with common credentials, launch of IP Office Manager fails.

Before you begin

You must know the user ID and password of the service user that is common to all systems in the solution.

Procedure

1. For the system where the security settings were reset, open Web Manager using the address `https://<ip_address>:7070/WebManagement/WebManagement.html`.
2. Log on as **Administrator**.
3. In Web Manager, select **Security Manager** > **Service Users**.
4. Create the common service user.
5. Log out of this Web Manager session.
6. Start another Web Manager session on the system using the address `https://<ip_address>/index.html`.
7. Log on as the common service user.
8. In Web Manager, select **Security Manager** > **Service Users**.
9. Click **Synchronize Service User and System Password**.
10. Select **Applications** > **IP Office Manager**.

Related links

Applications on page 448

Shared Administration User Account

About this task

When managing multiple systems, it may be useful to create a common user name and password on all the systems for configuration access. This tool can be used to create a new service user account, **SCN_Admin**, for configuration access.

This process requires you to have a user name and password for security configuration access to each of the systems.

Managing a Common Configuration Administration Account

Procedure

1. Select **Tools | Server Edition Service User Management**.
2. The **Select IP Office** menu displays the list of discovered systems.
3. Select the systems for which you want to create a common configuration account.

   Typically this should be all systems. Click **OK**.
4. A user name and password for security configuration access to each system is requested.

   Enter the values and click **OK**. If the same values can be used for all systems enter those values, select **Use above credentials for all remaining, selected IPOs**. If each system requires a different security user names and password, deselect **Use above credentials for all remaining, selected IPOs**.
5. The systems will be listed and whether they already have an **SCN_Admin** account is shown.
6. To create the **SCN_Admin** account on each system and set the password for those account click on **Create Service User**.
7. Enter the common password and click **OK**.
8. The password can be changed in future using the Change Password option.
9. Click **Close**.

Voicemail Administration

If the Voicemail Pro client application is installed on the same PC as Manager, it can be launched from Manager. If not already installed, the Voicemail Pro client application can be downloaded from the Primary Server via its web control menus. Refer to the Server Edition Deployment Guide.

Starting the Voicemail Pro Client

Using the following method automatically starts the Voicemail Pro client with information about the system to be administered.

1. In the Server Edition Solution View, select the server for which you want to administer the voicemail application that the server hosts. This can be either the Primary Server or Secondary Server. If **Solution** is selected, it is assumed that the voicemail server on the Primary Server is being administered.
2. Click on the  **Voicemail Administration** link on the right-hand edge of the menu.

Alternate Method

The Voicemail Pro client can . When started this way, it will be necessary to manually enter the IP address and other details of the system you want to monitor after starting the System Status Application.

Click **File | Advanced | Launch Voicemail Pro Client**.

Server Edition Resiliency

Related links

Voicemail Pro Resiliency on page 655
Avaya one-X Portal resiliency on page 657
Phone Resiliency on page 659
Configuring Resiliency on page 662

Resilience

A single Server Edition Primary server supports redundant hard disk drives and power supply units. You can also configure Alternate Route Selection.

Add a Server Edition Secondary to provide resilience at any level. The Server Edition Secondary Server provides resilience for the Server Edition Primary Server users, H.323 and SIP extensions, hunt groups, and voicemail without any administration. The Server Edition Secondary server can provide resilience for Avaya one-X® Portal for IP Office.

A Server Edition Expansion System can be backed up to either the Server Edition Primary, Server Edition Secondary, or another Server Edition Expansion System. The dual star Multi-Site Network topology when a Server Edition Secondary Server is present supports diverse routing between all nodes.

For Server Edition Select deployments, IP Office Lines (SCN trunks) can be configured between Server Edition Expansion Systems. Hunt groups can be configured local to the Expansion system and resiliency for hunt groups and phones can be configured, with failover to the Server Edition Primary, Server Edition Secondary, or another Server Edition Expansion System.

At all times, no server hardware is forced to be idle, enabling you decide whether to provide true redundancy, or shared resource resilience.

The IP Office Server Edition Solution provides resilience for supported H.323 phones, SIP endpoints, and DECT R4 deployments. IP Office Lines between systems can be configured to allow control to be automatically passed to a backup IP Office when the home system is not available.

Resilient components

The following components of IP Office Server Edition Solution are resilient:

- IP Office Server Edition
- Voicemail Pro server
- Avaya one-X® Portal server
- H.323 telephones
- SIP endpoints
- DECT R4
- Hunt groups
- Interdevice links
- Trunks
- Incoming Call Routes
- Management

Multisite network

A multisite network enhances resilience by providing the following capabilities:

- Transparency for most of the features
- Resilience of users and hunt groups
- Back up system for Voicemail Pro
- Network topology provides resilience
- None of the hardware is idle
- Simple to activate resilience

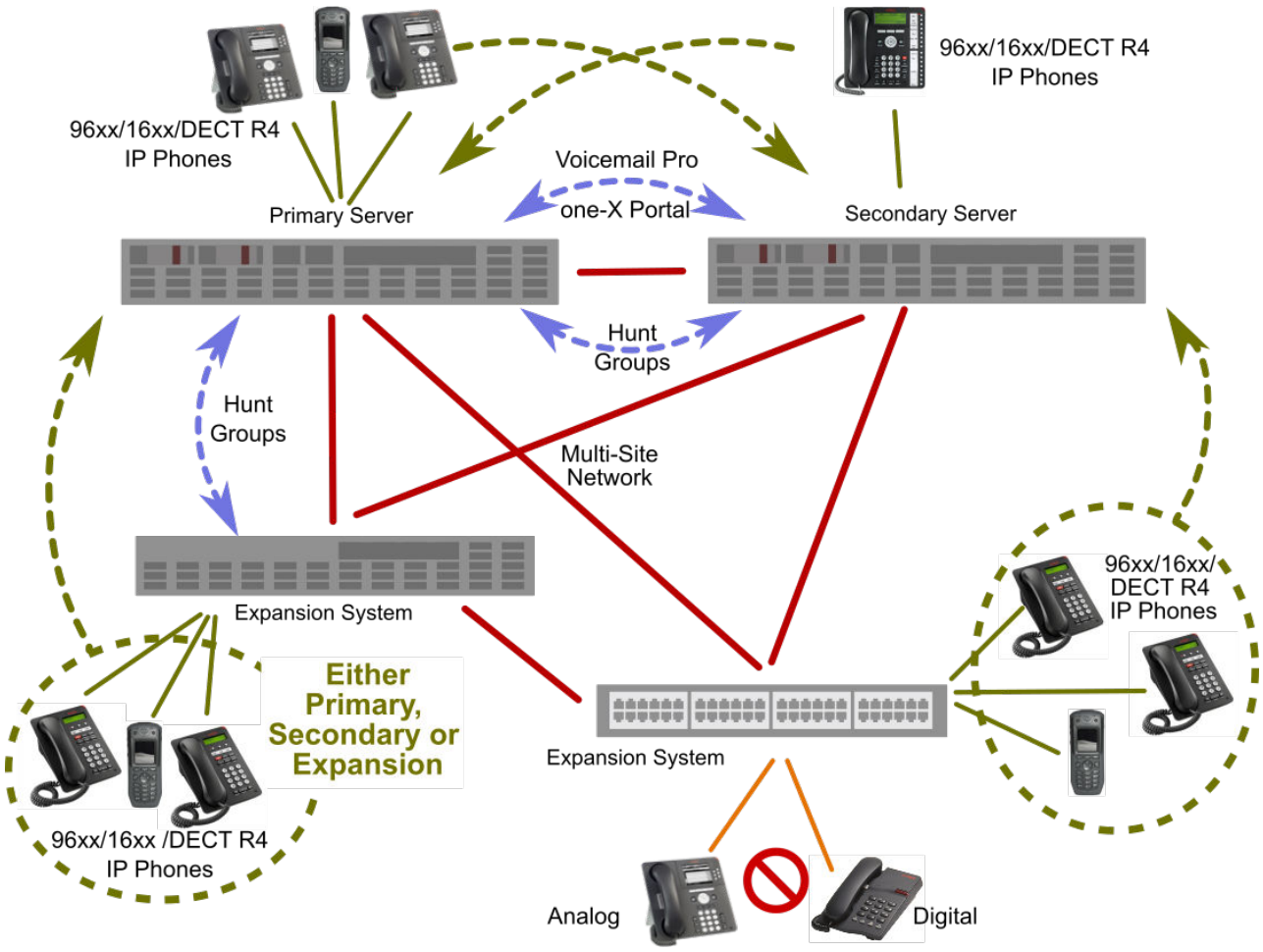


Figure 3: Resiliency Architecture

Resilient management

You can continue to administer and manage the failure of IP Office Server Edition server and devices in an IP Office Server Edition Solution network through the Server Edition Secondary Server. This provides management without the offline capability, and a facility to realign the configuration after the outages have been resolved. The resynchronization feature highlights the time and source of configuration change and enables the administrator to decide which change set to retain. In addition, you can directly manage each device and application to allow configuration whilst isolated. You can use the resynchronization capability to realign the configurations after the devices are reconnected.

Voicemail Pro Resiliency

One Active Voicemail Pro server

Server Edition supports one active Voicemail Pro server on the Server Edition Primary server. A backup Voicemail Pro server is supported on the Server Edition Secondary server for resiliency.

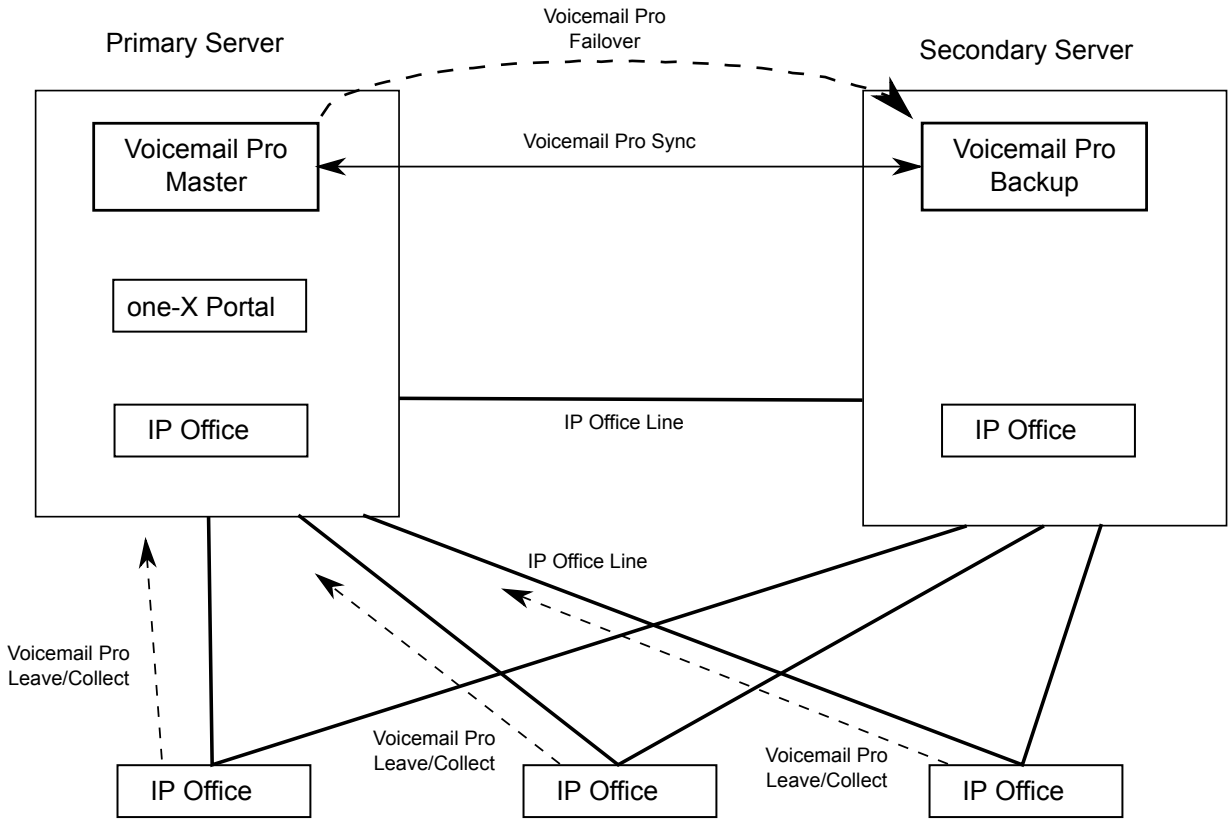


Figure 4: One active Voicemail Pro server

Dual Active Voicemail Pro servers

Server Edition deployments with Select licensing support two active Voicemail Pro servers, doubling the maximum channel capacity and dual processing locations. Each expansion system and all contained users can be configured to use one or the other. Each Voicemail Pro server provides backup for the other. The two Voicemail Pro servers are both active for a configured subset of users. They share a common configuration and message store. Each can support all mailboxes, message waiting indicators (MWI) and call flows under failure conditions.

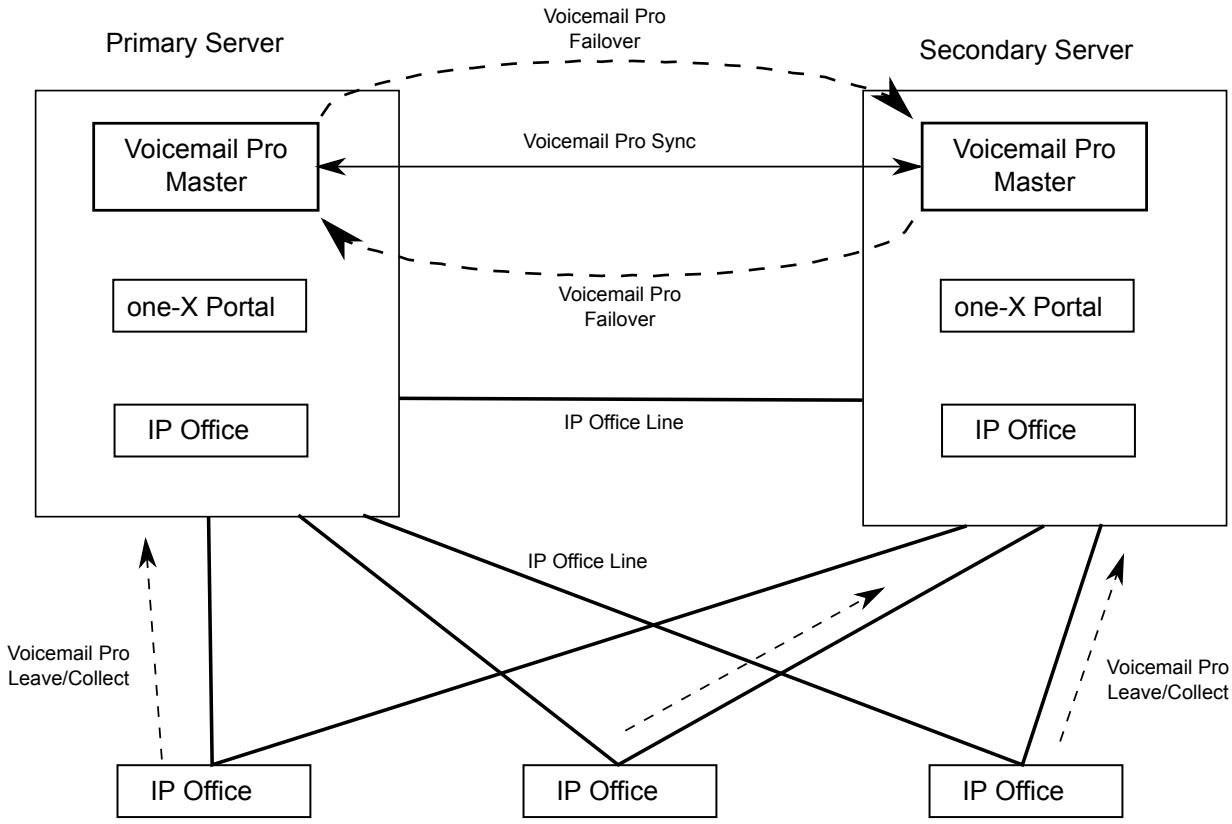


Figure 5: Dual Active Voicemail Pro servers

Supported Configurations

The following configuration are supported.

- Dual Voicemail Pro, each acting as a backup
- Dual Voicemail Pro, no backup operation
- Single master Voicemail Pro on Primary, no backup (non-Select)
- Single master Voicemail Pro on Primary and backup on Secondary (non-Select)
- Single master Voicemail Pro on Secondary and backup on Primary

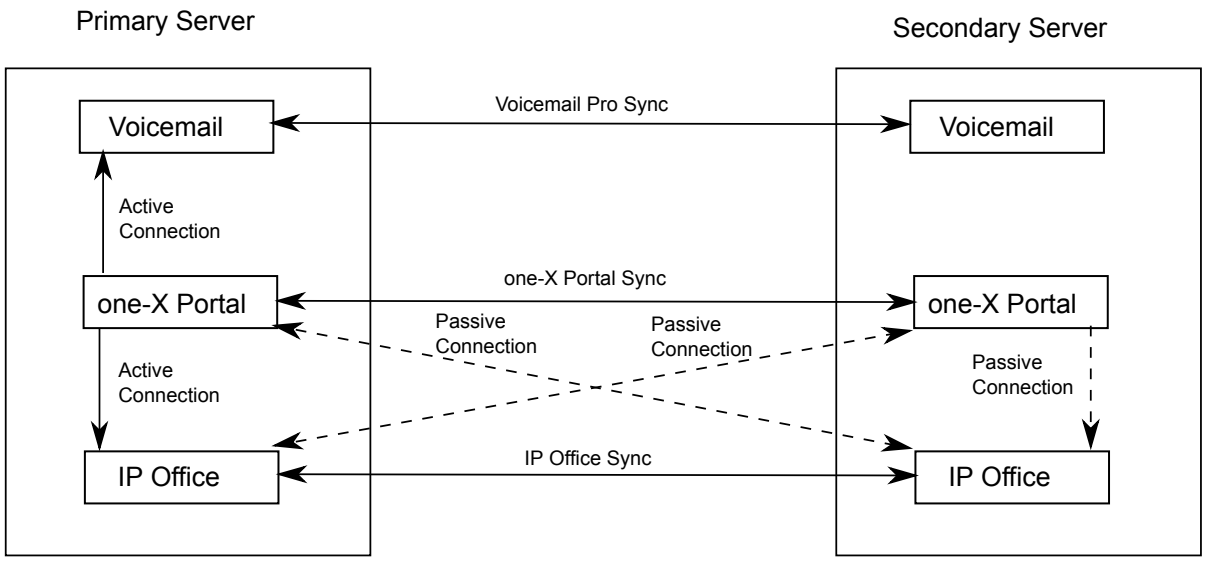
Related links

Server Edition Resiliency on page 653

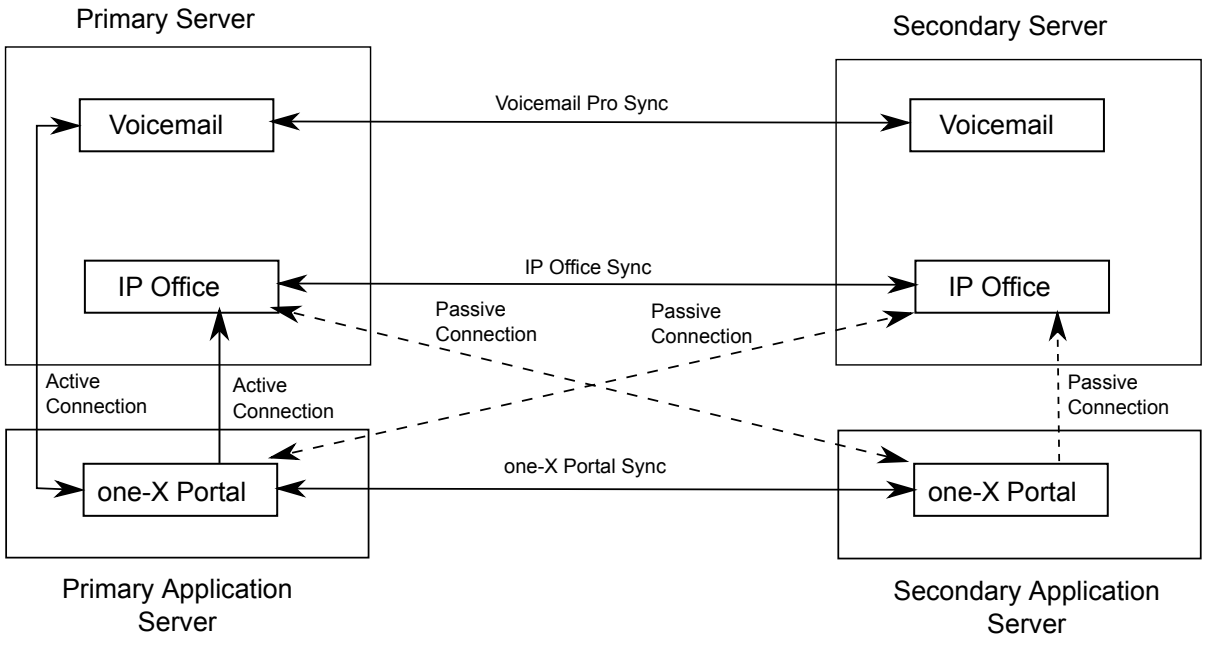
Avaya one-X® Portal resiliency

Server Edition Select deployments support a backup Avaya one-X® Portal server, providing resiliency for Unified Communication (UC) features. The resilient one-X Portal server is installed by default on the Server Edition Secondary server. Resilient one-X Portal servers can also be located on standalone application servers.

Resilient one-X Portal on the Server Edition Primary and Server Edition Secondary Servers



Resilient Avaya one-X® Portal on Standalone Application Servers



Avaya one-X® Portal Failover and Failback

When the primary Avaya one-X® Portal server is not available, failover occurs and the backup server becomes active. Clients automatically recognize that the primary Avaya one-X® Portal

server is not available and log in to the backup server. Logged in users are automatically logged in to the backup Avaya one-X® Portal server.

When the primary Avaya one-X® Portal server is once again available, users automatically failback to it. The backup Avaya one-X® Portal server redirects login requests to the primary Avaya one-X® Portal server.

If connectivity between the primary and backup Avaya one-X® Portal servers is lost for an extended time, both Avaya one-X® Portal servers become active and accept login requests. Once connectivity is reestablished, the two servers are synchronized and all users are logged in to the primary one-X Portal server.

Note:

When both Avaya one-X® Portal servers are active, any changes made by users logged in to the backup server will be lost when failback occurs.

one-X Portal Resiliency with IP Office and Voicemail Pro

If the Voicemail Pro server on the Server Edition Primary server is not available, the primary Avaya one-X® Portal server fails over to the Voicemail Pro server on the Server Edition Secondary server. When the Voicemail Pro server on the Server Edition Primary server is once again available, the primary Avaya one-X® Portal server automatically performs a failback to the Voicemail Pro server on the Server Edition Primary server.

Related links

Server Edition Resiliency on page 653

Phone Resiliency

Phone Failover

When phone resiliency is configured, the home system shares information about the registered phones and users on those phones with the backup system. If the home system is no longer visible to the phones, failover occurs and the phones register with the backup system.

Phone Failback

If the phone's home system has been up for more than 10 minutes, the system causes idle phones to perform a failback to the home system. If the phone is unable to connect to the home system, there is a five minute grace period, referred to as homeless prevention, where the phone can be logged in to either the home or backup system.

Automatic failback to the home system is the default mode. Failback can be configured to operate manually. This may be desired if for example, the home system will be unavailable for some time. In manual mode, failback does not occur until the phone has been logged out or rebooted.

Note:

Manual failback is not supported for SIP phones.

Configuration Options

Resiliency is configured on **IP Office Line** > **Line** under **SCN Resiliency Options**. The options are:

- **Backs up my IP Phones**
- **Backs up my Hunt Groups**
- **Backs up my Voicemail**
- **Backs up my IP DECT Phones**
- **Backs up my one-X Portal**

Notes on Phone Resiliency Behavior

- Failover handover takes a minimum of 3 minutes (longer for larger networks). This ensures that failover is not invoked when it is not required; for example, when the home system is simply being rebooted to complete a non-mergeable configuration change.
- Failover is only intended to provide basic call functionality while the cause of failover occurring is investigated and resolved. If users make changes to their settings while in failover, for example changing their DND mode, those changes will not apply after failback.
- Calls anchored on the home system lose all voice paths during failover. Direct media calls in a stable state might maintain voice paths until the next call event, but this is not guaranteed.

  Media preservation is not supported on SIP phones.
- If the failover system is rebooted while it is providing failover services, the failover services are lost.
- Failover features require that the phones local to each system are still able to route data to the backup system when the home system is not available. This will typically require each system site to be using a separate data router.
- When an IP phone fails over, the backup system allows it to operate indefinitely as a “guest”, but only until the system resets. Licenses will never be consumed for a guest phone.
- Hot desking users are automatically logged out. When their base extension fails back to the home system, the user is automatically logged in on their base extension.
- The media security configuration should be the same on all systems. For example, if an extensions home system is set to **Best Effort**, the failover system should also be set to **Best Effort**.
- For secure communication using TLS/SRTP, all IP Office systems must have an identity certificate that has been signed by the same trusted root CA.

  Note:

  - Authentication of the client's certificate by the server is not a requirement. IP Office does not support client certificate validation for all SIP endpoint types.

Supported Network Configurations

Phone resiliency is supported between any IP Office systems linked through an IP Office Line with **Networking Level** set to **SCN**. This includes failover from an IP500 V2 system to another IP500 V2 system.

For Server Edition deployments, failover from one node to any other node in the solution is supported.

Note:

Resiliency can be configured by specifying a **Location** with a unique IP address for the backup system. For cloud deployments, some systems cannot be configured as a **Location**. See Configuring Location Based Resiliancy on page 666.

Supported Phones

Phone resiliency is supported on the phones listed below. Each IP Office system can be the initial or backup system for a mixture of resilient phone types.

H.323 Phones:

- Resiliency is supported on 1600 and 9600 series phones.

SIP Phones:

The following SIP phones are supported:

- 1120
- 1140
- 1220
- 1230
- E129
- B179
- H175

SIP Soft Clients:

The following SIP soft clients are supported. Note that for these client, resiliency is also dependent on Avaya one-X® Portalresilience.

- Avaya Equinox™ for Windows
- one-X Mobile Preferred for Android
- one-X Mobile Preferred for iOS

Note:

Resiliency is not supported for:

- Avaya Lync Plug-in
- IP Office SoftConsole

Notes on Supported Phones:

- E129, 1100 Series, 1200 Series, B179 and Avaya Equinox™ for Windows always attempt to register to multiple servers. The homeless prevention feature is not applicable to these phones.
- The B179 phone does not have a configuration file setting for the backup system. You must use the phone web interface to configure the **Secondary SIP Server** setting and the **Fallback Account** settings.
- For SIP phone resiliency, all IP Office systems in the Server Edition solution or SCN cluster must have the same **System** > **LAN** > **VoIP** > **SIP Domain** setting.

The **SIP Domain** is not the same as the IP Office fully qualified domain name (FQDN). They are not synonymous but can be related through DNS SRV A records. A single SIP Domain can include multiple SIP servers.

- On Avaya Communicator, the **System** > **LAN** > **VoIP** > **SIP Domain** value must be configured in the **Domain name** field under **Settings**.
- Remote worker SIP phones will not failover when the failover server is CPE and their home system is cloud based.

Related links

Server Edition Resiliency on page 653

Configuring Resiliency

Related links

Server Edition Resiliency on page 653

Configuring Resiliency Using the Resiliency Administration Tool

This process adjusts the settings of the IP Office lines between systems to indicate which lines are being used to give/receive fallback options and what fallback options.

Note:

You can activate the resilience for an expansion system either on a primary server or a secondary server only. You cannot activate the resilience for an expansion system on both the primary server and secondary server.

Procedure

1. On the Solution page, select **Configure** > **Resiliency Administration**
2. The **Resiliency Administration** page opens.

   Select the options required.

   - **Backup Primary Server IP Phones, Hunt Groups, Voicemail and one-X Portal on Secondary Server** When selected, the Secondary Server will support hunt group operation during any failure of the Primary Server. Also when selected, the Secondary Server will support the continued operation of Avaya IP phones normally registered to the Primary Server.
   - **Backup Secondary Server IP Phones on Primary Server** When selected, the Primary Server will support the continued operation of Avaya IP phones normally registered to the Secondary Server.
   - **Backup Expansion Systems**
     - For each expansion system, you can select to **Backup Phones** and **Backup Hunt Groups** by clicking the check boxes.
     - In the **Resilient To** field, select the IP Office system that will act as the backup.

3. Click **Update**.

   The **SCN Resiliency Options** settings for the IP Office lines are adjusted to match the selections.

Linking Server Edition Expansion Systems

You can link Server Edition Select expansion systems with an IP Office Line in order to enable resiliency capability. When you link expansion systems using the Link Expansions tool, an IP Office Line is configured with default settings. You must select the security level for the line.

Procedure

1. Log in to Web Manager.
2. On the **Solution** page, click **Configure** > **Link Expansions**
3. In the Link Expansions window, in the **First Expansion** field, select an expansion system from the list.
4. In the **Second Expansion** field, select an expansion system from the list.
5. Under **Select Link Type**, select one of the following options:
   - **SCN Websocket (Secure)**: Recommended for security and NAT traversal.
   - **SCN Websocket**: Supports NAT traversal with limited security.
   - **SCN**: Legacy SCN line. Not recommended for new deployment.
6. If the Link Type is set to **SCN Websocket (Secure)** or **SCN Websocket**, you must configure a password.

Configuring Voicemail Pro Resiliency

Supported configurations are listed in the table below. A dual Voicemail Pro configuration is supported on Server Edition deployments with Select licensing.

Configuration Type	Voicemail IP Address on Primary	Backup Voicemail IP Address on Primary	Voicemail IP Address on Secondary	Backup Voicemail IP Address on Secondary
Dual Voicemail Pro, each acting as a backup	Primary Server IP Address	Secondary Server IP Address	Secondary Server IP Address	Primary Server IP Address
Dual Voicemail Pro, no backup operation	Primary Server IP Address		Secondary Server IP Address	
Single master Voicemail Pro on Primary, no backup **[1]**	Primary Server IP Address			

Table continues…

Configuration Type	Voicemail IP Address on Primary	Backup Voicemail IP Address on Primary	Voicemail IP Address on Secondary	Backup Voicemail IP Address on Secondary
Single master Voicemail Pro on Primary and backup on Secondary **[1]**	Primary Server IP Address	Secondary Server IP Address		
Single master Voicemail Pro on Secondary and backup on Primary			Secondary Server IP Address	Primary Server IP Address

Notes:

1. Non-Select.
2. For resiliency operation, you must also ensure that the default SMTP Sender setting of the voicemail server is set to be the server's fully qualified domain name. Within the voicemail server preferences, select **System Preferences | Email | SMTP Sender**. The **Domain** and **Server** fields of the first entry must be set to the fully-qualified domain name of the voicemail server, not ***local host***. This needs to be done on both the primary and secondary voicemail servers.

Procedure

1. Log in to Web Manager.
2. On the menu bar, click **System Settings** and then select **System**.
3. On the Systems page, locate the Primary server and then click on the **Server Menu** icon on the right.

   The System Configuration page for the Primary Server opens.
4. In the navigation pane on the left, select **Voicemail**.
5. In the **Voicemail Type** field, select **Voicemail Lite/Pro**.
6. Set the **Voicemail IP Address** and **Backup Voicemail IP Address** as required based on the table above.
7. Repeat for the Secondary server configuration.

Configuring one-X Portal Resiliency

Use this procedure to turn on one-X Protal Resiliency. Note that if resiliency is not turned on, the one-X Portal server on the Server Edition Secondary remains in a stopped state.

Procedure

1. Log in to Web Manager.
2. Select **System Settings** > **Lines**.

3. Select the **IP Office Line** connection from the Primary server to the Secondary Server and click the edit icon.
4. On the **Line** page, set **Back up my one-X Portal** to **Yes**.

Next steps

You must configure resiliency on one-X Portal. See the section “Resilience” in *Administering Avaya one-X® Portal for IP Office™ Platform* .

Configuring Phone Resiliency

Procedure

1. Using Web Manager, log in to the backup system that phones will failover to.
2. On the menu bar, click **System Settings** and the select **Lines**.
3. On the Lines page, locate the IP Office Line that connects to the home system and then click the edit icon on the right.

   The **Line** page is displayed.
4. Under **SCN Resiliency Options**, check the box for **Supports Resiliency**.
5. Check the boxes for the desired resiliency options.

   The options are:

   - **Backup my IP phones**
   - **Backup my Hunt Groups**
   - **Backup my Voicemail**
   - **Backup my IP DECT Phones**
6. Check the identity certificate on both IP Office systems to ensure they are derived from the same CA. See **Security Manager** > **Certificates**.
7. If you are configuring resiliency for SIP phones, the SIP Domain value must be the same on both the local and backup systems.
   a. On the menu bar, click **System Settings** and then select **Systems**.
   b. On the Systems page, locate the backup system and then click on the **Server Menu** icon on the right.
   c. On the System Configuration page, in the navigation pane on the left, select **LAN1**.
   d. Click the **VoIP** tab and record the **SIP Domain** value.
   e. Repeat the steps to find the **SIP Domain** value on the home system.
   f. Ensure the values are the same on both systems.

Configuring Manual Phone Failback

Automatic failback to the home system is the default mode. Failback can be configured to operate manually. This may be desired if for example, the home system will be unavailable for some time. In manual mode, failback does not occur until the phone has been logged out or rebooted.

Note:

SIP endpoints do not support manual phone failback.

Procedure

1. Using Web Manager, log in to the home system for the resilient phones.
2. On the menu bar, click System Settings and the select System.
3. On the Systems page, locate the home system for the resilient phones and they click the **Server Menu** icon on the right.
4. On the System Configuration page, in the navigation pane on the left, click **Telephony**.

   The **Telephony** tab is displayed.
5. In the **Phone Fallback** field, select **Manual**.
6. Click **Update**.

Configuring Location Based Extension Resiliency

Server Edition Select location based resiliency allows you to create a group of extensions by applying a common **Location** value to each extension. You can then specify the fallback IP Office server for the group. The location based fallback overrides the system fallback configuration.
Using location based resiliency

- Phones on the Primary and Secondary server can fall back to an Expansion system
- Phones on an Expansion system can fall back to another Expansion system

Location based resiliency is supported on Avaya 1600 and 9600 series phones and all SIP endpoints.

Procedure

1. In Manager, open the **Location** page and define a location for the phone group.
2. If the phone group is in a remote location, you can define the **Time Settings** for the group.
3. In the **Fallback System** field, select the system where the phone group will fall back to.

   Note that the **Fallback System** list only contains systems where an IP Office Line has been configured.
4. Save the location.
5. For all phones that will be part of the group, open the extension page for the phone and select the new **Location**.

   Note that you can also set an IP address and subnet mask at the location level to match the phone IP addresses.
6. On the system where the extension is configured, open the **Line | IP Office Line** page.
7. Under **SCN Resiliency Options**, enable **Supports Resiliency**.

Synchronizing the Configurations

About this task

Normally during configuration of the Server Edition solution, records that are shared (Incoming Call Route, Time Profile, Account Code and User Rights) are automatically synchronized with the configuration of the individual servers as they are edited. However, when new servers are added to the network or systems have their configuration individually edited, it is possible that some share records may become out of synch with the Primary Server. This process can be used to re-establish the correct shared records.

Synchronizing the Configurations

Procedure

1. In the Server Edition Solution View, right-click on **Solution**.
2. Select **Synchronize Configurations**.
3. Select **Yes** to confirm the removal.

Starting Web Control

About this task

Web control is the term used for a set of web based administration menus used by Linux based servers. That includes the Primary Server, Secondary Server and Expansion System (L) in a Server Edition solution. The menus provide functions such as stopping and starting individual services being run by the server. The menus for the Primary Server provide special network functions such as backing up and upgrading the whole network.

Procedure

1. In the Server Edition Solution View, select the system for which you want to display its web control menus.

   The option is not available for Expansion System (V2).

2. Click on the  **Web Control** link on the right-hand edge of the menu.
3. The PCs default web browser is started with the address to the system.
4. When the login menu is displayed, login using the same configuration name and password as used for Manager configuration access.

Chapter 13: Configuring SIP Trunks

Related links

Overview

A growing number of service providers now offer PSTN access to businesses via public SIP trunk connections, either to extend their reach beyond their typical copper based network coverage areas, or so that multiple services (voice and internet access) can be bundled into a single network connection. Although detailed public SIP trunk service offerings vary depending on the exact nature of the offer from the specific service provider, SIP trunks can potentially provide several advantages compared to traditional analog or digital trunks. These advantages include:

- cost savings resulting from reduced long distance charges, more efficient allocation of trunks, and operational savings associated with managing a consolidated network
- simplified dialing plans and number portability
- geographic transparency for local accessibility creating a virtual presence for incoming calls
- trunk diversity and redundancy
- multi-media ready to roll out future SIP enabled applications
- fewer hardware interfaces to purchase and manage, reducing cost and complexity
- faster and easier provisioning

IP Office delivers functionality that enhances its ability to be deployed in multi-vendor SIP-based VoIP networks. While this functionality is primarily based on the evolving SIP standards, there is no guarantee that all vendors, interpret and implement the standards in the same way. To help the SIP service provider, Avaya operates a comprehensive SIP Compliance Testing Program referred to as GSSCP. Avaya's DevConnect program validates the operation of the IP Office solution with the service provider’s SIP trunk offering.

Related links

Configuring SIP Trunks on page 668

Configuring a SIP Trunk

This procedure provides the basic steps for configuring a SIP trunk between two IP Office systems.

Before you begin

- You must know the IP address of both ends of the trunk.
- You must have valid licenses on both IP Office systems.
- On Server Edition, make sure you have a non-zero value in the **SIP Trunk Sessions** field on the **License | Remote Server** tab. If you do not, you will see Monitor messages about insufficient licenses.

Procedure

1. In the Manager navigation pane, right click **Line** and select **New** > **SIP Line**.
2. Record the **Line Number** value that appears on the SIP Line page for use later.
3. In the **ITSP Domain Name** field, enter the domain name required by the far end.

   If nothing is configured in this field, then IP Office inserts the far end's **ITSP Proxy Address** from the **Transport** tab as the ITSP domain in the SIP messaging.
4. Use the default values for the remaining fields.
5. Select the **Transport** tab.
6. In the **ITSP Proxy Address** field, enter the IP Address of the far end.
7. Select the **SIP URI** tab.
8. Click **Add**.
9. Enter values for the **Incoming Group** and **Outgoing Group** fields.

   You can use the **Line Number** from the **SIP Line** tab for both values.
10. In the Manager navigation page, select **Incoming Call Route**.
11. On the **Standard** tab, in the **Line Group ID** field, enter the **Line Number** from the **SIP Line** tab.
12. Select the **Destinations** tab.
13. In the **Destination** column, replace the value with a period (“.”).
14. In the Manager navigation pane, select **Short Code**.
15. Add a short code to dial the trunk you have just added.
16. One end of the trunk is now configured. Save the configuration to the IP Office.

17. Using Manager, open the configuration for the IP Office at the other end of the SIP trunk and repeat the steps.

Related links

Configuring SIP Trunks on page 668

SIP Line Requirements

Use of SIP requires the following:

- **SIP Service Account** An account or accounts with a SIP internet service provider (ITSP). The method of operation and the information provided will vary. The key requirement is a SIP URI, a web address of the form **name@example.com**. This is the equivalent of a SIP telephone number for making and receiving calls via SIP.
- **Voice Compression Channels** SIP calls use system voice compression channels in the same way as used for standard IP trunks and extensions. For an IP500 V2 system, these are provided by the installation of VCM modules within the control unit. RTP relay is applied to SIP calls where applicable.
- **Licensing** SIP trunks require licenses in the system configuration. These set the maximum number of simultaneous SIP calls supported by the system.
- **Firewall Traversal** Routing traditional H.323 VoIP calls through firewalls often fails due to the effects of NAT (Network Address Translation). For SIP a number of ways to ensure successful firewall traversal can be used. The system does not apply any firewall between LAN1 and LAN2 to SIP calls.
  - **STUN (Simple Traverse of UDP NAT)** UDP SIP can use a mechanism called STUN to cross firewalls between the switch and the ITSP. This requires the ITSP to provide the IP address of their STUN server and the system to then select from various STUN methods how to connect to that server. The system can attempt to auto-detect the required settings to successfully connect. To use STUN, the line must be linked to the Network Topology settings of a LAN interface using the line's Use Network Topology Info setting.
  - **TURN (Traversal Using Relay NAT)** TCP SIP can use a mechanism called TURN (Traversal Using Relay NAT). This is not currently supported.
  - **Session Border Control** STUN does not have to be used for NAT traversal when SBC is between IP Office and the ITSP, since the SBCE will be performing NAT traversal.
- **SIP Trunks** These trunks are manually added to the system configuration. Typically a SIP trunk is required for each SIP ITSP being used. The configuration provides methods for multiple URI's from that ITSP to use the same trunk. For each trunk at least one SIP URI entry is required, up to 150 SIP URI's are supported on the same trunk. Amongst other things this sets the incoming and outgoing groups for call routing.
- **Outgoing Call Routing** The initial routing uses any standard short code with a dial feature. The short code's Line Group ID should be set to match the Outgoing Group ID of the SIP URI channels to use. However the short code must also change the number dialed into a

destination SIP URI suitable for routing by the ITSP. In most cases, if the destination is a public telephone network number, a URI of the form **123456789@example.com** is suitable. For example:

- **Code**: 9N#
- **Feature**: Dial
- **Telephone Number**: N"@example.com"
- **Line Group ID**: 100

While this can be done in the short code, it is not an absolute necessity. The ITSP Proxy Address or ITSP Domain Name will be used as the host/domain part.

- **Incoming Call Routing** Incoming SIP calls are routed in the same way as other incoming external calls. The caller and called information in the SIP call header can be used to match Incoming CLI and Incoming Number settings in normal system Incoming Call Route records.
- **DiffServ Marking** DiffServ marking is applied to calls using the DiffServer Settings on the System | LAN | VoIP tab of the LAN interface as set by the line's **Use Network Topology Info** setting.

SIP URIs

Calls across SIP require URI's (Uniform Resource Identifiers), one for the source and one for the destination. Each SIP URI consists of two parts, the user part (for example **name**) and the domain part (for example **example.com**) to form a full URI (in this case **name@example.com**). SIP URI's can take several forms:

- name@117.53.22.2
- name@example.com
- 012345678@example.com

Typically each account with a SIP service provider will include a SIP URI or a set of URI's. The domain part is then used for the SIP trunk configured for routing calls to that provider. The user part can be assigned either to an individual user if you have one URI per user for that ITSP, or it can also be configured against the line for use by all users who have calls routed via that line.

If the wildcard * is used in the SIP trunk's **Local URI**, **Contact** and **Display** fields, that SIP trunk will accept any incoming SIP call. The incoming call routing is still performed by the system incoming call routes based on matching the values received with the call or the URI's incoming group setting. For outgoing calls using this SIP URI, all valid short code CLI manipulations are used (transforming calling party number to ISDN will be ignored). For a full list of valid CLI manipulations, see “Telephone Number Field Characters” under Short Code Characters on page 694. For example, character ‘i’ is not supported since it sets calling party number plan to isdn and number type to national.

Resource Limitation

A number of limits can affect the number of SIP calls. When one of these limits is reached the following occurs: any further outgoing SIP calls are blocked unless some alternate route is available using ARS; any incoming SIP calls are queued until the required resource becomes available. Limiting factors are:

- the number of licensed SIP sessions.

- the number of SIP sessions configured for a SIP URI.
- the number of voice compression channels.
  - **SIP Line Call to/from Non-IP Devices** Voice compression channel required.
  - **Outgoing SIP Line Call from IP Device** No voice compression channel required.
  - **Incoming SIP Line Call to IP Device** If using the same codec, voice compression channel reserved until call connected. If using differing codecs then 2 channels used.

SIP Information Display

The full from and to SIP URI will be recorded for use by SMDR, CBC and CCC. For all other applications and for telephone devices, the SIP URI is put through system directory matching the same as for incoming CLI matching. First a match against the full URI is attempted, then a match against the user part of the URI. Directory wildcards can also be used for the URI matching.

Related links

Configuring SIP Trunks on page 668

SIP Prefix Operation

The prefix fields **Prefix**, **National Prefix**, **Country Code** and **International Prefix** are available with the SIP Line settings. These fields are used in the following order:

1. If an incoming number (called or calling) starts with the + symbol, the + is replaced with the **International Prefix**.
2. If the **Country Code** has been set and an incoming number begins with that **Country Code** or with the **International Prefix** and **Country Code**, they are replaced with the **National Prefix**.
3. If the **Country Code** has been set and the incoming number does not start with the **National Prefix** or **International Prefix**, the **International Prefix** is added.
4. If the incoming number does not begin with either the **National Prefix** or **International Prefix**, then the **Prefix** is added.

For example, if the SIP Line is configured with prefixes as follows:

- **Prefix**: 9
- **National Prefix**: 90
- **International Prefix**: 900
- **Country Code**: 44

Number Received	Processing	Resulting Number
+441707362200	Following rule 1 above, the + is replace with the **International Prefix** (900), resulting in 900441707362200. The number now matches the **International Prefix** (900) and **Country Code** (44).Following rule 2 above they are replace with the **National Prefix** (90).	**901707362200**
00441707362200	Following rule 2 above the **International Prefix** (900) and the **Country Code** (44) are replaced with the **National Prefix** (90).	**90107362200**
441707362200	Following rule 2 above, the **Country Code** (44) is replace with the **National Prefix** (90).	**901707362200**
6494770557	Following rule 3 above the **International Prefix** (900) is added.	**9006494770557**

OPTIONS Operation

Options are not sent only when active SIP registration is present. In all other cases, OPTIONS are sent.

The interval is determined as by the No User source number **SIP_OPTIONS_PERIOD=X** as follows.

- If no **SIP_OPTIONS_PERIOD** parameter is defined and the **LAN1 | Network Topology | Binding Refresh Time** is 0, then the default value of 300 seconds is used.
- To establish a period less than 300 seconds, do not define a **SIP_OPTIONS_PERIOD** parameter and set the **Binding Refresh Time** to a value less than 300 seconds. The OPTIONS message period will be equal to the **Binding Refresh Time**.
- To establish a period greater than 300 seconds, a **SIP_OPTIONS_PERIOD** parameter must be defined. The **Binding Refresh Time** must be set to a value greater than 300 seconds. The OPTIONS message period will be the smaller of the **Binding Refresh Time** and the **SIP_OPTIONS_PERIOD**.

Related links

Configuring SIP Trunks on page 668

SIP messaging

SIP trunk prerequisites

Before any calls can be made, the system must have sufficient SIP trunk licenses for the maximum number of simultaneous SIP trunk calls expected.

On Server Edition systems, the **System | Telephony | Telephony | Maximum SIP Sessions** value must match the total number of SIP extension and trunk calls that can occur at the same time.

Related links

Configuring SIP Trunks on page 668
Outgoing call message details on page 674
Incoming call message details on page 679
Codec selection on page 684
DTMF transmission on page 685
Fax over SIP on page 685
Hold scenarios on page 685
SIP REFER on page 687

Outgoing call message details

Related links

SIP messaging on page 674
Destination URI on page 674
From field content on page 675
To field content on page 675
Contact field content on page 676
P-Asserted Identity field content on page 676
Typical outgoing call scenarios on page 677

Destination URI

The destination URI in an INVITE message has the general format of an e-mail address. Specific rules have been defined for expressing telephone numbers in this format. These rules are defined in RFC 2806 and RFC 3261 (section 19.1.6). A sample URI for a call on a SIP trunk is:

```
sip: 12125551234@ITSP_Domain SIP/2.0
```

The **ITSP_Domain** in the following headers is taken from the **SIP Line | ITSP Domain Name** field. If that is empty, the IP Address of the IP Office LAN interface is used or the public address of that interface if topology discovery is used.

Related links

Outgoing call message details on page 674

From field content

If the call is originated from an IP Office endpoint, the settings on the **SIP line | SIP URI** tab determine whether the information should be taken from the trunk's SIP credentials, or from the **User | SIP** tab.

- If the channel's Local URI is set to * then the extension number is used for the User part of the identity.

  ```
  From: "SipDisplayNameAlice" <sip: 311@ITSP_Domain>;tag=8a9fed65b
  ```

- If the channel's Local URI is set to 'Use Internal Data' then the **User | SIP | SIP Name** will be used for the User part of the identity, and the ITSP Domain for the host part.

  ```
  From: "SipDisplayNameAlice" <sip: SipName@ITSP_Domain>;tag=8a9fed65b
  ```

- If the SIP Name field also contains a domain (indicated by the presence of @) then that domain will be used.

  ```
  From: "SipDisplayNameAlice" <sip: SipName@USER_Domain>;tag=8a9fed65b
  ```

- If Call-ID is blocked either by short code or if the **User | SIP | Anonymous** checkbox is checked then the From: header will be anonymous, unless the **SIP Line | Send From in Clear** checkbox is checked.

  ```
  From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=8a9fed65b
  ```

- If the channel's **Local URI** is set to **Use Credentials …** then there must first be at least one set of SIP Credentials defined, and that account selected in the channel's **Registration** dropdown selection box. The corresponding field from the **SIP Line | SIP Credentials** tab will be used for the User part of the identity.

  ```
  From: "Line17Cred2" <sip:Line17Cred2@ITSP_Domain>;tag=8a9fed65b
  ```

- The contact identity is populated similarly to the **From:** header. If Call-Id blocking is invoked: via **W** in a short code, or by checking the **User | SIP | Anonymous** checkbox then the **Contact:** field becomes semi-anonymous:

  ```
  Contact: <sip:anonymous@135.55.86.70:5060;transport=udp
  ```

Related links

Outgoing call message details on page 674

To field content

Since the identity of the called party is not known at the time of the initial INVITE, the **To:** field shows only the information necessary to route the call, which is the dialed digits after any short code and ARS manipulation, prefix manipulation, and removal of any end-of-dial digits (# in North America).

```
To: <sip: 12125551234@ITSP_Domain>
```

Related links

Outgoing call message details on page 674

Contact field content

The contact identity is populated similarly to the **From:** header. If Call-Id blocking is invoked: via **W** in a short code, or by checking the **User | SIP | Anonymous** checkbox then the **Contact:** field becomes semi-anonymous:

```
Contact: <sip:anonymous@135.55.86.70:5060;transport=udp
```

Related links

Outgoing call message details on page 674

P-Asserted Identity field content

Without Call-Id blocking, this field essentially mirrors the **From:** field.

P-Asserted-Identity: " SipDisplayName " <sip: SipName@ITSP_Domain>

Note:

You can enter the wildcard character “*”. Entering this value populates the SIP PAI header with the caller information available to IP Office.

Call-Id blocking: using **W** in a short code, or by checking the **User | SIP | Anonymous** checkbox results in the **P-Asserted** field being the only header that carries the calling party information, and so is unchanged from the non-blocked case above.

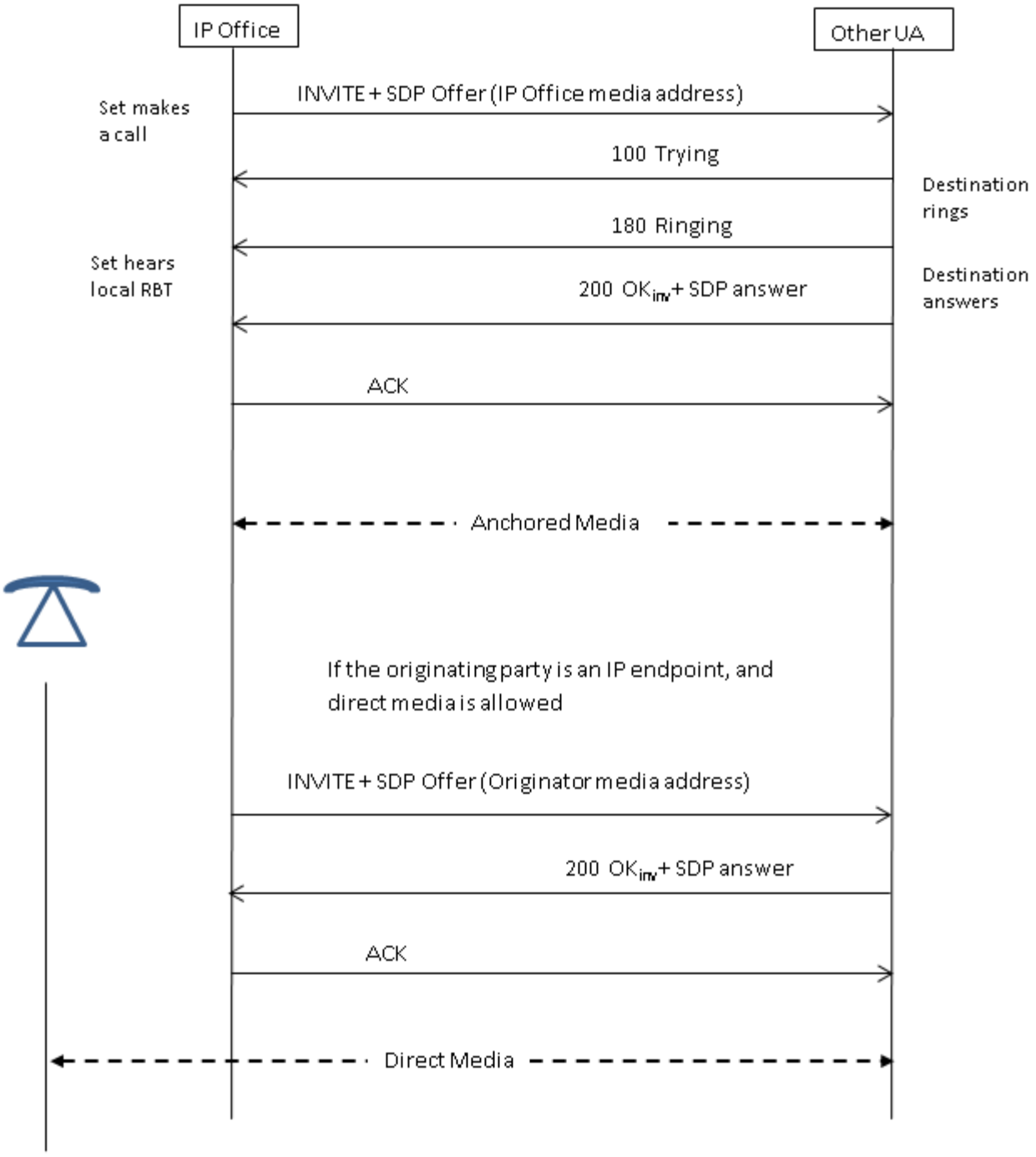
```
P-Asserted-Identity: " SipDisplayName" <sip:SipName@ITSP_Domain>
```

Related links

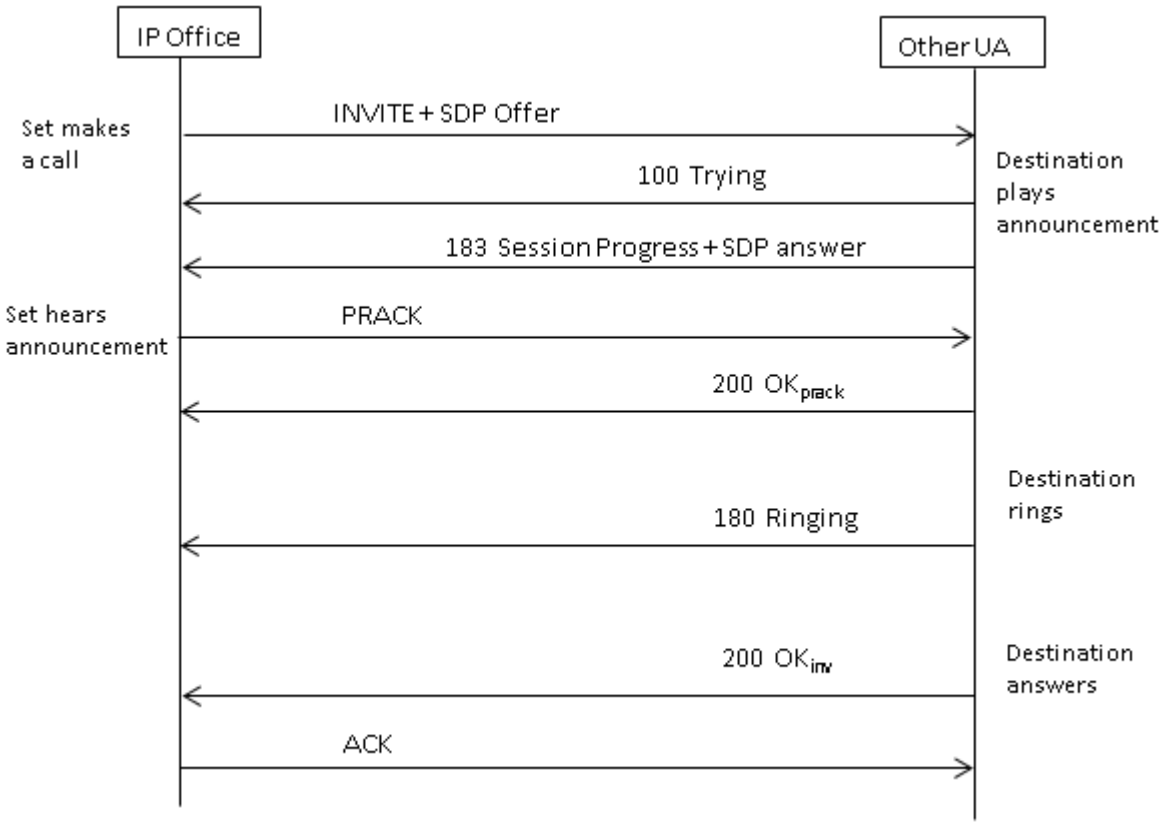
Outgoing call message details on page 674

Typical outgoing call scenarios

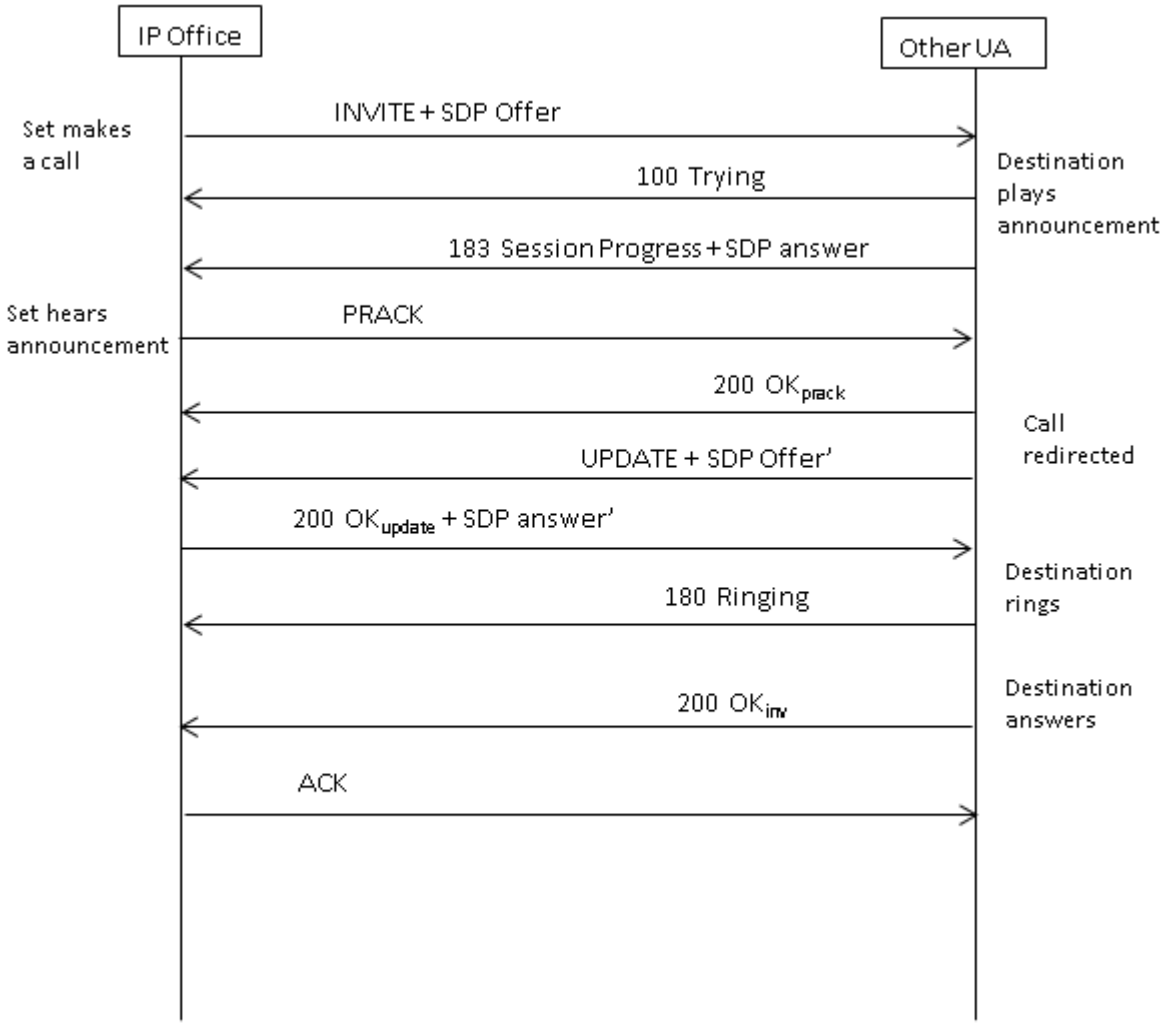
INVITE with SDP, local ringback



INVITE with SDP, early media



INVITE with SDP, early media re-directed by destination



Related links

Outgoing call message details on page 674

Incoming call message details

Related links

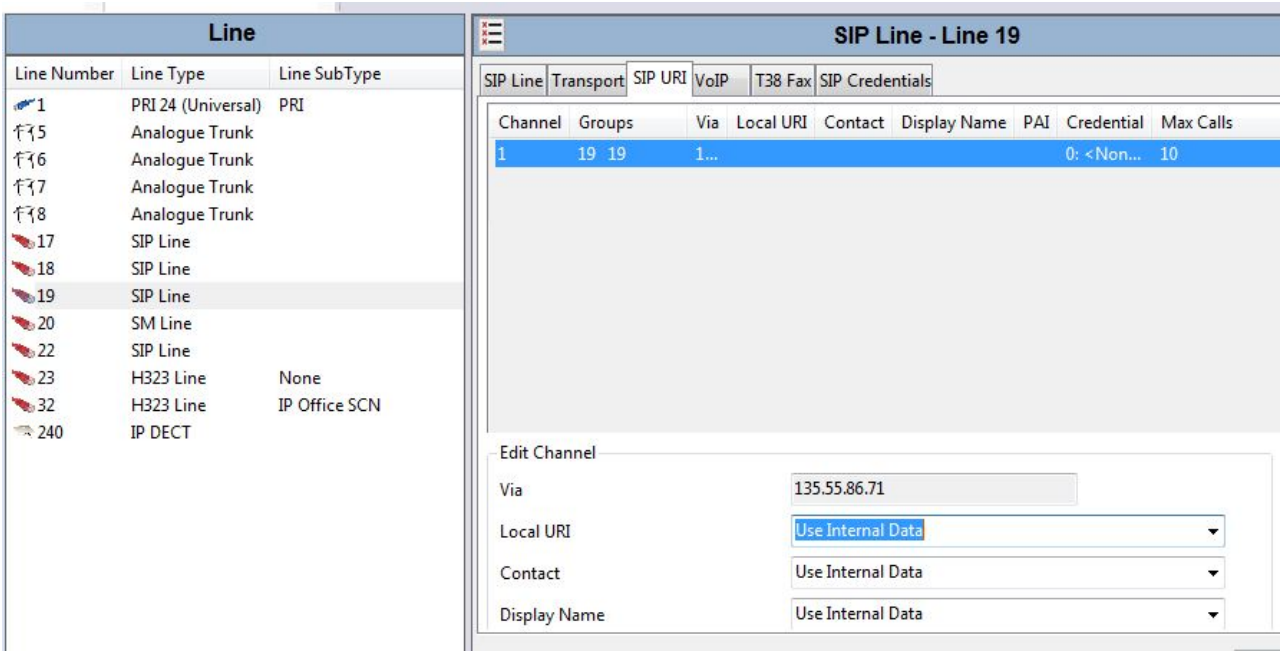
SIP messaging on page 674
Incoming call routing on page 679
Media path connection on page 680
Typical incoming call scenarios on page 681

Incoming call routing

When a SIP INVITE is received by IP Office, its origin is compared to the known IP addresses of the SIP lines configured. If a match is not found, then the INVITE is presented internally to the

extension interface to determine if it matches any of the registered terminals. SIP messages from unknown endpoints are discarded, and solicit no response from IP Office.

SIP lines have incoming and outgoing groups associated with them, which are configured on the **SIP line | SIP URI** tab. In the example below, the incoming and outgoing groups are both 19, and the **Local URI** specifies **Use Internal Data**. With this **Local URI** setting, to route a call to a user, the **User | SIP | SIP Name** field is used to match against the incoming digits.



The incoming group indicates the identity of an **Incoming Call Route**, which is used to match the incoming digits in the Request-URI to a target. That target could be an extension, a hunt group, another trunk, or an ARS entry.

Due to this grouping, calls incoming to several different trunks or trunk types can use the same **Incoming Call Route**, but in order for this to work,the **Local URI** must be manually set to <*>.

Incoming Call Routes are identified by the **Line Group ID** or optionally, an **Incoming Number** may be specified to match against in the received digits. Then a **Destination** specified, which may be a specific target, or may contain only a <.> to indicate that the digits are to be matched against known system targets.

Related links

Incoming call message details on page 679

Media path connection

IP Office does not provide in-band ringback to incoming SIP trunk calls. This is different from what is done for H.323. The only scenario in which an incoming SIP trunk call will hear in-band ringback occurs when the call terminates on an analog trunk. With analog trunks, the media path is cut through immediately because IP Office has no way of determining the state (ringing, busy, answered) of the trunk.

IP Office connects “early” media before the call is answered by sending a 183 Session Progress response only if the following two conditions are met:

- A PROGRESS (in-band tone indication OR 183 Session Progress with SDP) message is received from the destination (this can only happen in a SIP-to-PRI or SIP-to-SIP tandem scenario).
- The INVITE message contains SDP.

IP Office does not attempt to connect early media on PROGRESS when there is no SDP in the initial INVITE, since this is unlikely to succeed. The reason there is no SDP in INVITE is probably that the originating system does not know the originator’s media address yet. A typical scenario where this is the case occurs when the call on the originating system comes from an H.323 SlowStart trunk.

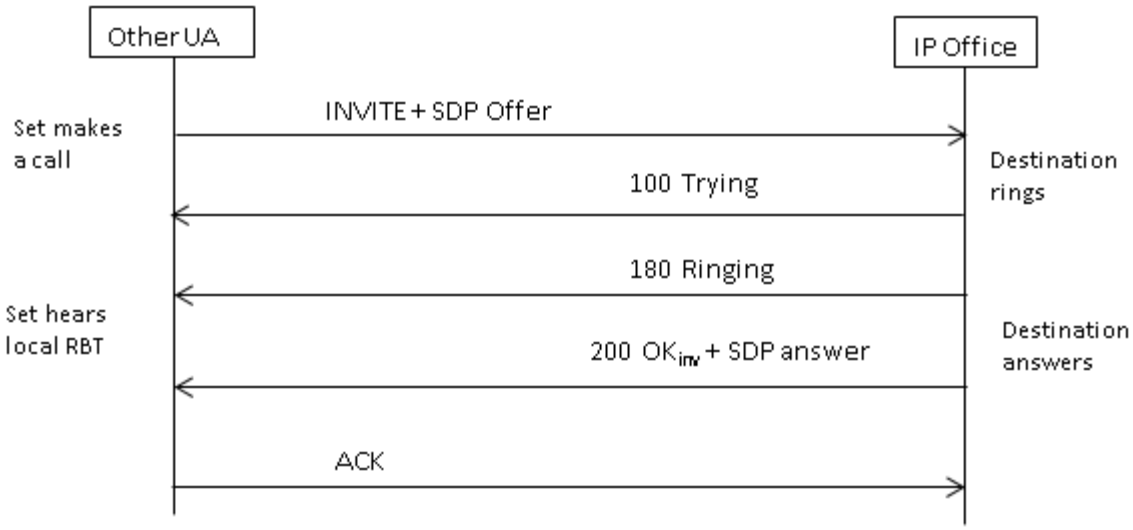
Related links

Incoming call message details on page 679

Typical incoming call scenarios

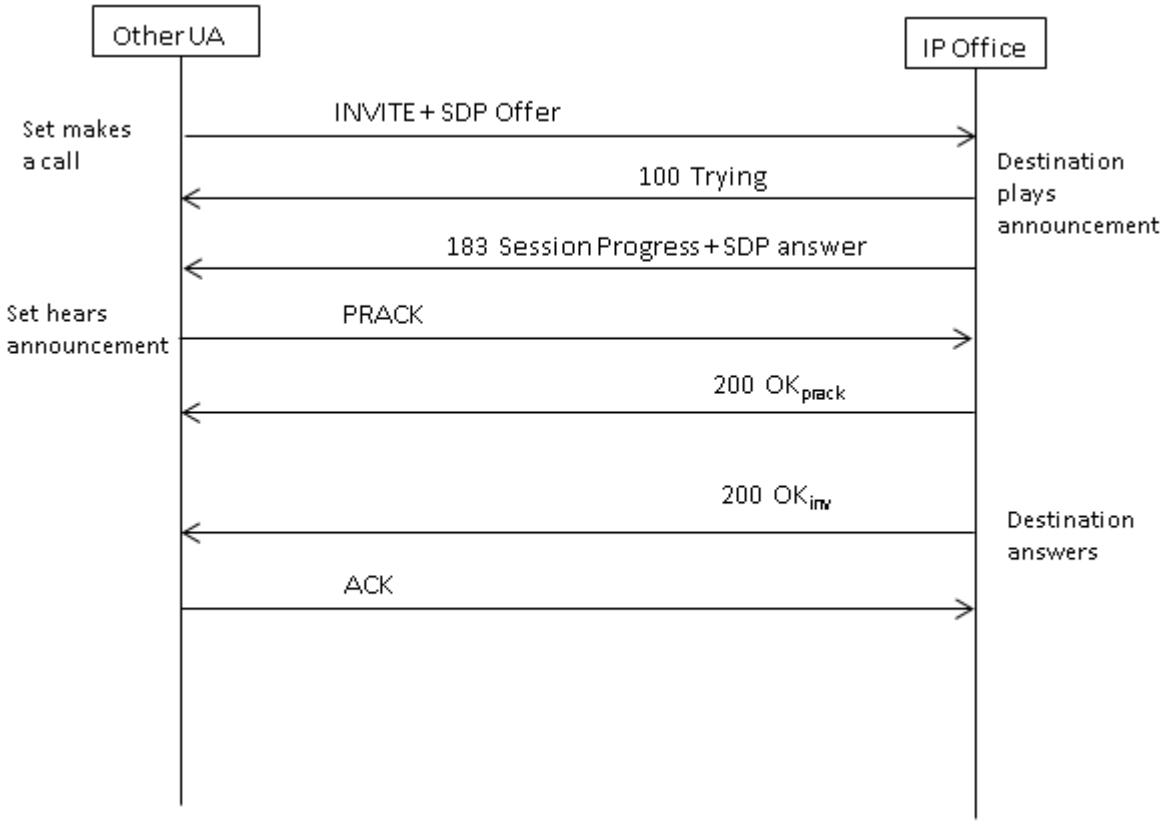
INVITE with SDP, local ringback

If the destination is an analog trunk, the 180 Ringing will be replaced with a 183 Progress with SDP followed immediately by a “fake” answer in order that the media will be connected right away so that the originator hears whatever in-band tones are present on the analog trunk (ringback or busy). If the target is an extension that is unconditionally call forwarded over an analog trunk, then there will be a 180 Ringing without SDP, followed immediately by the “fake” answer.



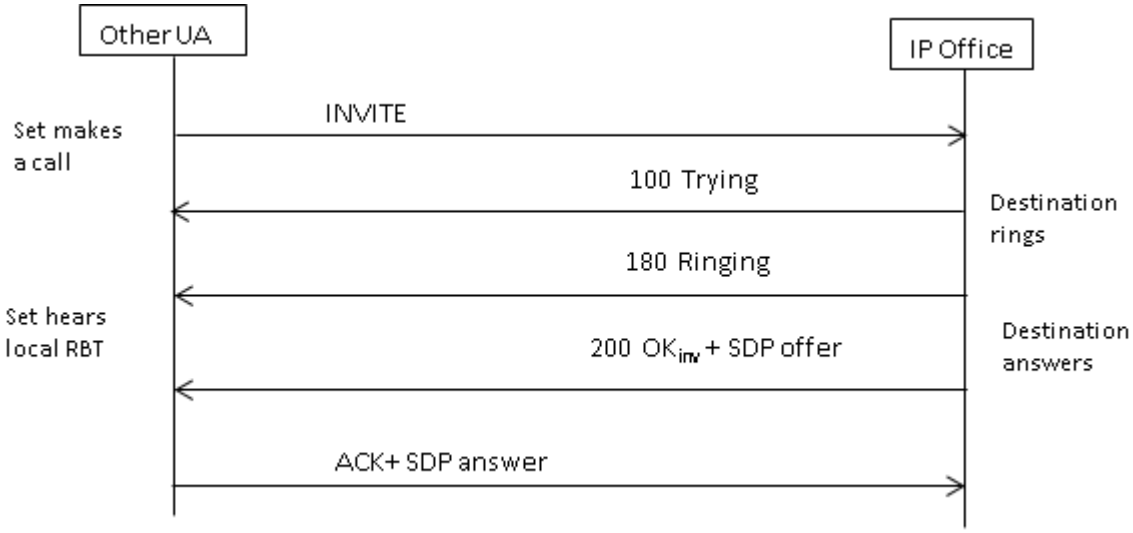
INVITE with SDP, early media

If the SIP Trunk receives a FAR_PROGRESS (in-band) message from its peer in the core (e.g. from a tandem PRI or SIP trunk), it sends a 183 Session Progress message with SDP to the far end. IP Office will connect the media on receipt of 180 or 183 with SDP.



INVITE without SDP, local ring back

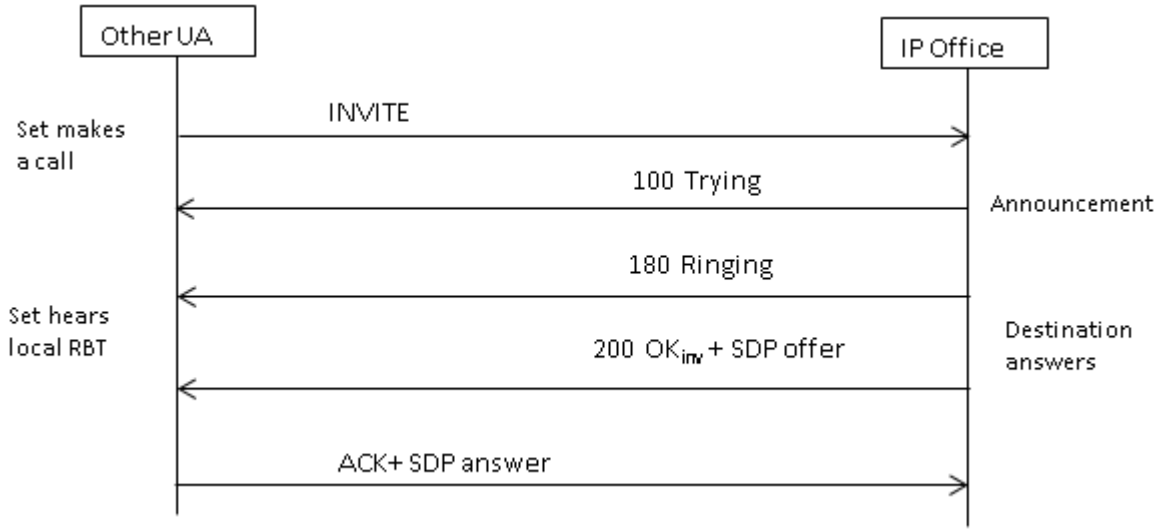
IP Office does not attempt to send early media in this scenario.



INVITE without SDP, early media

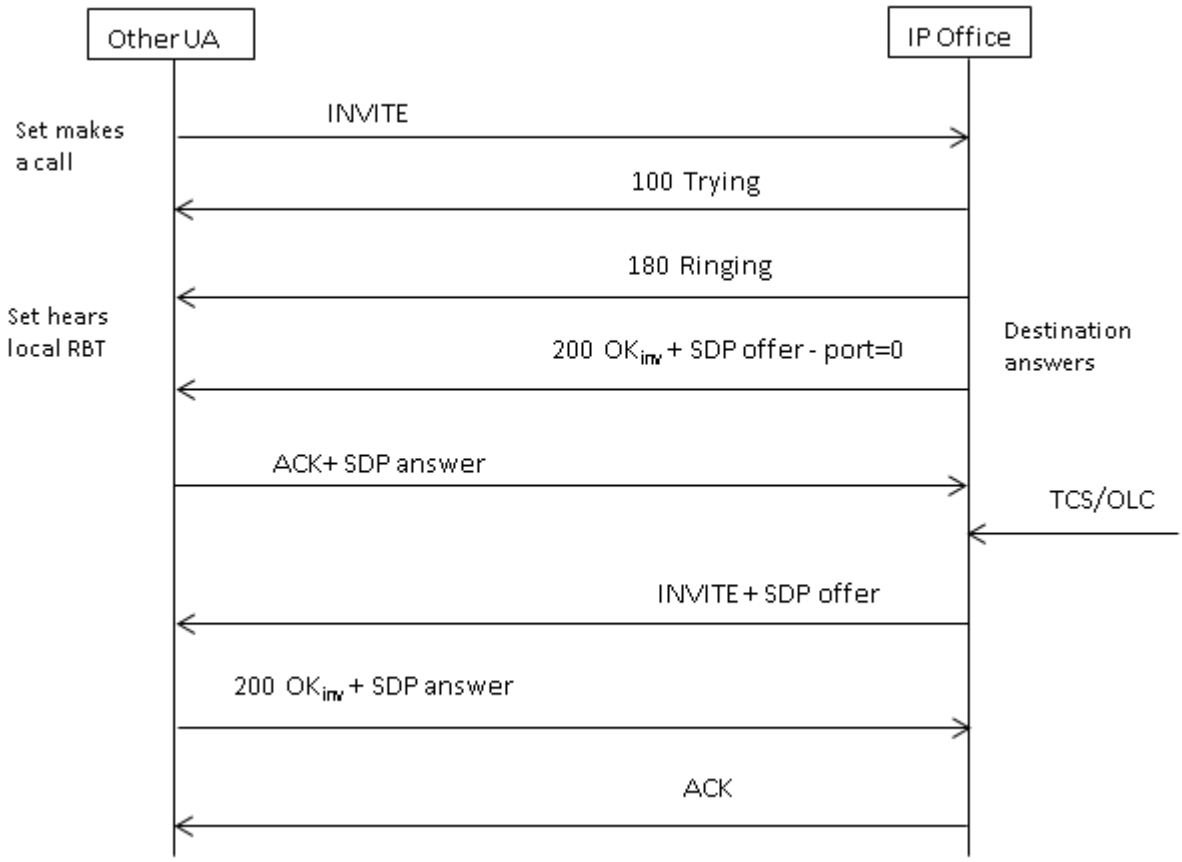
In this scenario, the far end attempts to connect media before the call is answered. IP Office does not provide early media when receiving an empty INVITE, but rather 180 Ringing instead. There is

no requirement to provide an SDP in the 180 Ringing provisional response, as that response is not sent reliably using the PRACK mechanism.



INVITE without SDP, call terminates on H.323 endpoint

If the destination of the call is an H.323 trunk, the destination media address is not known when the call is answered. Therefore, the SDP offer in 200 OK will contain a null port number (and IP address). Once the logical channels are opened on the H.323 side, IP Office sends a re-INVITE using the real media address.



Related links

Incoming call message details on page 679

Codec selection

Codec selection is based on the Offer/Answer model specified in RFC 3264. The endpoint that issues the offer includes the list of codecs that it supports. IP Office offers the codecs set on the **SIP line | VoIP** tab, not those that are set on the extension.

The other endpoint sends an answer that should normally contain a single codec. If there are multiple codecs in the answer, IP Office only considers the first codec. If the SIP Line is configured to do Codec Lockdown (Re-Invite Supported is a prerequisite) then it will send another INVITE with the single chosen codec.

Related links

SIP messaging on page 674

DTMF transmission

DTMF over RTP (RFC 2833) can be used in IP Office. Asymmetric dynamic payload negotiation is supported when it is necessary to bridge multiple SIP endpoints that do not support payload negotiation. The value used for an initial offer is configured on the **System | Codecs** tab. The default value is 101. Upon receipt of an offer with an RFC2833 payload type, IP Office will automatically use the proposed value rather than its own configured value. This helps to support networks that do not negotiate payload types.

There are cases in which direct media is desirable between SIP trunks and endpoints that do not support RFC2833. To allow for this, if key presses are indicated from the extension, the IP Office will ‘shuffle’ the media in. This connects its own media engine to the endpoint and to the SIP trunk, and injects the digits in-band using the negotiated dynamic payload. After fifteen seconds of no key presses, the media will be shuffled back out to re-establish a direct connection again.

Related links

SIP messaging on page 674

Fax over SIP

T.38 Fax over SIP is supported on the IP500 V2 platform deployed as standalone or as an expansion gateway. G.711 fax is also supported, and is supported on Linux servers. For networks that do or do not support T.38, IP Office allows both G3 and Super G3 fax machines to interoperate.

There are configuration parameters that control the behavior in different networks. If T.38 is supported in a network, then it may make sense to select T.38 as the Fax Transport preference in order to make use the inherent quality provided by the redundancy mechanisms. On the other hand, if all of the fax machines in the network are Super G3 capable, there may be a need to take advantage of the increased speed that this encoding provides. Since T.38 is not capable of encoding Super G3, G.711 may be a better choice for the Fax Transport. In either case, IP Office will accept codec change requests from the far SIP endpoint to switch to T.38 or to G.711.

T.38 Fax Transport and Direct Media are mutually exclusive on a given SIP Line. IP Office keeps itself in the media path so that it can detect fax tones to make the switch to T.38.

Related links

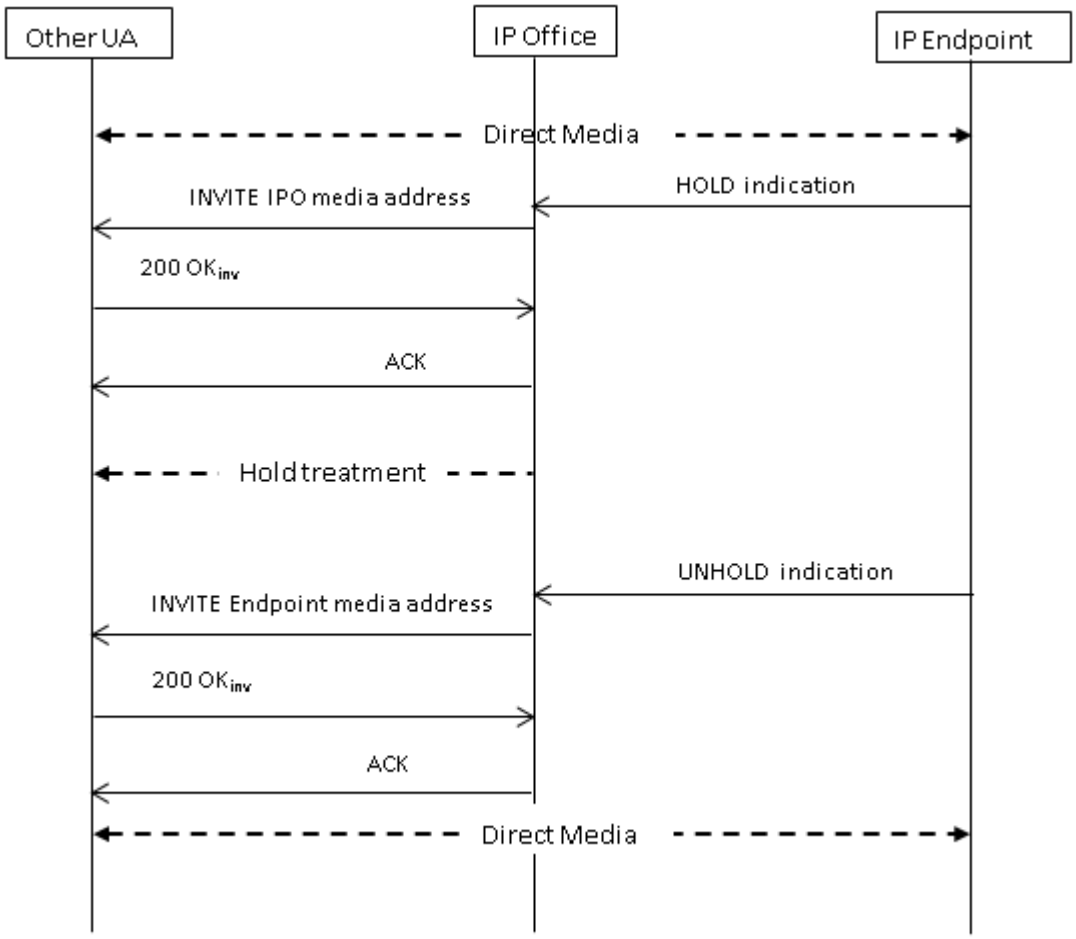
SIP messaging on page 674

Hold scenarios

Hold originated by IP Office

When an IP Office DS extension or non-IP trunk puts a SIP trunk on hold, there is no indication to the network. The voice path is merely switched in the TDM domain to the appropriate hold

treatment source, be it tones, silence or music. For IP extensions and trunks, be they H.323 or SIP, if the call uses direct media, there will be a re-INVITE sent to redirect the media source from the extension or trunk endpoint to a port on the IP Office in order to connect hold treatment. When the call is then unheld, another INVITE will go out to connect the extension with the far end.



Hold originated by far end

The far end of a SIP trunk can put the IP Office on hold by sending it re-INVITE with an SDP Offer containing:

- A **sendonly** attribute. IP Office replies with an SDP Answer containing the **recvonly** attribute.
- An **inactive** attribute. IP Office replies with **inactive**.
- A zero media connection address (c=0.0.0.0). IP Office replies with **inactive**.

Unhold

A held call is unheld by means of an SDP Offer with the **sendrecv** attribute (or no direction attribute, since **sendrecv** is assumed if not specified).

Unhold from mutual hold

Either end can un-hold the other end, i.e., allow it to transmit again, by sending a new Offer with the **sendrecv** or **recvonly**attribute. The other end replies with **sendonly** if the call is still on hold at its end.

Related links

SIP messaging on page 674

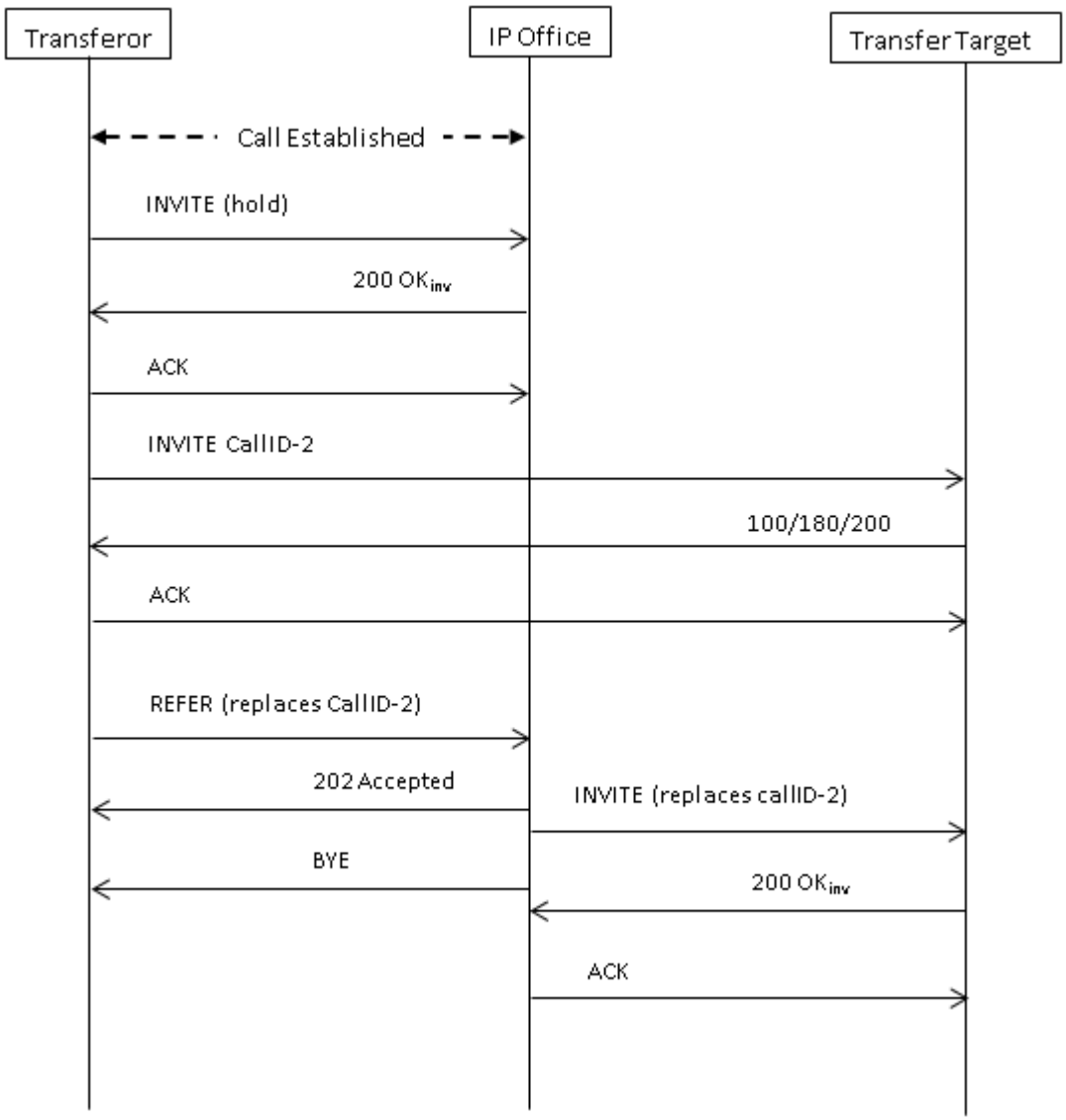
SIP REFER

After a SIP call has been established between two parties (the “Primary” call), the SIP REFER method is used by the **TransferOR** end of the call to transfer the **TransferEE** end to a **Transfer Target**. The REFER message provides the Transfer Target’s contact information in the Refer-To header. This causes the TransferEE to establish the Secondary call to the Transfer Target, thus completing the transfer.

For public SIP trunks, IP Office supports only consultative call transfer using REFER. Consultative transfer is also known as Attended. With consultative transfer, the TransferOR puts the Primary call on hold and establishes a **Consult** call to another party. After the consultation, the TransferOR completes the transfer, causing the TransferEE to connect to the Transfer Target, thereby replacing the Transfer Target’s call with the TransferOR.

REFER can be configured to accept incoming, reject incoming, or decide based on the presence of REFER in the **Allow:** header in responses to OPTIONS messages. Similarly, there is the same configuration for outgoing REFER.

Although the TransferOR and TransferEE must be SIP endpoints, the Transfer Target may be a TDM, PRI, H.323 or SIP terminal on the same IP Office, or an endpoint reachable over the same SIP line as the REFER request is received from.



Related links

SIP messaging on page 674

IP Office SIP trunk specifications

This section outlines the SIP trunk capabilities supported by IP Office.

Related links

Configuring SIP Trunks on page 668
RFCs on page 690
Transport protocols on page 691

RFCs

- ITU-T T.38 Annex D, Procedures for real-time Group 3 facsimile communication over IP networks
- RFC 1889 - RTP: A Transport Protocol for Real-Time Applications
- RFC 2327 - SDP: Session Description Protocol
- RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication
- RFC 2833/RFC 4733 - RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 2976 - The SIP INFO Method
- RFC 3087 - Control of Service Context using SIP Request-URI
- RFC 3261 - Session Initiation Protocol
- RFC 3262 - Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3263 - Session Initiation Protocol (SIP): Locating SIP Servers
- RFC 3264 - An Offer/Answer Model with the Session Description Protocol (SDP)
- RFC 3311 - The Session Initiation Protocol (SIP) UPDATE Method
- RFC 3323 - A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3325 - Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted
- RFC 3326 - The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3398 - Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping
- RFC 3407 - Session Description Protocol (SDP) Simple Capability
- RFC 3489 - STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 3515 – The Session Initiation Protocol (SIP) Refer method
- RFC 3550 - RTP: A Transport Protocol for Real-Time Applications
- RFC 3551 - RTP Profile for Audio and Video Conferences with Minimal Control
- RFC 3665 - Session Initiation Protocol Basic Call Flow Examples
- RFC 3666 - Session Initiation Protocol PSTN Call Flows
- RFC 3725 - Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)
- RFC 3824 - Using E.164 numbers with the Session Initiation Protocol (SIP)
- RFC 3842 - A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol
- RFC 3891 - The Session Initiation Protocol (SIP) "Replaces" Header
- RFC 3960 - Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
- RFC 4028 - Session Timers in the Session Initiation Protocol (SIP)
- RFC 4566 - SDP: Session Description Protocol
- RFC 5359 - Session Initiation Protocol Service Examples
- RFC 5379 - Guidelines for Using the Privacy Mechanism for SIP
- RFC 5806 - Diversion Indication in SIP
- RFC 5876 - Updates to Asserted Identity in the Session Initiation Protocol (SIP)
- RFC 6337 - Session Initiation Protocol (SIP) Usage of the Offer/Answer Model
- RFC 6432 - Carrying Q.850 Codes in Reason Header Fields in SIP (Session Initiation Protocol) Responses

Related links

IP Office SIP trunk specifications on page 688

Transport protocols

- UDP
- TCP
- RTP
- RTCP

Related links

IP Office SIP trunk specifications on page 688

Request methods

- INVITE
- ACK
- BYE
- CANCEL
- INFO
- REFER
- REGISTER
- SUBSCRIBE
- NOTIFY
- PRACK
- OPTIONS
- UPDATE
- PUBLISH
- MESSAGE
- PING

Related links

IP Office SIP trunk specifications on page 688

Response methods

- 100 Trying
- 180 Ringing
- 181 Call Is Being Forwarded
- 182 Call Queued
- 183 Session progress
- 200 OK
- 202 ACCEPTED
- 3XX
- 4XX
- 5XX
- 6XX

Related links

IP Office SIP trunk specifications on page 688

Headers

- Accept
- Alert-Info
- Allow
- Allow-Event
- Authorization
- Call-ID
- Contact
- Content-Length
- Content-Type
- CSeq
- Diversion
- From
- History-Info
- Max-Forwards
- P-Asserted-Identity
- P-Early-Media
- P-Preferred-Identity
- Privacy
- Proxy-Authenticate
- Proxy-Authorization
- Proxy-Require
- Require
- Remote-Party-ID
- Server
- Session-Timers
- Supported
- To
- User-Agent
- Via
- WWW-Authenticate

Related links

IP Office SIP trunk specifications on page 688

Chapter 14: Short Code Overview

The system uses short codes to match the number dialed to an action. The number dialed or part of the number dialed can be used as parameter for the feature. This section provides an overview of short codes and information on configuration.

Warning:

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

The short method for describing short codes in this manual, for example **9N/Dial/./0**, indicates the settings of the following fields of a short code: **Code/Feature/Telephone Number/Line Group ID**. For a description of the individual fields see Short Code.

Examples The method of detailing a short codes settings lists the short code fields separated by a /.

***17/VoicemailCollect/?U** A user dialing ***17** is connected to voicemail.

***14*N#/FollowMeTo/N** If a user dials ***14*210#** at their own extension, their calls are redirected to extension 210.

Dialing Short Codes The following types of short code applied to on-switch dialing. The result may be an action to be performed by the system, a change to the user's settings or a number to be dialed. The order below is the order of priority in which they are used when applied to user dialing.

User Short Codes These are usable by the specific user only. User short codes are applied to numbers dialled by that user and to calls forwarded via the user.

User Rights Short Codes These are usable by any users associated with the user rights in which they are set. User Rights short codes are only applied to numbers dialed by that user. For example they are not applied to calls forwarded via the user.

System Short Codes These are available to all users on the system. They can be overridden by user or user rights short codes.

Post-Dialing Short Codes When any the short code above result in a number to be dialed, further short code can be applied to that number to be dialed. This is done using the following types of short codes.

ARS (Alternate Route Selection) Short Codes The short code that matches dialing can specify that the resulting number should be passed to an ARS form. The ARS form can specify which routes should be used for the call by using further short code matches and also provide option to use other ARS forms based on other factors such as time and availability of routes.

Transit Network Selection (TNS) Short Codes Used on T1 ISDN trunks set to use AT&T as the Provider. Applied to the digits presented following any other short code processing.

Incoming Number Short Codes On certain types of trunks short codes can be applied to the incoming digits received with calls.

Line Short Codes These short codes are used to translate incoming digits received with calls. The stage at which they are applied varies between different line types and may be overridden by an extension number match.

Related links

Short Code Characters on page 694
User Dialing on page 698
Application Dialing on page 699
Secondary Dial Tone on page 700
? Short Codes on page 701
Short Code Matching Examples on page 702
Default System Short Code List on page 707

Short Code Characters

Each short code, regardless of its type, has the following fields:

- **Short Code**: Default =Blank. Range = Up to 31 characters. The digits which if matched trigger use of the short code. Characters can also be used to create short codes which cannot be dialed from a phone but can be dialed from application speed dials. However some characters have special meaning, see the table below.
- **Telephone Number**: Default = Blank. Range = Up to 32 characters. The number output by the short code. When necessary, this is used as parameter for the selected short code Feature. See the table below for the special characters that can be used here.
- **Line Group ID**: Default = 0 This field is used for short codes that result in a number to be dialed.It acts as a drop-down from which either an outgoing line group or an ARS form can be selected.
- **Feature**: Default = Dial This sets the action performed by the short code when used. See Short Code Features.
- **Locale**: Default = Blank Features that transfer the caller to voicemail can indicate the language locale required for prompts. This is subject to the language being supported and installed on the voicemail server.

When the system routes a call to the voicemail server it indicates the locale for which matching prompts should be provided if available. The locale sent to the voicemail server by the system is determined as show below. If the required set of prompts is not available, the voicemail will

fallback to another appropriate language and finally to English (refer to the appropriate voicemail installation manual for details).

- **Short Code Locale**: The short code locale, if set, is used if the call is routed to voicemail using the short code.
- **Incoming Call Route Locale**: The incoming call route locale, if set, is used if caller is external.
- **User Locale**: The user locale, if set, is used if the caller is internal.
- **System Locale**: If no user or incoming call route locale is set, the system locale is used unless overridden by a short code locale.

Systems using Embedded Voicemail, if the required set of upgraded language prompts to match the locale is not present on the system SD card, Manager will display an error. The required prompt set can be uploaded from Manager using the Add/Display VM Locales option.

Force Account Code: Default = Off When selected, for short codes that result in the dialing of a number, the user is prompted to enter a valid account code before the call is allowed to continue.

Short Code Field Characters

? - Default Match This character can be used on its own to create a short code match in the absence of any other short code match. See ? Short Codes.

?D - Default Number Dialing This character combination makes a call to the defined phone number as soon as the user goes off-hook. See ? Short Codes.

?D(x) - Default Number Dialing The character x represents time in seconds. If a phone is off-hook or speaker is enabled and no number is dialed for x seconds, the phone makes a call to the defined phone number. A maximum of 30 seconds is used for x though system accepts values more than 30 on the interface.

N - Match Any Digits Matches any dialed digits (including none). The Dial Delay Time or a following matching character is used to resolve when dialing is complete.

X - Match a Digit Matches a single digit. When a group of X's is used, the short code matches against the total number of X's.

[ ] - Secondary Dial Tone Trigger For pre-4.0 IP Office systems used to trigger secondary dial tone. Not used for Release 4.0+. See Secondary Dial Tone.

; - Receive Sending Complete When used this must be the last character in the short code string. If the **Dial Delay Count** is **0**, a **;** instructs the system to wait for the number to be fully dialed, using the **Dial Delay Time** or the user dialing **#**, to indicate completion and then acting on the short code. If the **Dial Delay Count** is not zero, the dialing is only evaluated when **#** is pressed.

The majority of North-American telephony services use en-bloc dialing. Therefore the use of a ; is recommended at the end of all dialing short codes that use an N before routing those calls to a trunk or ARS. This is also recommended for all dialing where secondary dial tone short codes are being used.

Telephone Number Field Characters

A - Allow Outgoing CLI Allow the calling party number sent with the call to be used. This character may be required by service providers in some locales.

C - Use Called Number Field Place any following digits in the outgoing call's Called number field rather than the Keypad field.

D - Wait for Connect Wait for a connect message before sending any following digits as DTMF.

E - Extension Number Replace with the extension number of the dialing user. Note that if a call is forwarded this will be replaced with the extension number of the forwarding user.

h - Hold Music Source When used as part of the short code telephone number field, this character allows the source for music on hold to be selected. Enter `h(X)` where **X** indicates the required hold music source if available. For IP500 V2 systems, the value of **X** can be 1 to 4. For systems on a Linux based server, the value of **X** can be 1 to 32. This overrides any previous hold music selection that may have been applied to the call. When used with ParkCall shortcodes, the **h(X)** should be entered before the park slot number part of the telephone number.

I - Use Information Packet Send data in an Information Packet rather than Set-up Packet.

K - Use Keypad Field Place any following digits in the outgoing call's Keypad field rather than the Called Number field. Only supported on ISDN and QSIG.

l - Last Number Dialed (lower case L) Use the last number dialed.

L - Last Number Received Use the last number received.

N - Dialed Digit Wildcard Match Substitute with the digits used for the **N** or **X** character match in the Short Code number field.

p - Priority The priority of a call is normally assigned by the Incoming Call Route or else is **1-Low** for all other calls. Dial Extn short codes can use **p(x)** as a suffix to the **Telephone Number** to change the priority of a call. Allowable values for **x** are **1**, **2** or **3** for low, medium or high priority respectively.

In situations where calls are queued, high priority calls are placed before calls of a lower priority. This has a number of effects:

- Mixing calls of different priority is not recommended for destinations where Voicemail Pro is being used to provided queue ETA and queue position messages to callers since those values will no longer be accurate when a higher priority call is placed into the queue. Note also that Voicemail Pro will not allow a value already announced to an existing caller to increase.
- If the addition of a higher priority call causes the queue length to exceed the hunt group's Queue Length Limit, the limit is temporarily raised by 1. This means that calls already queued are not rerouted by the addition of a higher priority call into the queue.

r - Ring Tone Plan When used as part of the short code telephone number field, this character can specify a Ring Tone Plan number. Enter `r(X)` where **X** is 1 to 8 indicating the Ring Tone Plan number to use.

S - Calling Number Place any following digits into the outgoing call's calling number field. Using S does not alter any allow or withhold CLI setting associated with the call, the short code characters **A** or **W** should be used respectively. Note that for SIP trunks, the SIP URI configuration options override this setting.

Outgoing CLI Warning Changing the outgoing CLI for calls requires the line provider to support that function. You must consult with your line provider before attempting to change the outgoing CLI, failure to do so may result in loss of service. If changing the outgoing CLI is allowed, most line providers required that the outgoing CLI used matches a number valid for return calls on the same

trunks. Use of any other number may cause calls to be dropped or the outgoing CLI to be replaced with a valid number.

On mobile twinned calls, if the original party information is used or a specific calling party information CLI is set, that number overrides setting the outgoing CLI using short codes.

SS - Pass Through Calling Number Pass through the Calling Party Number. For example, to provide the incoming ICLID at the far end of a VoIP connection, a short code **?** with telephone number **.SS** should be added to the IP line.

i - National Both the **S** and **SS** characters can be followed by an **i**, that is **Si** and **SSi**. Doing this sets the calling party number plan to ISDN and number type to National. This may be required for some network providers.

t - Allowed Call Duration Set the maximum duration in minutes for a call plus or minus a minute. Follow the character with the number of minutes in brackets, for example **t(5)**.

U - User Name Replace with the User Name of the dialing user. Used with voicemail.

W - Withhold Outgoing CLI Withhold the sending of calling ID number. Operation is service provider dependent.

Y - Wait for Call Progress Message Wait for a Call Progress or Call Proceeding message before sending any following digits as DTMF. For example, the Y character would be necessary at a site where they have signed up with their telephone service provider to withhold international dialing until a DTMF pin/account number is entered that initiates the call progress/proceeding message.

Z - Calling Party Name This option can be used with trunks that support the sending of name information. The **Z** character should be followed by the name enclosed in **" "** quotation marks. Note that their may be name length restrictions that vary between line providers. The changing of name information on calls being forwarded or twinned may also not be supported by the line provider.

@ - Use Sub Address Field Enter any following digits into the sub-address field.

. - Dialed Digits Replace with the full set of dialed digits that triggered the short code match.

, - One Second Pause Add a one second pause in DTMF dialing.

; - Receive Sending Complete When used this must be the last character in the short code string. If the **Dial Delay Count** is **0**, a **;** instructs the system to wait for the number to be fully dialed, using the **Dial Delay Time** or the user dialing **#**, to indicate completion and then acting on the short code. If the **Dial Delay Count** is not zero, the dialing is only evaluated when **#** is pressed.

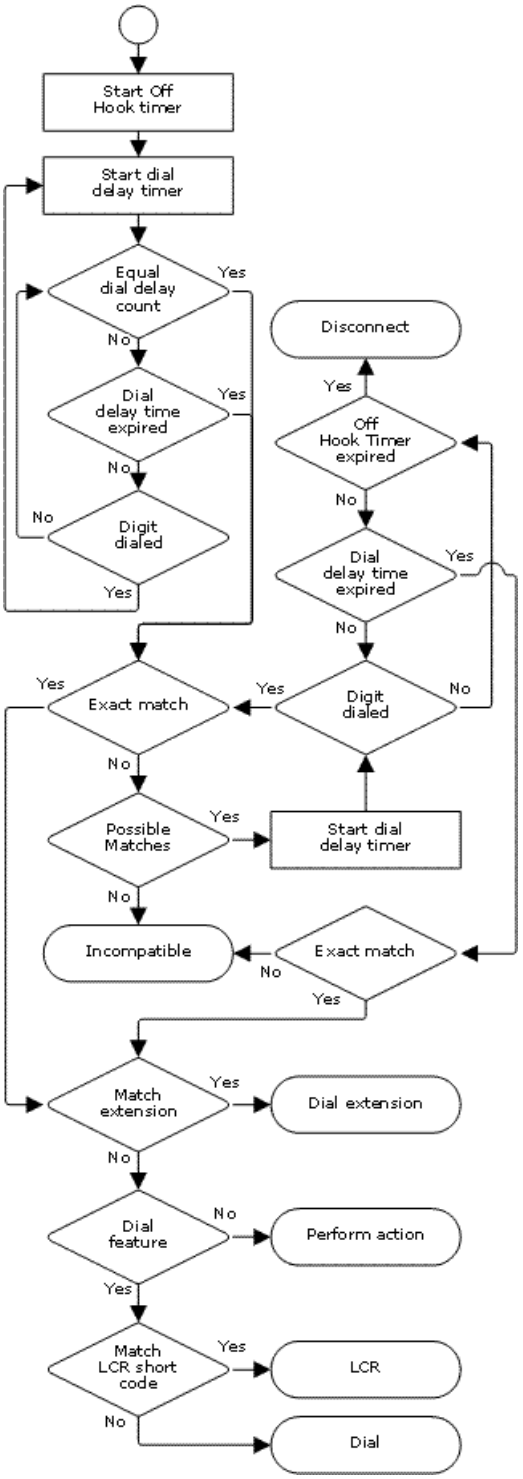
" " - Non Short Code Characters Use to enclose any characters that should not be interpreted as possible short code special characters by the system. For example characters being passed to the voicemail server.

Related links

Short Code Overview on page 693

User Dialing

Summary: Looks at how the system looks for possible short code matches to user dialing.



The following system settings influence user dialing.

Dial Delay Count: Default = 0 (US/Japan), 4 (ROW) This value sets the number of digits dialed before the system looks for a short code match.

Dial Delay Time: Default = 4 seconds (US/Japan), 1 second (ROW) This value sets the maximum allowed interval between the dialing of each digit. If exceeded, the system looks for a short code match even if the Dial Delay Count has not been reached.

Off-Hook Timer: Length Fixed by locale. When a user goes off-hook, the system starts a 30 second off-hook timer (10 seconds in Italy). If the off-hook timer expires before a short code match occurs, the user is disconnected.

The following rules are used when short code matching is performed for user dialing:

- A short code is used immediately an exact match is found unless followed by a ;.
- If no match is found but partial matches exist, the user can continue dialing.
- If no match or partial matches are found, incompatible is returned.
- The following precedence is used to determine which short codes are used:
- Extension number matches override all short codes.
- User short codes override user rights and system short codes.
- User Rights short code matches override system short codes.
- When multiple exact matches occur,
- The match with the most specified digits rather than wildcards is used.
- If there are still more than one match, the match with the most exact length is used. This means X wildcards will override N when both match.

Related links

Short Code Overview on page 693

Application Dialing

Numbers speed dialed by system applications such as SoftConsole are treated differently. Since the digits are received en bloc as a single group, they can override some short code matches. The same applies to short codes used within system configuration settings such as Incoming Call Route destinations.

Example:

- Telephone Number: 12345678
- Short Code 1: 1234XX/Dial/Extn/207
- Short Code 2: 12345678/Dial Extn/210

If dialed manually by the user, as soon as they have dialed 123456 a match to short code 1 occurs. They can never dial short code 2.

If dialed using an application, 12345678 is sent as a string and a match to short code 2 occurs.

Partial Dialing

If the application dialing does not trigger an exact match, the user can dial additional digits through their extension. The processes for normal user dialing are applied.

Non-Digit Short Codes

Short codes can be created that use alphabetic characters instead of numbers. While these short codes cannot be dialed from a phone, they can be dialed using application speed dials and settings. However characters that are interpreted as special short code characters will still be interpreted as such.

Related links

Short Code Overview on page 693

Secondary Dial Tone

Some locales prefer to provide users with secondary dial tone once they have started dialing external calls. This dial tone is heard by the user until they have completed dialing and a trunk is seized at which point call progress tones are provided by the trunk, or camp on/busy tone is provided by the system if the required trunk cannot be seized.

Release 4.0 and Higher

The use of secondary dial tone is provided through the **Secondary Dial Tone** check box option on the ARS form to which the call is routed. When on, this setting instructs the system to play secondary dial tone to the user.

The tone used is set as either **System Tone** (normal dial tone) or **Network Tone** (secondary dial tone). Both tone types are generated by the system in accordance with the system specific locale setting. Note that in some locales normal dial tone and secondary dial tone are the same.

When **Secondary Dial Tone** is selected, the ARS form will return tone until it receives digits with which it can begin short code matching. Those digits can be the result of user dialing or digits passed by the short code which invoked the ARS form. For example with the following system short codes:

In this example, the 9 is stripped from the dialed number and is not part of the telephone number passed to the ARS form. So in this case secondary dial tone is given until the user dials another digit or dialing times out.

- **Code**: 9N
- **Telephone Number**: N
- **Line Group ID**: 50 Main

In this example, the dialed 9 is included in the telephone number passed to the ARS form. This will inhibit the use of secondary dial tone even if secondary dial tone is selected on the ARS form.

- **Code**: 9N
- **Telephone Number**: 9N
- **Line Group ID**: 50 Main

Pre-4.0 IP Office Secondary Dial Tone

Pre-4.0 systems provided dial tone through the use of the short code feature Secondary Dial Tone and the [ ] special characters. For example, on a system where 9 is used as a prefix for external dialing, the system short code 9/./Secondary Dial Tone/0 will trigger secondary dial tone when users dial a number prefixed with 9. This method is not supported by Release 4.0 which provides ARS forms for the control of outgoing calls.

In order to allow further digit matching, the digits dialed are put back through short code matching against any short codes that start with [n] where n is the digit used to trigger the system secondary dial tone short code.

On all systems where secondary dial tone is used, a ; should also be used in dialing short codes that contain N.

For example:

System Short Codes

- 9/SecondaryDialTone/.
- [9]0N;/Dial/0

User Short Code

[9]0N;/Busy/0

The user dials 90114445551234. The 9 is matches the system secondary dial tone short code and unlike other short codes this is applied immediately. The user's dialing is put through short code matching again using the normal order of precedence but matched to possible short codes beginning [9]. In this case the user's [9]0N; short code would take precedence over the system [9]0N; short code.

Related links

Short Code Overview on page 693

? Short Codes

The ? character can be used in short codes in the following ways:

Default Short Code Matching:

? short codes are used in short code matching in the following way. If no user or system short code match is found, the system will then look for a ? short code match. It will look first for a user ? short code and then, if not found, a system ? short code.

Example: On systems outside North America, the system short code **?/Dial/./0** is added as a default short code. This short code provides a match for any dialing to which there is no other match. Therefore, on systems with this short code, the default is that any unrecognized number will be dialed to Outgoing Line Group 0.

Hot-Line Dialing:

A user short code **?D** can be used to perform a short code action immediately the user extension goes off-hook. This is supported with Dial type short code features. Typically it is used with door, lift and lobby phones to immediately connect the phone to a number such as the operator or reception.

Voicemail Collect Short Codes:

The ? character can appear in the **Telephone Number** field of a short code. This is done with short codes using the VoicemailCollect feature. In this instance the ? character is not interpreted by the system, it is used by the voicemail server.

Related links

Short Code Overview on page 693

Short Code Matching Examples

The following examples are not meant as practical examples. However they are simple to implement and test on real system without conflicting with its normal operation. They illustrate the interaction between different short codes in resolving which short code is an exact match. They assume that extension numbers are in the 200 to 299 range.

The term 'dials' means dialing the indicated digit or digits without the inter-digit Dial Delay Time expiring.

The term 'pause' means a wait that exceeds the inter-digit Dial Delay Time.

Scenario 1		
Short Code 1 = 60/Dial Extn/203 Dial Delay Count = 0. Dial Delay Time = 4 seconds.		
Test	Dialing	Effect
1	8	No possible match, incompatible returned immediately
2	6	No exact match but there is a potential match, so the system waits. When the Dial Delay Time expires, no exact match is found so incompatible is returned.

Table continues…

3	60	Exact match to Short Code 1. Extension 203 called immediately.
4	61	No possible match, the system returns incompatible.

Scenario 2		
Short Code 1 = 60/Dial Extn/203 Short Code 2 = 601/Dial Extn/210 Dial Delay Count = 0. Dial Delay Time = 4 seconds.		
Test	Dialing	Effect
1	8	No possible match, incompatible returned immediately
2	60	Exact match to Short Code 1. Extension 203 called immediately.
3	601	Exact match to Short Code 1 as soon as the 0 is dialed. The user cannot manually dial 601.

Scenario 3		
Short Code 1 = 60/Dial Extn/203 Short Code 2 = 601/Dial Extn/210 Dial Delay Count = 3. Dial Delay Time = 4 seconds.		
Test	Dialing	Effect
1	8	Insufficient digits to trigger matching. The system waits for additional digits or for Dial Delay Time to expire. When Dial Delay Time expires, no possible match is found so incompatible is returned.
2	60	Insufficient digits to trigger matching. The system waits for additional digits or for Dial Delay Time to expire. When Dial Delay Time expires, matching started and exact match to Short Code 1 occurs. .
3	601	Third digit triggers matching. Exact match to Short Code 2. Extension 210 dialed immediately.
4	60#	# is treated as a digit and as the third digit triggers matching. No exact match found. The system returns incompatible.

Scenario 4		
Short Code 1 = 60;/Dial Extn/203 Short Code 2 = 601/Dial Extn/210 Dial Delay Count = 3. Dial Delay Time = 4 seconds.		
Test	Dialing	Effect
1	8	Insufficient digits to trigger matching. The system waits for additional digits or for Dial Delay Time to expire. When Dial Delay Time expires, no possible match is found so incompatible is returned.
2	6	Insufficient digits to trigger matching. The system waits for additional digits or for the interdigit Dial Delay Time to expire. If the Dial Delay Time expires, a potential match exists to a short code that uses ; so the system waits for an additional digit until the off-hook timer expires.
3	60	As above but an additional digit now may create a match. If 1 is dialed, it creates an exact match to Short Code 2 and is used immediately. If 0, * or 2 to 9 is dialed, no possible match exists. The system returns incompatible. If the next digit is a #, it is treated as signaling dialing complete rather than being a digit. Short code 1 becomes an exact match and is used immediately.
4	601	Third digit triggers matching. Exact match to Short Code 2. Extension 210 dialed immediately.

Scenario 5
Short Code 1 = 601/Dial Extn/203 Short Code 2 = 60N/Dial Extn/210 Dial Delay Count = 0. Dial Delay Time = 4 seconds.

Table continues…

Test	Dialing	Effect
1	6	No exact match but there is a potential match, so the system waits for additional dialing. If the Dial Delay Time expires, no exact match is found so incompatible is returned.
2	60	Potential match to both short codes. The system waits for additional dialing. If the Dial Delay Time expires, Short Code 2 becomes an exact match with N blank.
3	601	Exact match to Short Code 1. Used immediately
4	602	Exact match to Short Code 2. Used immediately.

Scenario 6		
Short Code 1 = 601/Dial Extn/203 Short Code 2 = 60N/Dial Extn/210 Short Code 3 = 60X/Dial Extn/207 Dial Delay Count = 0. Dial Delay Time = 4 seconds.		
Test	Dialing	Effect
1	6	No exact match but there are potential matches so the system waits for additional dialing. If the Dial Delay Time expires, no exact match has occurred so incompatible is returned.
2	60	Potential match to all short codes. System waits for additional dialing. If the Dial Delay Time expires, Short Code 2 becomes an exact match with N blank. If a digit is dialed, Short Code 3 becomes a more exact match and is used.
3	601	Exact match all short code, however Short Code 1 is treated as being more exact (more matching digits) and is used immediately

Table continues…

4	602	Exact match to short codes 2 and 3, however the Short Code 3 is treated as being more exact (length match) and is used immediately.

Scenario 7		
Short Code 1 = 601/Dial Extn/203 Short Code 2 = 60N/Dial Extn/210 Short Code 3 = 6XX/Dial Extn/207 Dial Delay Count = 0. Dial Delay Time = 4 seconds.		
Test	Dialing	Effect
1	6	No exact match but there are potential matches so the system waits for additional dialing. If the Dial Delay Time expires, no exact match has occurred so incompatible is returned.
2	60	Potential match to all short codes. System waits for additional dialing. If the Dial Delay Time expires, Short Code 2 becomes an exact match with N blank. If a digit is dialed, Short Code 3 becomes an more exact match and is used.
3	601	Exact match all short code, however Short Code 1 is treated as being more exact (more matching digits) and is used immediately
4	602	Exact match to short codes 2 and 3, however the Short Code 2 is treated as being more exact (more matching digits) and is used immediately.
5	612	Exact match to Short Code 3.

Related links

Short Code Overview on page 693

Default System Short Code List

Most control units are available in A-Law and U-Law models. Typically U-Law models are supplied to North American locales, A-Law models are supplied to the rest of the world. In addition to the using different default companding for digital lines and phone, A-Law and U-Law models support different default short codes. The following table lists the default system short codes present in a system's configuration.

Standard Mode

Short Code	Telephone Number	Feature	A-Law	ULAW
***00**	Blank	Cancel All Forwarding	✓	✓
***01**	Blank	Forward Unconditional On	✓	✓
***02**	Blank	Forward Unconditional Off	✓	✓
***03**	Blank	Forward On Busy On	✓	✓
***04**	Blank	Forward On Busy Off	✓	✓
***05**	Blank	Forward On No Answer On	✓	✓
***06**	Blank	Forward On No Answer Off	✓	✓
***07*N#**	N	Forward Number	✓	✓
***08**	Blank	Do Not Disturb On	✓	✓
***09**	Blank	Do Not Disturb Off	✓	✓
***10*N#**	N	Do Not Disturb Exception Add	✓	✓
***11*N#**	N	Do Not Disturb Exception Del	✓	✓
***12*N#**	N	Follow Me Here	✓	✓
***13*N#**	N	Follow Me Here Cancel	✓	✓
***14*N#**	N	Follow Me To	✓	✓
***15**	Blank	Call Waiting On	✓	✓
***16**	Blank	Call Waiting Off	✓	✓
***17**	?U	Voicemail Collect	✓	✓
***18**	Blank	Voicemail On	✓	✓
***19**	Blank	Voicemail Off	✓	✓

Table continues…

Short Code	Telephone Number	Feature	A-Law	ULAW
***20*N#**	N	Set Hunt Group Night Service	✓	✓
***21*N#**	N	Clear Hunt Group Night Service	✓	✓
***22*N#**	N	Suspend Call	✓	✗
***23*N#**	N	Resume Call	✓	✗
***24*N#**	N	Hold Call	✓	✗
***25*N#**	N	Retrieve Call	✓	✗
***26**		Clear CW	✓	✗
***27*N#**	N	Hold CW	✓	✗
***28*N#**	N	Suspend CW	✓	✗
***29**	Blank	Toggle Calls	✓	✓
***30**	Blank	Call Pickup Any	✓	✓
***31**	Blank	Call Pickup Group	✓	✓
***32*N#**	N	Call Pickup Extn	✓	✓
***33*N#**	N	Call Queue	✓	✓
***34N;**	N	Hold Music	✓	✓
***35*N#**	N	Extn Login	✓	✓
***36**	Blank	Extn Logout	✓	✓
***37*N#**	N	Call Park	✓	✓
***38*N#**	N	Unpark Call	✓	✓
***39**	1	Relay On	✓	✓
***40**	1	Relay Off	✓	✓
***41**	1	Relay Pulse	✓	✓
***42**	2	Relay On	✓	✓
***43**	2	Relay Off	✓	✓
***44**	2	Relay Pulse	✓	✓
***45*N#**	N	Acquire Call	✓	✓
***46**	Blank	Acquire Call	✓	✓
***47**	Blank	Conference Add	✓	✓
***48**	Blank	Voicemail Ringback On	✓	✓
***49**	Blank	Voicemail Ringback Off	✓	✓
***50**	Blank	Forward Huntgroup On	✓	✓

Table continues…

Short Code	Telephone Number	Feature	A-Law	ULAW
***51**	Blank	Forward Huntgroup Off	✓	✓
***52**	Blank	Cancel or Deny	✓	✓
***53*N#**	N	Call Pickup Members	✓	✓
***55**	Blank	Stamp Log	✓	✓
***57*N#**	N	Forward On Busy Number	✓	✓
***70**	Blank	Call Waiting Suspend	✓	✗
***70*N#**	N	Dial Physical Extn by Number	✗	✓
***71*N#**	N	Dial Physical Extn by Id	✗	✓
9000	"MAINTENANCE"	Relay On	✓	✓
***91N;**	N".1"	Record Message	✓	✓
***92N;**	N".2"	Record Message	✓	✓
***99;**	"edit_messages"	Voicemail Collect	✓	✓
9N	N	Dial	✗	✓
?	.	Dial	✓	✗

Server Edition

Short Code	Telephone Number	Feature	A-Law	ULAW
***00**	Blank	Cancel All Forwarding	✓	✓
***01**	Blank	Forward Unconditional On	✓	✓
***02**	Blank	Forward Unconditional Off	✓	✓
***03**	Blank	Forward On Busy On	✓	✓
***04**	Blank	Forward On Busy Off	✓	✓
***05**	Blank	Forward On No Answer On	✓	✓
***06**	Blank	Forward On No Answer Off	✓	✓
***07*N#**	N	Forward Number	✓	✓

Table continues…

Short Code	Telephone Number	Feature	A-Law	ULAW
***08**	Blank	Do Not Disturb On	✓	✓
***09**	Blank	Do Not Disturb Off	✓	✓
***10*N#**	N	Do Not Disturb Exception Add	✓	✓
***11*N#**	N	Do Not Disturb Exception Del	✓	✓
***12*N#**	N	Follow Me Here	✓	✓
***13*N#**	N	Follow Me Here Cancel	✓	✓
***14*N#**	N	Follow Me To	✓	✓
***17**	?U	Voicemail Collect	✓	✓
***18**	Blank	Voicemail On	✓	✓
***19**	Blank	Voicemail Off	✓	✓
***20*N#**	N	Set Hunt Group Night Service	✓	✓
***21*N#**	N	Clear Hunt Group Night Service	✓	✓
***29**	Blank	Toggle Calls	✓	✓
***30**	Blank	Call Pickup Any	✓	✓
***31**	Blank	Call Pickup Group	✓	✓
***32*N#**	N	Call Pickup Extn	✓	✓
***33*N#**	N	Call Queue	✓	✓
***34N;**	N	Hold Music	✓	✓
***35*N#**	N	Extn Login	✓	✓
***36**	Blank	Extn Logout	✓	✓
***37*N#**	N	Call Park	✓	✓
***38*N#**	N	Unpark Call	✓	✓
***44**	2	Relay Pulse	✓	✓
***45*N#**	N	Acquire Call	✓	✓
***46**	Blank	Acquire Call	✓	✓
***47**	Blank	Conference Add	✓	✓
***48**	Blank	Voicemail Ringback On	✓	✓
***49**	Blank	Voicemail Ringback Off	✓	✓
***50**	Blank	Forward Huntgroup On	✓	✓

Table continues…

Short Code	Telephone Number	Feature	A-Law	ULAW
***51**	Blank	Forward Huntgroup Off	✓	✓
***52**	Blank	Cancel or Deny	✓	✓
***53*N#**	N	Call Pickup Members	✓	✓
***55**	Blank	Stamp Log	✓	✓
***57*N#**	N	Forward On Busy Number	✓	✓
***66*N#**	N	Conference Meet Me	✓	✓
***70**	Blank	Call Waiting Suspend	✓	✗
***70*N#**	N	Dial Physical Extn by Number	✗	✓
***71*N#**	N	Dial Physical Extn by Id	✗	✓
***99;**	"edit_messages"	Voicemail Collect	✓	✓
9N	N	Dial	✗	✓ [1]
?	.	Dial	✓	✓ [1]

For U-Law systems, a **9N** is a default short code on the Primary Server while a **?** short code is a default on all other servers.

Additional short codes of the form *DSSN, *SDN, *SKN, these are used by the system for internal functions and should not be removed or altered. Short codes *#N and **N may also visible, these are used for ISDN functions in Scandinavian locales.

The default ***34** short code for music on hold has changed to ***34N;**.

Related links

Short Code Overview on page 693

Chapter 15: Short Code Features

Note that this document describes all existing short codes. The short codes available in the Manager application depends on the software release.

Auto Attendant

This feature is used with Embedded Voicemail. It is not supported by Server Edition. It allows the recording of the greetings used by auto-attendant services and the transfer of calls to that auto attendant. This feature was previously called **Record Greeting**.

Details

Telephone Number: ✓

Four system short codes (***81XX**, ***82XX**, ***83XX** and ***84XX**) are automatically added for use with all auto attendants, for the morning, afternoon, evening and menu options greetings respectively. These use a telephone number of the form **"AA:" N"** . **Y "** where **N** is the replaced with the auto attendant number dialed and **Y** is 1, 2, 3 or 4 for the morning, afternoon, evening or menu option greeting.

- An additional short code of the form (for example) ***80XX/Auto Attendant/"AA:"N** can be added manual if internal dialed access to auto attendants is required.
- To add a short code to access a specific auto attendant, the name method should be used.
- For IP Office deployed in a Enterprise Branch environment, the short codes *800XX, *801XX…*809XX, *850XX, and *851XX are automatically created for recording a Page prompt.

Default Short Code: ✓ See Configuration Settings | Auto Attendant.

Programmable Button Control: ✗

Release: 2.0+.

Auto Intercom Deny Off

Details

Telephone number: ✗

Default short code: ✗

Programmable Button Control: ✓ Auto Intercom Deny Off

Auto Intercom Deny On

Details

Telephone number: ✗

Default short code: ✗

Programmable Button Control: ✓ Auto Intercom Deny On

Break Out

This feature is usable within a system multi-site network. It allows a user on one system in the network to specify that the following dialing be processed by another system on the network as if the user dialed it locally on that other system. Pre-Release 5.0: This feature requires the IP Offices to have **Advanced Small Community Networking** licenses.

Details

Telephone Number: The IP Address or Name of the system, using * characters in place of . characters.

Default Short Code: ✗

Programmable Button Control: BkOut

Release: 4.0+.

Example On a system, to break out via a system called RemoteSwitch with the IP Address 192.168.42.3, either of the following short codes could be used.

Example 1

Code: *80*N#

Telephone Number: N

Feature: Break Out

Example 2

Code: *81

Telephone Number: RemoteSwitch

Feature: Break Out

Example 1 allows break out using any remote switch by dialing its IP address, for example *80*192*168*42*3#. Example 2 does this for a specific remote system by dialing just *81.

Barred

This short code feature can be used for call barring by using the short code as the call destination. This short code feature was previously called **Busy**. It has been renamed but its function has not changed.

When used in an ARS form that has been configured with an Alternate Route, for callers whose dialing has matched the short code no further routing is applied.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✗

Release: 1.0+.

Busy On Held

When on, busy on held returns busy to new calls when the user has an existing call on hold. This short code feature is useful when a user does not want to be distracted by an additional incoming call when they have a call on hold.

Details

Telephone Number: ✓ Y or 1 for on, N or 0 for off.

Default Short Code: ✗

Programmable Button Control: ✓ BusyH

Release: 1.0+.

Example: Turning Busy on Held on

If on, when the user has a call on hold, new calls receive busy tone (ringing if analog) or are diverted to Voicemail if enabled, rather than ringing the user.

Note:

This overrides call waiting when the user has a call on hold.

Short Code: *12

Telephone Number: Y

Feature: BusyOnHeld

Example: Turning Busy on Held off

Another short code must be created to turn the Busy on Held feature off. If off, when the uses has a call on hold, new calls will still get directed to the user.

Short Code: *13

Telephone Number: N

Feature: BusyOnHeld

Call Intrude

This feature allows you to intrude on the existing connected call of the specified target user. All call parties are put into a conference and can talk to and hear each other. A **Call Intrude** attempt to a user who is idle becomes a Priority Call.

The ability to intrude and be intruded is controlled by two configuration settings, the Can Intrude (User | Telephony | Supervisor Settings) setting of the user intruding and the Cannot Be Intruded (User | Telephony | Supervisor Settings) setting of target being intruded on. The setting of any other internal party is ignored. By default, no users can intrude and all users are set to cannot be intruded.

Note that this feature requires conference resources from the system for the duration of the intrusion.

Users can use privacy features that to indicate that a call cannot be intruded on. See Private Calls.

Intruding onto a user doing silent monitoring (Call Listen on page 716) is turned into a silent monitoring call.

The system support a range of other call intrusion methods in addition to this feature.

Details

Telephone Number: ✓ Target extension number.

Default Short Code: ✗

Programmable Button Control: ✓ Intru

See also: Call Listen on page 716, Coaching Intrusion on page 730, Dial Inclusion on page 739, Whisper Page on page 788.

Release: 1.0+.

Call Listen

This feature allows you to monitor another user's call without being heard. Monitoring can be accompanied by a tone heard by all parties. Use of the tone is controlled by the Beep on Listen setting on the System | Telephony | Tones & Music tab. The default for this setting is on. If enabled, this is the only indication of monitoring given to the monitored user. There is no phone display indication of monitoring.

Warning:

The use of features to listen to a call without the other call parties being aware of that monitoring may be subject to local laws and regulations. Before enabling the feature you must ensure that you have complied with all applicable local laws and regulations. Failure to do so may result in severe penalties.

The use of call listen is dependant on:

The target being a member of the group set as the user's Monitor Group (User | Telephony | Supervisor Settings). The user does not have to be a member of the group.

The ability to intrude and be intruded is controlled by two configuration settings, the Can Intrude (User | Telephony | Supervisor Settings) setting of the user intruding and the Cannot Be Intruded (User | Telephony | Supervisor Settings) setting of target being intruded on. The setting of any other internal party is ignored. By default, no users can intrude and all users are set to cannot be intruded.

This feature uses system conference resources. If insufficient conference resource are available it will not be possible to use this feature.

A number of features are supported for call listening:

- Users can be given privacy features that allow them to indicate that a call cannot be monitored. See Private Calls.
- IP extensions can be monitored including those using direct media. Previously the monitoring of IP extensions could not be guaranteed.
- The monitoring call can be initiated even if the target user is not currently on a call and remains active until the monitoring user clears the monitoring call.
- The user who initiated the call listen can also record the call.

Intruding onto a user doing silent monitoring (Call Listen) is turned into a silent monitoring call.

1400, 1600, 9500 and 9600 Series phones with a user button can initiate listening using that button if the target user meets the criteria for listening.

The system support a range of other call intrusion methods in addition to this feature.

Details

Telephone Number: ✓ Target extension number (extension must be local).

Default Short Code: ✗

Programmable Button Control: ✓ Listn

See also: Call Intrude on page 715, Coaching Intrusion on page 730, Dial Inclusion on page 739, Whisper Page on page 788.

Release: 1.0+.

Example

User 'Extn205' wants to be able to monitor calls received by members of the Hunt Group 'Sales'.

1. For user 'Extn205', in the Monitor Group (User | Telephony | Supervisor Settings) list box select the hunt group.
2. Ensure that **Can Intrude** is checked.
3. Create a user short code to allow Extn205 to start monitoring.
   - **Short Code**: *89*N#
   - **Telephone Number**: N
   - **Line Group ID**: 0.
   - **Feature**: CallListen
4. For each member of the hunt group, check that their **Cannot be Intruded** setting is unchecked.
5. Now when a member of the 'Sales' hunt group is on a call, Extn205 can replace N in the short code with the extension number of that member and monitor their call.

Call Park

Parks the user's current call into the specified park slot number. The call can then be retrieved by other extensions (refer to the appropriate telephone user guide). While parked the caller hears music on hold if available. The 'Unpark Call' feature can be used to retrieve calls from specific park slots.

Park Timeout (System | Telephony | Telephony) controls how long a call will remain parked. When this expires the call will recall to the parking user if they are idle or when they next become idle. The recall call will continue ring and does follow any forwards or go to voicemail.

Details

Telephone Number: ✓ Park slot number. If no park slot number is specified when this short code is used, the system automatically assigns a park slot number based on the extension number of the user parking the call plus one digit 0 to 9.

Park slot IDs can be up to 9 digits in length. Names can also be used for application park slots.

Default Short Code: ✓ *37*N#

Programmable Button Control: ✓ Call Park

See also: Unpark Call.

Release: 1.0+.

Example

This short code is a default within the system configuration. This short code can be used to toggle the feature on/off. N represents the park slot number in which the call will be parked. For example, if a user wants to park a call to slot number 9, the user would dial *37*9#. The call will be parked there until retrieved by another extension or the original extension.

Short Code: *37*N#

Telephone Number: N

Feature: ParkCall

Call Park and Page

Parks the user's current call into the highest park slot number within the range specified on the **System | Telephony | Park & Page** tab, in the **Central Park Range** field. For example, if the specified **Central Park Range** is 1XX, then the Park & Page short code would attempt to Park on 199. If the range is 567XX, then the call would attempt to Park on 56799.

Call Park and Page via short code is primarily useful for phones with no display, or phones on which a Call Park operation is seldom performed. It provides a way for the user to Central Park in a pre-known location. If the highest Central Park slot is already in use, then the short code Call Park and Page attempt will not be successful.

In order to perform a Page after a successful Call Park via short code, the user must enter a valid Page short code.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✓ Call Park and Page

Release: 9.0+.

Call Pickup Any

Pick up the first available ringing call.

Details

Telephone Number: ✗

Default Short Code: ✓ *30

Programmable Button Control: ✓ PickA

See also: Call Pickup Extn, Call Pickup Group, Call Pickup Members, Acquire Call, Call Pickup Line, Call Pickup User.

Release: 1.0+.

Example

Below is an example of the short code setup:

- **Short Code**: *30
- **Feature**: CallPickupAny

Call Pickup Extn

Pick up a ringing call from a specific extension.

Details

Telephone Number: ✓ Target extension number.

Default Short Code: ✓ *32*N#

Programmable Button Control: ✓ CpkUp

See also: Call Pickup Any, Call Pickup Group, Call Pickup Members, Acquire Call, Call Pickup Line, Call Pickup User.

Release: 1.0+.

Example

This short code is a default within the system configuration. N represents the specific extension. For example, if a user dials *32*201#, they will pick up the call coming into extension 201.

Short Code: *32*N#

Telephone Number: N

Feature: CallPickupAny

Call Pickup Group

Pick up a call ringing any hunt group of which the user is a member. The user can use this feature even if their membership of the group is currently set as disabled.

Details

Telephone Number: ✗

Default Short Code: ✓ *31

Programmable Button Control: ✓ PickG

See also: Call Pickup Any, Call Pickup Extn, Call Pickup Members, Acquire Call, Call Pickup Line, Call Pickup User.

Release: 1.0+.

Example

Below is an example of the short code setup.

Short Code: *31

Feature: CallPickupGroup

Call Pickup Line

Pick up an incoming call which is alerting, parked or held. The pickup uses the Line Appearance ID specified in Telephone Number field of the short code. It cannot be used to pickup conferenced calls. The normal user intrusion features are not applied to this pickup feature. This feature is not supported on T3 phones.

Details

Telephone Number: ✓ Target Line Appearance ID.

Default Short Code: ✗

Programmable Button Control: ✗

See also: Call Pickup Any, Call Pickup Extn, Call Pickup Group, Call Pickup Members, Acquire Call, Call Pickup User.

Release: 4.0+ (Added in the Release 4.0 Q2 2007 maintenance release).

Example

This short code is a default within the system configuration. N represents the specific Line Appearance ID.

Short Code: *89*N#

Telephone Number: N

Feature: CallPickupLine

Call Pickup Members

This feature can be used to pick up a ringing or queuing call at an extension that is a member of the Hunt Group specified. The call picked up does not have to be a hunt group call. The function includes group members even if their membership of the group is currently disabled.

Details

Telephone Number: ✓ Group number or "Group name".

Default Short Code: ✓ *53*N#

Programmable Button Control: ✓ PickM

See also: Call Pickup Any, Call Pickup Extn, Call Pickup Group, Acquire Call, Call Pickup Line, Call Pickup User.

Release: 1.0+.

Example

Below is an example of the short code setup. N represents the extension number of the Hunt Group. For example, if a user dials *53*500#, they will pick up the call coming into extension 500 (the hunt group's extension).

Short Code: *53*N#

Telephone Number: N

Feature: CallPickupMembers

Call Pickup User

Pick up an incoming call which is alerting, parked or held. The pickup uses the user extension number specified in Telephone Number field of the short code. If there are multiple calls, priority is given to picking up alerting, then parked and then held in that order of priority. It cannot be used to pickup conferenced calls. The normal user intrusion features are not applied to this pickup feature. This feature is not supported on T3 phones.

Details

Telephone Number: ✓ Target user extension number.

Default Short Code: ✗

Programmable Button Control: ✗

See also: Call Pickup Any, Call Pickup Extn, Call Pickup Group, Call Pickup Members, Acquire Call, Call Pickup Line.

Release: 4.0+.

Example

N represents the specific user.

Short Code: *89*N#

Telephone Number: N

Feature: CallPickupUser

Call Queue

Queue the current call to the destination phone, even when the destination phone is busy. This is the same as a transfer except it allows you to transfer to a busy phone.

Details

Telephone Number: ✓ Target extension number.

Default Short Code: ✓ *33*N#

Programmable Button Control: ✓ Queue

Release: 1.0+.

Example

Below is an example of the short code setup. N represents the extension the caller wishes to queue for. For example, if a user dials *33*201# while connected to a caller, this caller will be queued for extension 201.

Short Code: *33*N#

Telephone Number: N

Feature: CallQueue

Call Record

This feature allows you to record a conversation. To use this requires Voicemail Pro. Refer to your local regulations in relation to the recording of calls.

This feature uses system conference resources. If insufficient conference resource are available it will not be possible to use this feature.

Release 4.0+: The system provides privacy features that allow users to indicate that a call should not be recorded. See Private Calls.

Details

Telephone Number: ✓ Target extension number.

Default Short Code: ✗

Programmable Button Control: ✓ Recor

Release: 1.0+.

Example: Record your own extension's call

To use this short code, the user should place the call on hold and dial *55. They will automatically be reconnected to the call when recording begins.

Short Code: *55

Telephone Number: None

Feature: CallRecord

Call Steal

This function can be used with or without a specified user target.

If the target has alerting calls, the function will connect to the longest waiting call.

If the target has no alerting calls but does have a connected call, the function will take over the connected call, disconnecting the original user. This usage is subject to the **Can Intrude** setting of the **Call Steal** user and the **Cannot Be Intruded** setting of the target.

If no target is specified, the function attempts to reclaim the user's last ringing or transferred call if it has not been answered or has been answered by voicemail.

Details

Telephone Number: ✓ Target extension number or blank for last call transferred.

Default Short Code: ✓ *45*N# and *46

Programmable Button Control: ✓ Aquire

Release: 2.1+

Example: Taking Over a Call

In this example, N represents the extension to be taken over. For example, if a user dials *45*201#, they will take over the current call on extension 201.

Short Code: *45*N#

Telephone Number: N

Feature: Call Steal

Example: Reclaiming a Call

This short code reclaims the last call from your extension. This function is useful when you want to catch a call you have just missed that has gone off to Voicemail.

Short Code: *46

Feature: Call Steal

Call Waiting On

Enables call waiting on the user's extension. When on, if the user receives a second calls when already on a call, they hear a call waiting tone in the speech path.

Call waiting settings are ignored for users with multiple call appearance buttons. In this case the appearance buttons are used to indicate additional calls. Call waiting is automatically applied for users with 'internal twinned' phones.

Details

Telephone Number: ✗

Default Short Code: ✓ *15 (not on Server Edition)

Programmable Button Control: ✓ CWOn

See also: Call Waiting Off, Call Waiting Suspend.

Release: 1.0+.

Example

Below is a sample of the short code setup.

Short Code: *15

Feature: CallWaitingOn

Call Waiting Off

Disables call waiting on the user's extension. Call waiting may be applied for users with internal twinned phones regardless of their call waiting settings.

Details

Telephone Number: ✗

Default Short Code: ✓ *16 (not on Server Edition)

Programmable Button Control: ✓ CWOff

See also: Call Waiting On, Call Waiting Suspend.

Release: 1.0+.

Example

Below is a sample of the short code setup.

Short Code: *16

Feature: Call Waiting Off

Call Waiting Suspend

For phones using call waiting, this feature temporarily disables call waiting for the duration of the user's next call.

Details

Telephone Number: ✗

Default Short Code: ✓ *70 (A-Law only)

Programmable Button Control: ✓ CWSus

See also: Call Waiting On, Call Waiting Off.

Release: 1.0+.

Example

Below is a sample of the short code setup. This short code is a default within the system configuration.

Short Code: *70

Feature: CallWaitingSuspend

Cancel All Forwarding

This feature cancels all forms of forwarding on the user's extension including "Follow Me" and "Do Not Disturb".

Details

Telephone Number: ✗

Default Short Code: ✓ *00

Programmable Button Control: ✓ FwdOf

See also: Forward On Busy On, Forward On Busy Off, Forward On No Answer On, Forward On No Answer Off, Forward Unconditional On, Forward Unconditional Off, Do Not Disturb On, Do Not Disturb Off.

Release: 1.0+.

Example

Below is a sample of the short code setup.

Short Code: *00

Feature: CancelCallForwarding

Cancel Ring Back When Free

Cancels any existing ring back (also known as callback) set by the user.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✓ RBak-

See also: Ring Back When Free.

Release: 1.0+.

Example: Cancel Ring Back When Free

This example Short Code will cancel Ring Back When Free on the specified extension. N represents the target extension from which you have set a ring back. For example, if Paul has set a ring back on extension 201, he must dial *84*201# to cancel that ring back request.

Short Code: *84*N#

Telephone Number: N

Feature: CancelRingBackWhenFree

Change Login Code

Allows a user to change their login code. The login code must meet the **Login Code Complexity** requirements defined on the Manager **System | Telephony** tab.

Details

Telephone Number: ✓ The user's current and new log in codes separated by a *, see the examples below.

Default Short Code: ✗

Programmable Button Control: ✗

Example

The user has a **Login Code** of **1234** and wants to change it to **5678**. To use the short code below, the user must dial ***60*1234*5678#**.

Short Code: *60*N#

Telephone Number: N

Feature: Change Login Code.

Example

For a user with no login code currently set, they can still use the short code to set a login code. For example using the short code created above to set their login code to 1234 they should dial ***60**1234#**.

Example

System phone users can also use this short code to change the login code of an other user. For example 403 is configured as a system phone with a login code of **1234**. User 410 has forgotten their login code and needs it changed. User 403 can do this by dialing the following:

60*410*1234<new code>**#**

Clear After Call Work

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✓ ACWrk

See also: Start After Call Work.

Release: 4.2 4Q 2008 Maintenance release+.

Clear Call

This feature can be used to end the current call.

Details

Telephone Number: ✗

Default Short Code: ✓ *52

Programmable Button Control: ✓ Clear

Release: 1.0+.

Example

Below is a sample of the short code setup. This example could be used in a situation where you are doing a supervised transfer and the party to be transferred to does not want to take the call. In this scenario, you can put the call on hold and dial *52. This will clear the last connected call (for example the party who has just refused the transfer), and retrieve the original call or dial tone.

Short Code: *52

Feature: Deny/ClearCall

Clear CW

This feature is most commonly used to end the user's current call and answer the waiting call.

Note:

Call waiting settings are ignored for users with multiple call appearance buttons.

Details

Telephone Number: ✗

Default Short Code: ✓ *26 (A-Law only) (not on Server Edition)

Programmable Button Control: ✓ ClrCW

Release: 1.0+.

Example

Below is a sample of the short code setup.

Short Code: *26

Feature: ClearCW

Clear Hunt Group Night Service

This feature changes the specified hunt group from Night Service mode to In Service mode.

Setting and clearing hunt group night service can be done using either manual controls or using a system time profile. The use of both methods to control the night service status of a particular hunt group is not supported.

This function is currently not supported between systems in a multi-site network. It can only be used by a user currently logged onto the same system as hosting the hunt group.

Details

Telephone Number: ✓ Hunt group extension number. If left blank, the short code will affect all hunt groups of which the user is a member.

The **Set Hunt Group Night Service** and **Clear Hunt Group Night Service** short code and button features can be used to switch an SSL VPN service off or on respectively. The service is indicated by setting the service name as the telephone number or action data. Do not use quotation marks.

Default Short Code: ✓ *21*N#

Programmable Button Control: ✓ HGNS-

See also: Clear Hunt Group Out Of Service, Set Hunt Group Night Service, Set Hunt Group Out Of Service.

Release: 1.0+.

Example

Below is a sample of the short code setup. N represents the telephone number of the hunt group to be taken out of "Night Service" mode and placed into "In Service" mode. For example, when *21*201# is dialed, the hunt group associated with extension 201 will be taken out of "Night Service" mode.

Short Code: *21*N#

Telephone Number: N

Feature: ClearHuntGroupNightService

Clear Hunt Group Out Of Service

This feature changes the specified hunt group from Out of Service mode to In Service mode. This will not override a hunt group in night service due to a time profile.

Details

Telephone Number: ✓ Hunt group extension number. If left blank, the short code will affect all hunt groups of which the user is a member.

Default Short Code: ✗

Programmable Button Control: ✓ HGOS-

See also: Clear Hunt Group Night Service, Set Hunt Group Night Service, Set Hunt Group Out Of Service.

Release: 1.0+.

Example

Below is a sample short code using the Clear Hunt Group Out Of Service feature. N represents the telephone number of the hunt group to be taken out of "Out of Service" mode. For example,

when *55*201# is dialed, the hunt group associated with extension 201 will be placed into "In Service" mode.

Short Code: *55*N#

Telephone Number: N

Feature: ClearHuntGroupOutOfService

Clear Quota

This feature refreshes the time quota for all services or a specific service.

Details

Telephone Number: ✓ "Service name" or "" (all services).

Default Short Code: ✗

Programmable Button Control: ✓ Quota

Release: 1.0+.

Coaching Intrusion

This feature allows the you to intrude on another user's call and to talk to them without being heard by the other call parties to which they can still talk. For example: User A is on a call with user B. When user C intrudes on user A, they can hear users A and B but can only be heard by user A.

The ability to intrude and be intruded is controlled by two configuration settings, the Can Intrude (User | Telephony | Supervisor Settings) setting of the user intruding and the Cannot Be Intruded (User | Telephony | Supervisor Settings) setting of target being intruded on. The setting of any other internal party is ignored. By default, no users can intrude and all users are set to cannot be intruded.

Warning:

The use of features to listen to a call without the other call parties being aware of that monitoring may be subject to local laws and regulations. Before enabling the feature you must ensure that you have complied with all applicable local laws and regulations. Failure to do so may result in severe penalties.

The system support a range of other call intrusion methods in addition to this feature.

Details

Telephone Number: ✓ Target extension number.

Default Short Code: ✗

Programmable Button Control: ✓ Coach.

See also: Call Intrude, Call Listen, Dial Inclusion, Whisper Page.

Release:9.0+

Conference Add

Conference add controls can be used to place the user, their current call and any calls they have on hold into a conference. When used to start a new conference, the system automatically assigns a conference ID to the call. This is termed ad-hoc (impromptu) conferencing.

If the call on hold is an existing conference, the user and any current call are added to that conference. This can be used to add additional calls to an ad-hoc conference or to a meet-me conference. Conference add can be used to connect two parties together. After creating the conference, the user can drop from the conference and the two incoming calls remain connected.

For further details refer to the Conferencing section.

Details

Telephone Number: ✗

Default Short Code: ✓ *47

Programmable Button Control: ✓ Conf+

See also: Conference Meet Me.

Release: 1.0+.

Example

Below is a sample of the short code setup.

Short Code: *47

Feature: ConferenceAdd

Conference Meet Me

Conference meet-me refers to features that allow a user or caller to join a specific conference by using the conference's ID number (either pre-set in the control or entered at the time of joining the conference).

IP500 and IP500 V2 systems require a **Preferred Edition** license.

Note:

Conference Meet Me features can create conferences that include only one or two parties. These are still conferences that are using resources from the host system's conference capacity.

Conference ID Numbers

By default, ad hoc conferences are assigned numbers starting from 100 for the first conference in progress. Therefore, for conference Meet Me features specify a number away from this range ensure that the conference joined is not an ad hoc conference started by other users. It is no longer possible to join a conference using conference Meet Me features when the conference ID is in use by an ad-hoc conference.

User Personal Conference Number Each user's own extension number is treated as their own personal conference number. Only that user is able to start a conference using that number as the conference ID. Any one else attempting to start a conference with that number will find themselves in a conference but on hold until the owner also joins. Personal conferences are always hosted on the owner's system.

Note:

When a user calls from their mobile twinned number, the personal conference feature will only work if they access the conference using an FNE 18 service.

Multi-Site Network Conferencing

Meet Me conference IDs are now shared across a multi-site network. For example, if a conference with the ID 500 is started on one system, anyone else joining conference 500 on any system will join the same conference. Each conference still uses the conference resources of the system on which it was started and is limited by the available conference capacity of that system.

Previously separate conferences, each with the same conference ID, could be started on each system in a multi-site network.

Other Features

Transfer to a Conference Button A currently connected caller can be transferred into the conference by pressing **TRANSFER**, then the Conference Meet Me button and **TRANSFER** again to complete the transfer. This allows the user to place callers into the conference specified by the button without being part of the conference call themselves. This option is only support on Avaya phones with a fixed **TRANSFER** button (excluding T3 and T3 IP phones).

Conference Button Status Indication When the conference is active, any buttons associated with the conference ID indicate the active state.

For further details refer to the Conferencing section.

Details

Telephone Number: ✓ Conference number. This can be an alphanumeric value up to 15 characters.

Default Short Code: ✗ / ✓ *66*N# on Server Edition systems.

Programmable Button Control: ✓ CnfMM

See also: Conference Add.

Release: 1.0+.

CW

Pick up the waiting call. This feature provides same functionality as pressing the **Recall** or **Hold** key on the phone. Unlike the Clear CW feature, this feature does not disconnect you from the existing call when the second call is picked up.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✗

Release: 1.0+.

Dial

This short code feature allows users to dial the number specified to an outside line.

Details

Telephone Number: ✓ Telephone number.

Default Short Code: ✓ Various depending on locale and system type.

Programmable Button Control: ✓ Dial

See also: Dial Direct, Dial Emergency, Dial Extn, Dial Inclusion, Dial Paging.

Release: 1.0+.

Example: Creating a Speed Dial

In this example, users entering 401 on their telephone key pad will dial the New Jersey Office on 212 555 0000.

Short Code: 401

Telephone Number: 2125550000

Example: Replace Outgoing Caller ID

This short code is useful in a "call center" environment where you do not want customers to have access to the number of your direct line; you want the general office number displayed. The sample short code below will force the outgoing caller ID to display 123.

Note:

The usability of this feature is dependent upon your local service provider.

Short Code: ?

Telephone Number: .s123

Example: External Dialing Prefix

The short code is for dialing a prefix for an outside line N represents the external number you want to call.

Short Code: 9N

Telephone Number: N

Example: Blocking Caller ID

This is for blocking Caller ID for external calls. This feature can be applied to specific external numbers or to all out going calls. In most situations, the company will choose to block the caller ID for all external calls or leave it available for all external calls.

Short Code: 9N

Telephone Number: NW

Example: Maximum Call Length

The character t can be used in dialing short codes to set the maximum allowed duration of a call. For example, the following short code will dial a number but then disconnect the call after 20 minutes (plus or minus a minute).

Short Code: 9N

Telephone Number: Nt(20)

Dial 3K1

Sets the ISDN bearer capabilities to 3.1Khz audio call.

Details

Telephone Number: ✓ Telephone number.

Default Short Code: ✗

Programmable Button Control: ✓ D3K1

Release: 1.0+.

Dial 56K

Sets the ISDN bearer capabilities to 56Kbps data call.

Details

Telephone Number: ✓ Telephone number.

Default Short Code: ✗

Programmable Button Control: ✓ D56K

Release: 1.0+.

Dial 64K

Sets the ISDN bearer capabilities to 64Kbps data call.

Details

Telephone Number: ✓ Telephone number.

Default Short Code: ✗

Programmable Button Control: ✓ D64K

Release: 1.0+.

Dial CW

Call the specified extension number and force call waiting indication on if the extension is already on a call.

If the user has call appearance buttons programmed, call waiting will not get activated. The next incoming call will appear on an available call appearance button. When there are no available call appearance buttons, the next incoming call will receive busy tone.

Details

Telephone Number: ✓ Extension number.

Default Short Code: ✗

Programmable Button Control: ✓ DCW

Release: 1.0+.

Example

N represents the extension number to be dialed. For example, a user dialing *97*201# will force call waiting indication on at extension 201 if extension 201 is already on a call.

Short Code: *97*N#

Telephone Number: N

Feature: DialCW

Dial Direct

Automatic intercom functions allow you to call an extension and have the call automatically answered on speaker phone after 3 beeps. The extension called must support a handsfree speaker. If the extension does not have a handsfree microphone then the user must use the handset if they want to talk. If the extension is not free when called, the call is presented as a normal call on a call appearance button if available.

Details

Telephone Number: ✓ Extension number

Default Short Code: ✗

Programmable Button Control: ✓ Dirct

See also: Dial Paging.

Release: 1.0+.

Example

This allows the extension specified to be automatically answered. N represents the extension that will be forced to automatically answer. For example, when a user dials *83*201#, extension 201 will be forced to automatically answer the call.

Short Code: *83*N#

Telephone Number: N

Feature: DialDirect

Dial Direct Hot Line

When the line appearance button is mapped to a short code using the DialDirectHotLine short code feature, no secondary dial tone is generated and the number is dialed directly. This feature should not be confused with the hot line feature enabled using ?D short codes.

Details

Telephone Number: ✓

Default Short Code: ✗

Programmable Button Control: ✗

Release: 3.0 to 4.0, 8.0+

Example

Below is a sample short code using the DialDirectHotLine feature. The short code *83* should then be set as the prefix for the particular line required.

Short Code: *83*

Telephone Number: .

Feature: DialDirectHotLine

Dial Emergency

Dials the number specified regardless of any call barring applicable to the user.

On all systems, regardless of locale; system and or ARS short codes using the Dial Emergency feature should be created for any required emergency service numbers. Those short codes should be usable by all users from all extensions. Those short codes should route the calls to suitable lines. If the system uses prefixes for external dialing, the dialing of emergency numbers with and without the prefix should be allowed.

The blocking of emergency calls or the rerouting of emergency calls to a intermediate destination other than the central office may be against local and nation laws.

Details

Telephone Number: ✓ Telephone number.

Default Short Code: ✗

Programmable Button Control: ✓ Emrgy

Release: 1.0+.

Dial Extn

This feature can be used to dial an internal extension number (user or hunt group).

Details

Telephone Number: ✓ Extension number.

p(x) can be added as a suffix to the **Telephone Number** to change the priority of a call. Allowable values for **x** are **1**, **2** or **3** for low, medium or high priority respectively. For example **Np(1)**.

Default Short Code: ✗

Programmable Button Control: ✗

See also: Dial Direct, Dial Paging, DialPhysicalExtensionByNumber, DialPhysicalNumberByID.

Release: 1.0+.

Example: Dial on Pick up

The following user short code dials the extension specified the moment the user's handset is picked up.

Short Code: ?D

Telephone Number: 201

Line Group ID: 0

Feature: Dial Extn

Dial Fax

This feature is used to route fax calls via Fax Relay.

Details

Telephone Number: ✓ Fax destination number.

Default Short Code: ✗

Programmable Button Control: ✗

Release: 5.0+.

Example

In this example, the line group ID matches the URI configured on a SIP line that has been configured for Fax Relay.

Short Code: 6N

Telephone Number: N"@192.16.42.5"

Line Group ID: 17

Feature: Dial Fax

Dial Inclusion

This feature allows you to intrude on another user's call to talk to them. Their current call is put on hold while you talk and automatically reconnected when you end the intrusion. The intruder and the target extension can then talk but cannot be heard by the other party. This can include intruding into a conference call, where the conference will continue without the intrusion target.

During the intrusion all parties hear a repeated intrusion tone. When the intruder hangs-up the original call parties are reconnected. Attempting to hold a dial inclusion call simply ends the intrusion. The inclusion cannot be parked.

The ability to intrude and be intruded is controlled by two configuration settings, the Can Intrude (User | Telephony | Supervisor Settings) setting of the user intruding and the Cannot Be Intruded (User | Telephony | Supervisor Settings) setting of target being intruded on. The setting of any other internal party is ignored. By default, no users can intrude and all users are set to cannot be intruded.

The system support a range of other call intrusion methods in addition to this feature.

Details

Telephone Number: ✓ Target extension number.

Default Short Code: ✗

Programmable Button Control: ✓ Inclu.

See also: Call Intrude, Call Listen, Coaching Intrusion, Whisper Page.

Release: 1.4+.

Example

N represents the extension to be intruded upon. For example, if a user dials *97*201# while extension 201 is on a call, then the user is intruding into extn. 201's current call.

Short Code: *97*N#

Telephone Number: N

Feature: DialInclusion

Dial Paging

This feature makes a page call to an extension or group. The target extension or group members must support page calls (that is be able to auto-answer calls).

Details

Telephone Number: ✓ Extension or group number.

Default Short Code: ✗

Programmable Button Control: ✓ Page

See also: Dial Direct.

Release: 1.0+.

When paging, always use only one codec (the preferred). It is the system administrator's responsibility to ensure all the phones in the paging group support the codec.

Dial Physical Extension by Number

Dial a specified extension number regardless of the current user logged in at that extension and any forwarding, follow me or do not disturb settings applied by the current extension user. Note that the extension number used is the Base Extension number set against the extension configuration settings.

Details

Telephone Number: ✓ Base Extension number.

Default Short Code: ✓ *70*N# (U-Law only) (not on Server Edition)

Programmable Button Control: ✓ PhyEx

See also: Dial Physical Extension By Id, Priority Call.

Release: 1.4+.

Example

The example below allows the extension with the base extension number 201 to be called regardless of the extension number of the user currently logged in at that extension.

Short Code: *97

Telephone Number: 201

Feature: DialPhysicalExtnByNumber

Dial Physical Extension By ID

Dial a specific extension using its system ID. This may be necessary in hot desking environments where some extensions have been created with no default extension number. Without an extension number, a call can not be made to that extension unless a short code is created.

Details

Telephone Number: ✓ Extension ID

Default Short Code: ✓ *71*N# (U-Law only)

Programmable Button Control: ✓ DialP

See also: DialPhysicalExtensionByNumber, Priority Call.

Release: 1.4+.

Example

In the above example, if the telephone at extension ID 16 is not associated with an extension number, a user can dial *97 to connect to that phone. This may be useful in hot desking environments where some extensions may not have a dedicated base extension number.

Short Code: *97

Telephone Number: 16

Feature: DialPhysicalNumberByID

Dial Speech

This feature allows a short code to be created to force the outgoing call to use the Speech bearer capability.

Details

Telephone Number: ✓ Telephone number.

Default Short Code: ✗

Programmable Button Control: ✓ DSpch

Release: 1.0+.

Dial V110

Sets the ISDN bearer capabilities to V110. The call is presented to local exchange as a "Data Call".

Details

Telephone Number: ✓ Telephone number.

Default Short Code: ✗

Programmable Button Control: ✓ DV110

Release: 1.0+.

Dial V120

Sets the ISDN bear capabilities using V.120.

Details

Telephone Number: ✓ Telephone number.

Default Short Code: ✗

Programmable Button Control: ✓ DV120

Release: 1.0+.

Dial Video

The call is presented to the local exchange as a "Video Call".

Details

Telephone Number: ✓ Telephone number.

Default Short Code: ✗

Programmable Button Control: ✓ Dvide

Release: 1.0+.

Disable ARS Form

This feature can be used to put an ARS form out of service. It can be used with ARS forms for which an Out of Service Route has been configured in Manager. The short code feature Enable ARS Form can be used to return an ARS form to in service.

Details

Telephone Number: ARS form number.

Default Short Code: ✗

Programmable Button Control: ✗

See also: Enable ARS Form

Release: 4.0+.

Disable Internal Forwards

This feature turns off the forwarding of internal calls for the user. It applies to Forward Unconditional, Forward on Busy and Forward on No Answer.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✗

See also: Disable Internal Forwards Unconditional, Disable Internal Forwards Busy or No Answer, Cancel All Forwarding, Enable Internal Forwards, Enable Internal Forwards Unconditional, Enable Internal Forwards Busy or No Answer.

Release: 3.2+.

Disable Internal Forward Unconditional

This feature turns off the forwarding of internal calls for the user. It applies to Forward Unconditional only.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✗

See also: Disable Internal Forwards, Disable Internal Forwards Busy or No Answer, Cancel All Forwarding, Enable Internal Forwards, Enable Internal Forwards Unconditional, Enable Internal Forwards Busy or No Answer.

Release: 3.2+.

Disable Internal Forward Busy or No Answer

This feature turns off the forwarding of internal calls for the user. It applies to Forward on Busy and Forward on No Answer.

Telephone Number: No

Default Short Code: No

Programmable Button Control: No

See also: Disable Internal Forwards, Disable Internal Forwards Unconditional, Cancel All Forwarding, Enable Internal Forwards, Enable Internal Forwards Unconditional, Enable Internal Forwards Busy or No Answer.

Display Msg

Allows the sending of text messages to digital phones on the local system.

Telephone Number: The telephone number takes the format N";T" where:

- **N** is the target extension.
- **T** is the text message. Note that the **";** before the text and the **"** after the text are required.

Default Short Code: No

Programmable Button Control: Displ

Example

Below is a sample of the short code setup. When used, the target extension will hear a single ring and then see the message. If the target extension is on a call then may need to scroll the display to a free call appearance in order to see the text message.

Short Code: *78*N#

Feature: Display Msg

Telephone Number: N";Visitor in Reception"

SIP Extension Message Waiting Indicator

You can use the Display Msg short code to turn a SIP extension message waiting indicator (MWI) on or off.

Telephone Number: The telephone number takes the format N";T" where:

- **N** is the target extension.
- **T** is the text message. Note that the **";** before the text and the **"** after the text are required.

To turn MWI on, the telephone number must be **N";Mailbox Msgs=1"**.

To turn MWI off, the telephone number must be **N";Mailbox Msgs=0"**.

Default Short Code: No

Example

Below is a sample of the short code setup to turn MWI on. When used, the target extension will receive a SIP message directing it to turn the MWI on.

Short Code: *99*N#

Feature: Display Msg

Telephone Number: N";Mailbox Msgs=1"

Example

Below is a sample of the short code setup to turn MWI off. When used, the target extension will receive a SIP message directing it to turn the MWI off.

Short Code: *98*N#

Feature: Display Msg

Telephone Number: N";Mailbox Msgs=0"

Do Not Disturb Exception Add

This feature adds a number to the user's "Do Not Disturb Exception Numbers List". This can be an internal extension number or external ICLID. Calls from that number, except hunt group calls, will ignore the user's Do Not Disturb setting. For further details see Do Not Disturb (DND).

Telephone Number: Telephone number or ICLID. Up to 31 characters. For ICLID numbers any prefix added by the system must also be included.

Default Short Code: *10*N#

Programmable Button Control: DNDX+

See also: Do Not Disturb Exception Delete, Do Not Disturb On, Do Not Disturb Off.

Example

N represents the number to be added to the user's "Do Not Disturb Exception List". For example, when a user has DND turned on and dials *10*4085551234#, incoming calls from telephone number (408) 555-1234. All other calls, except those numbers on the exception list hear busy tones or are redirected to voicemail if available.

Short Code: *10*N#

Telephone Number: N

Feature: DoNotDisturbExceptionAdd

Example

In this example, the last number received by the user is added to their exception list.

Short Code: *89

Telephone Number: L

Feature: DoNotDisturbExceptionAdd

Do Not Disturb Exception Delete

This feature removes a number from the user's "Do Not Disturb Exception List". For further details see Do Not Disturb (DND).

Details

Telephone Number: ✓ Telephone number or ICLID.

Default Short Code: ✓ *11*N#

Programmable Button Control: ✓ DNDX-

See also: Do Not Disturb Exception Add, Do Not Disturb On, Do Not Disturb Off.

Release: 1.0+.

Example

N represents the number to be deleted from the user's "Do Not Disturb Exception List". For example, when a user has DND turned on and the telephone number (408) 555-1234 in their "Do Not Disturb Exception List", dialing *10*4085551234# will remove this phone number from the list. Incoming calls from (408) 555-1234 will no longer be allowed through; instead they will hear busy tone or be redirected to voicemail if available.

Short Code: *11*N#

Telephone Number: N

Feature: DoNotDisturbExceptionDel

Do Not Disturb On

This feature puts the user into 'Do Not Disturb' mode. When on, all calls, except those from numbers in the user's exception list hear busy tones or are redirected to voicemail if available. For further details see Do Not Disturb (DND).

Details

Telephone Number: ✗

Default Short Code: ✓ *08

Programmable Button Control: ✓ DNDOn

See also: Do Not Disturb Off, Do Not Disturb Exception Add, Do Not Disturb Exception Delete.

Release: 1.0+.

Example

Below is a sample of the short code setup.

Short Code: *08

Feature: DoNotDisturbOn

Do Not Disturb Off

Cancels the user's 'do not disturb' mode if set. For further details see Do Not Disturb (DND).

Details

Telephone Number: ✗

Default Short Code: ✓ *09

Programmable Button Control: ✓ DNDOf

See also: Do Not Disturb On, Do Not Disturb Exception Add, Do Not Disturb Exception Delete.

Release: 1.0+.

Example

This short code is a default within the system configuration. Below is a sample of the short code setup.

Short Code: *09

Feature: DoNotDisturbOff

Enable ARS Form

This feature can be used to put an ARS form in service. It can be used with ARS forms that have been put out of service through Manager or the use of a Disable ARS Form short code.

Details

Telephone Number: ARS form number.

Default Short Code: ✗

Programmable Button Control: ✗

Release: 4.0+

Enable Internal Forwards

This feature turns on the forwarding of internal calls for the user. It applies to Forward Unconditional, Forward on Busy and Forward on No Answer.

Details

Telephone Number: ✕

Default Short Code: ✕

Programmable Button Control: ✕

See also: Disable Internal Forwards, Disable Internal Forwards Unconditional, Disable Internal Forwards Busy or No Answer, Cancel All Forwarding, Enable Internal Forwards Unconditional, Enable Internal Forwards Busy or No Answer.

Release: 3.2+.

Enable Internal Forward Unconditional

This feature turns on the forwarding of internal calls for the user. It applies to Forward Unconditional only.

Details

Telephone Number: ✕

Default Short Code: ✕

Programmable Button Control: ✕

See also: Disable Internal Forwards, Disable Internal Forwards Unconditional, Disable Internal Forwards Busy or No Answer, Cancel All Forwarding, Enable Internal Forwards, Enable Internal Forwards Busy or No Answer.

Release: 3.2+.

Enable Internal Forward Busy or No Answer

This feature turns on the forwarding of internal calls for the user. It applies to Forward on Busy and Forward on No Answer.

Details

Telephone Number: ✕

Default Short Code: ✕

Programmable Button Control: ✕

See also: Disable Internal Forwards, Disable Internal Forwards Unconditional, Disable Internal Forwards Busy or No Answer, Cancel All Forwarding, Enable Internal Forwards, Enable Internal Forwards Unconditional.

Release: 3.2+.

Extn Login

Extn Login allows a user who has been configured with a Login Code (User | Telephony | Supervisor Settings) to take over ownership of any extension. That user's extension number becomes the extension number of the extension while they are logged.

When used, the user will be prompted to enter their extension number and then their log in code. Login codes of up to 15 digits are supported with **Extn Login** buttons. Login codes of up to 31 digits are supported with **Extn Login** short codes.

When a user logs in, as many of their user settings as possible are applied to the extension. The range of settings applied depends on the phone type and on the system configuration.

By default, on 1400 Series, 1600 Series, 9500 Series and 9600 Series phones, the user's call log and personal directory are accessible while they are logged in. This also applied to M-Series and T-Series telephones.

On other types of phone, those items such as call logs and speed dials are typically stored locally by the phone and will not change when users log in and log out.

If the user logging in was already logged in or associated with another phone, they will be automatically logged out that phone.

Details

Telephone Number: ✓ Extension Number*Login Code. If just a single number is dialed containing no * separator, the system assumes that the extension number to use is the physical extension's Base Extension number and that the number dialed is the log in code.

Default Short Code: ✓ *35*N#

Programmable Button Control: ✓ Login

See also: Extn Logout.

Example: Individual Hot Desking

Based on the above sample short code, Paul (extension 204) can go to another phone (even if it is already logged in by another user) and log in as extension 204 by simply dialing 299. Once Paul has logged into this phone, extension 204 is logged out at Paul's original phone. For Paul to make use of this short code, his log in code must match that configured in the above short code. When Paul logs out of the phone he has "borrowed", his original extension will automatically be logged back in.

Short Code: 299

Telephone Number: 204*1234

Feature: Extnlogin

Example: Log In

The default short code for logging into a phone is configured as shown below. N represents the users extension number followed by a * and then their log in code, for example *35*401*123#.

Short Code: *35*N#

Telephone: N

Feature: ExtnLogin

Extn Logout

This feature logs the user off the phone at which they are logged in. This feature cannot be used by a user who does not have a log in code or by the default associated user of an extension unless they are set to forced log in.

Details

Telephone Number: ✗

Default Short Code: ✓ *36

Programmable Button Control: ✓ Logof

See also: Extn Login.

Release: 1.0+.

Example

Below is a sample short code using the Extn Logout feature. This short code is a default within the system configuration.

Short Code: *36

Feature: ExtnLogout

Flash Hook

This feature sends a hook flash signal to the currently connected line if it is an analog line.

Details

Telephone Number: Optional The telephone number field can be used to set the transfer destination number for a Centrex Transfer. In this case the use of the short code Forced Account Code and Forced Authorization Code are not supported and the Line Group Id must match the outgoing line to the Centrex service provider.

Default Short Code: ✗

Programmable Button Control: ✓ Flash

Release: 1.4+.

Example

Below is a sample short code using the Flash Hook feature.

Short Code: *96

Feature: FlashHook

FNE Service

This short code feature is used for Mobile Call Control and one-X Mobile Client support.

Details

Telephone Number: ✓ This number sets the required FNE function.

Default Short Code: ✗

Programmable Button Control: ✗

Release: 4.2+.

Follow Me Here

Causes calls to the extension number specified to be redirected to the extension initiating the 'Follow Me Here'. If the redirected call receives a busy tone or is not answered, then the call behaves as though the User's extension had failed to answer. For further details see Follow Me.

Details

Telephone Number: ✓ Extension to redirect to the dialing extension.

Default Short Code: ✓ *12*N#

Programmable Button Control: ✓ Here+

See also: Follow Me Here Cancel, Follow Me To.

Release: 1.0+.

Example

This feature is used at the Follow Me destination. N represents the extension number of the user wanting their calls redirected to that destination. For example, User A's extension is 224. However they are working at extension 201 and want their calls redirected there. If the following short code is available, they can do this by dialing *12*224# at extension 201.

Short Code: *12*N#

Telephone Number: N

Feature: FollowMeHere

Follow Me Here Cancel

Cancels any Follow Me set on the specified extension. This action can only be performed at the extension to which the Follow Me Here is targetted. For further details see Follow Me.

Details

Telephone Number: ✓ Extension being redirected to the dialing extension.

Default Short Code: ✓ *13*N#

Programmable Button Control: ✓ Here-

See also: Follow Me Here, Follow Me To.

Release: 1.0+.

Example

This feature is used at the Follow Me destination. N represents the extension number of the user whose calls are being redirected to that destination. For example, User A's extension is 224. However they are working at extension 201 and so have set a Follow Me on their own extension to redirect their calls to 201. If the following short code is available, they can cancel the Follow Me by dialing *13*224# at extension 201.

Short Code: *13*N#

Telephone Number: N

Feature: FollowMeHereCancel

Follow Me To

Causes calls to the extension to be redirected to the Follow Me destination extension specified. For further details see Follow Me.

Details

Telephone Number: ✓ Target extension number or blank (cancel Follow Me To)

Default Short Code: ✓ *14*N#

Programmable Button Control: ✓ FolTo

See also: Follow Me Here, Follow Me Here Cancel.

Release: 1.0+.

Example

This feature is used at the extension that wants to be redirected. N represents the extension number to which the user wants their calls redirected. For example, User A's extension is 224. However they are working at extension 201 and want their calls redirected there. If the following short code is available, they can do this by dialing *14*201# at extension 224.

Short Code: *14*N#

Telephone Number: N

Feature: FollowMeTo

Forward Hunt Group Calls On

Forward the user's hunt group calls (internal and external) to their forward number when the user has Forward Unconditional active. For further details see Forward Unconditional.

This option is only applied for calls to **Sequential** and **Rotary** type hunt groups. Calls from other types of hunt group types are not presented to the user when they have Forward Unconditional active. Note also that hunt group calls cannot be forwarded to another hunt group.

Details

Telephone Number: ✗

Default Short Code: ✓ *50

Programmable Button Control: ✓ FwdH+

See also: Forward Hunt Group Calls Off, Forward Unconditional On, Forward Unconditional Off.

Release: 1.0+.

Example

This short code is useful if the hunt group member temporarily uses another workstation and so does not require a permanent extension change.

Short Code: *50

Feature: ForwardHuntgroupCallsOn

Forward Hunt Group Calls Off

This feature cancels the forwarding of the user's hunt group calls. For further details see Forward Unconditional.

Details

Telephone Number: ✗

Default Short Code: ✓ *51

Programmable Button Control: ✓ FwdH-

See also: Forward Hunt Group Calls On, Forward Unconditional On, Forward Unconditional Off.

Release: 1.0+.

Example

Below is a sample of the short code setup.

Short Code: *51

Feature: ForwardHuntgroupCallsOff

Forward Number

Sets the number to which the user's calls are redirected. This can be an internal or external number. The number is still subject to the user's call barring settings. For further details see Forward Unconditional.

This feature does not activate forwarding; it only sets the number for the forwarding destination.

This number is used for all forward types; Forward Unconditional, Forward on Busy and Forward on No Answer, unless the user has a separate Forward on Busy Number set for forward on busy and forward on no answer functions.

Details

Telephone Number: ✓ Telephone number.

Default Short Code: ✓ *07*N#

Programmable Button Control: ✓ FwdNo

See also: Forward On Busy Number.

Release: 1.0+.

Example

N represents the forward destination. For example, if extension 224 wants to set the forwarding number to extension 201, the user can dial *07*201#.

Short Code: *07N*#

Telephone Number: N

Feature: ForwardNumber

Forward On Busy Number

Sets the number to which the user's calls are forwarded when Forward on Busy or Forward on No Answer are on. If no Forward on Busy Number is set, those functions use the Forward Number.

This feature does not activate the forwarding, it only sets the number for the forwarding destination.

Details

Telephone Number: ✓ Telephone number.

Default Short Code: ✓ *57*N#

Programmable Button Control: ✓ FwBNo

See also: Forward Number.

Release: 1.0+.

Example

N represents the extension number to be forwarded to. For example, if Paul (whose extension is 224) wants to set the forwarding number for his 'Forward on Busy' and/or 'Forward on No Answer' feature to extension 201, Paul can dial *57*201# followed by the short code for the forwarding function.

Short Code: *57N*#

Telephone Number: N

Feature: ForwardOnBusyNumber

Forward On Busy On

This feature enables forwarding when the user's extension is busy. It uses the Forward Number destination or, if set, the Forward on Busy Number destination. If the user has call appearance buttons programmed, the system will not treat them as busy until all the call appearance buttons are in use.

Forward Internal (User | Forwarding) can also be used to control whether internal calls are forwarded.

Details

Telephone Number: ✗

Default Short Code: ✓ *03

Programmable Button Control: ✓ FwBOn

See also: Forward On Busy Off, Cancel All Forwarding, Enable Internal Forward Busy or No Answer.

Release: 1.0+.

Example

Below is a sample of the short code setup.

Short Code: *03

Feature: ForwardOnBusyOn

Forward On Busy Off

This feature cancels forwarding when the user's extension is busy.

Details

Telephone Number: ✗

Default Short Code: ✓ *04

Programmable Button Control: ✓ FwBOf

See also: Forward On Busy On, Cancel All Forwarding.

Release: 1.0+.

Example

Below is a sample of the short code setup.

Short Code: *04

Feature: ForwardOnBusyOff

Forward On No Answer On

This feature enables forwarding when the user's extension is not answered within the period defined by their No Answer Time. It uses the Forward Number destination or, if set, the Forward on Busy Number destination.

Forward Internal (User | Forwarding) can also be used to control whether internal calls are forwarded.

Details

Telephone Number: ✗

Default Short Code: ✓ *05

Programmable Button Control: ✓ FwNOn

See also: Forward On No Answer Off, Cancel All Forwarding.

Release: 1.0+.

Example

Below is a sample of the short code setup. Remember that the forwarding number for this feature uses the 'Forward on Busy Number'.

Short Code: *05

Feature: ForwardOnNoAnswerOn

Forward On No Answer Off

This feature cancels forwarding when the user's extension is not answered.

Details

Telephone Number: ✗

Default Short Code: ✓ *06

Programmable Button Control: ✓ FwNOf

See also: Forward On No Answer On.

Release: 1.0+.

Example

Below is a sample of the short code setup.

Short Code: *06

Feature: ForwardOnNoAnswerOff

Forward Unconditional On

This feature enables forwarding of all calls, except group calls, to the Forward Number set for the user's extension. To also forward hunt group calls, Forward Hunt Group Calls On must also be used. For further details see Forward Unconditional.

Forward Internal (User | Forwarding) can also be used to control whether internal calls are forwarded.

Details

Telephone Number: ✗

Default Short Code: ✓

Programmable Button Control: ✓ FwUOn

See also: Forward Unconditional Off.

Release: 1.0+.

Example

Remember that this feature requires having a forward number configured.

Short Code: *01

Feature: ForwardUnconditionalOn

Forward Unconditional Off

This feature cancels forwarding of all calls from the user's extension.

Note:

This does not disable Forward on No Answer and or Forward on Busy if those functions are also on. For further details see Forward Unconditional.

Details

Telephone Number: ✗

Default Short Code: ✓ *02

Programmable Button Control: ✓ FwUOf

See also: Forward Unconditional On.

Release: 1.0+.

Example

Example

Below is a sample of the short code setup.

Short Code: *02

Feature: ForwardUnconditionalOff

Group Listen Off

Disables the group listen function for the user's extension. See Group Listen On.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✓ GroupListenOn

Release: 4.1+.

Example

Below is a sample short code using the Group Listen Off feature.

Short Code: *27

Feature: GroupListenOff

Group Listen On

Using group listen allows callers to be heard through the phone's handsfree speaker but to only hear the phone's handset microphone. When group listen is enabled, it modifies the handsfree functionality of the user's phone in the following manner

When the user's phone is placed in handsfree/speaker mode, the speech path from the connected party is broadcast on the phone speaker but the phone's base microphone is disabled.

The connected party can only hear speech delivered via the phone's handset microphone.

Group listen is not supported for IP phones or when using a phone's **HEADSET** button.

Currently connected calls are not affected by changes to this setting. If group listen is required it must be selected before the call is connected.

This enables listeners at the user's phone to hear the connected party whilst limiting the connected party to hear only what is communicated via the phone handset.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✓ GroupListenOn

Release: 4.1+.

Example

Below is a sample short code using the Group Listen Off feature.

Short Code: *28

Feature: GroupListenOn

Headset Toggle

Toggles between the use of a headset and the telephone handset.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✓ HdSet

Release: 1.4+.

Example

Below is a sample short code using the Headset Toggle feature. This short code can be used to toggle the feature on/off. If an Avaya supported headset is connected to your telephone, this short code can be used to toggle between using the headset and the telephone handset.

Short Code: *55

Feature: HeadsetToggle

Hold Call

This uses the Q.931 Hold facility, and "holds" the incoming call at the ISDN exchange, freeing up the ISDN B channel. The Hold Call feature "holds" the current call to a slot. The current call is always automatically placed into slot 0 if it has not been placed in a specified slot. Only available if supported by the ISDN exchange.

Details

Telephone Number: ✓ Exchange hold slot number or blank (slot 0).

Default Short Code: ✗

Programmable Button Control: ✓ Hold

See also: Hold CW, Hold Music, Suspend Call.

Release: 1.0+.

Example

Below is a sample short code using the Hold Call feature. This short code is a default within the system configuration. N represents the exchange hold slot number you want to hold the call on. For example, while connected to a call, dialing *24*3# will hold the call onto slot 3 on the ISDN.

Short Code: *24*N#

Telephone Number: N

Feature: HoldCall

Hold CW

This uses the Q.931 Hold facility, and "holds" the incoming call at the ISDN exchange, freeing up the ISDN B channel. The Hold CW feature "holds" the current call to an exchange slot and answers the call waiting. The current call is always automatically placed into slot 0 if it has not been placed in a specified slot. Only available if supported by the ISDN exchange.

Details

Telephone Number: ✓ Exchange slot number or blank (slot 0).

Default Short Code: ✓ *27*N# (A-Law only) (not on Server Edition)

Programmable Button Control: ✓ HoldCW

See also: Hold Call, Suspend Call.

Release: 1.0+.

Example

Below is a sample short code using the Hold CW feature.

Short Code: *27*N#

Feature: HoldCW

Hold Music

This feature allows the user to check the system's music on hold. See Music On Hold for more information.

Details

Telephone Number: Optional. If no number is specified, the default system source is assumed. The system supports up to 4 hold music sources, numbered 1 to 4. 1 represents the System Source. 2 to 4 represent the Alternate Sources.

Default Short Code: ✓

***34N;** where N is the number of the hold music source required.

Programmable Button Control: ✓ Music

Release: 1.0+.

Example

Below is a sample short code using the Hold Music feature. This short code is a default within the configuration.

Short Code: *34N;

Feature: HoldMusic

Hunt Group Disable

This feature disables the user's membership of the specified hunt group. They will no longer receive call to that hunt group until their membership is enabled again. To use this feature, you must already belong to the hunt group. See also Hunt Group Enable.

Details

Telephone Number: ✓ Group number.

Default Short Code: ✗

Programmable Button Control: ✓ HGDis

See also: Hunt Group Enable.

Release: 1.0+.

Example

N represents the hunt group number from which the user wants to be disabled from. For example, if Paul wants to be disabled from the Sales hunt group (extn. 500), he needs to dial *90*500#.

Short Code: *90*N#

Telephone Number: N

Feature: HuntGroupDisable

Hunt Group Enable

This feature enables the user's membership of a hunt group so they can begin to receive calls to the specified hunt group. To use this feature, the user must already belong to the hunt group. This short code can not be used to add someone to a hunt group, that must be done within Manager's Hunt Group form.

Details

Telephone Number: ✓ Group number.

Default Short Code: ✗

Programmable Button Control: ✓ HGEna

See also: Hunt Group Disable.

Release: 1.0+. Previously in Release 3.2 the **Set Hunt Group Night Service**, **Set Hunt Group Out of Service** and **Hunt Group Enable** short code features toggled. That behaviour is not supported in 4.0 and higher.

Example

This short code can be used to turn the feature on. N represents the hunt group number for which the user wants to start receiving calls. For example, if Paul is already a member of the sales hunt group (extn. 500) but has changed his availability status for that hunt group using hunt group disable, he can make himself available for receiving calls to the Sales hunt group again by dialing *91*500#.

Short Code: *91*N#

Telephone Number: N

Feature: HuntGroupEnable

Last Number Redial

This feature allows an extension to redial the last number they dialed.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✗

Release: 3.0+.

MCID Activate

This feature should only be used in agreement with the ISDN service provider and the appropriate local legal authorities. It allows users with **Can Trace Calls** (**User | Telephony | Supervisor Settings**) set to trigger a malicious call trace of their previous call at the ISDN exchange. Refer to Telephone Features Malicious Call Tracing for further details.

Note:

Currently, in Server Edition network, MCID is only supported for users using an MCID button and registered on the same IP500 V2 Expansion system as the MCID trunks.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: Advanced | Miscellaneous | MCID Activate.

Release: 4.0+.

Mobile Twinned Call Pickup

This short code feature allows the user to pickup a call ringing or connected at the destination of their mobile twinning number. This short code can only be used from the primary extension which is being used for the twinning operation.

Note that the use of mobile twinning requires entry of a Mobile Twinning license and may be subject to a time profile.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✗

See also: Set Mobile Twinning Number, Set Mobile Twinning On, Set Mobile Twinning Off.

Release: 3.2+.

Off Hook Station

Enables or disables whether the user's extension acts as a fully handsfree unit. Typically this is used when the answering and clearing of calls is done through an application. For more details see Off Hook Station (User | Telephony | Call Settings).

Details

Telephone Number: ✓ "Y" for on or "N" for off.

Default Short Code: ✗

Programmable Button Control: ✓ OHStn

Release: 1.0+.

Example: Turning the off hook station off

Short Code: *89

Telephone Number: N

Feature: OffHookStation

Example: Turning the off hook station on

Short Code: *98

Telephone Number: Y

Feature: OffHookStation

Outgoing Call Bar Off

Allows a user to switch off their outgoing call bar status. The short code user must enter their log in code, if set, in order to be successful.

If you add a short code using this feature to a system it is recommended that you also assign a login code to the No User user to prevent the short code being used to change the status of that user.

Details

Telephone Number: ✓ The user's log in code.

System phone users can use <target user>*<system phone user's login code>.

Default Short Code: ✗

Programmable Button Control: ✗

Release: 4.1+ (Added to Release 4.1 2008Q2 Maintenance release).

Example

The user has a **Login Code** of **1234**. To use the short code below below, the user must dial ***59*1234#**.

Short Code: *59*N#

Telephone Number: N

Feature: Outgoing Call Bar Off.

Example

A user set as a system phone can also switch off the Outgoing Call Bar status of another user. This is done using their own login code. For example the system phone 401 with login code 1234 can switch off the outgoing call bar status of extension 403 as follows:

***59*403*1234**

Outgoing Call Bar On

Allows a user to switch on their outgoing call bar status.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✗

Release: 4.1+ (Added to Release 4.1 2008Q2 Maintenance release).

Example

To use the short code below below, the user must dial ***58**.

Short Code: *58

Telephone Number: <blank>

Feature: Outgoing Call Bar On.

Private Call Off

Short codes using this feature turn off private call status for the user if set. The short code features Private Call and Private Call On can be used to turn private call on.

When on, any subsequent calls cannot be intruded on until the user's private call status is switched off. The exception is Whisper Page which can be used to talk to a user on a private call.

Note that use of private calls is separate from the user's intrusion settings. If the user's **Cannot be Intruded** (User | Telephony | Supervisor Settings) setting is enabled, switching private calls off does not affect that status. To allow private calls to be used to fully control the user status, **Cannot be Intruded** (User | Telephony | Supervisor Settings) should be disabled for the user.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: Advanced | Call | Private Call.

Release: 4.0+.

Private Call On

Short codes using this feature turn on the private call settings for the user regardless.

When on, any subsequent calls cannot be intruded on until the user's private call status is switched off. The exception is Whisper Page which can be used to talk to a user on a private call.

Note that use of private calls is separate from the user's intrusion settings. If the user's **Cannot be Intruded** (User | Telephony | Supervisor Settings) setting is enabled, switching private calls off does not affect that status. To allow private calls to be used to fully control the user status, **Cannot be Intruded** (User | Telephony | Supervisor Settings) should be disabled for the user.

Private call status can be switched off using a short code with the Private Call Off feature or a programmed button set to the Private Call action. To enable private call status for a single following call only the Private Call short code feature should be used.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: Advanced | Call | Private Call.

Release: 4.0+.

Priority Call

This feature allows the user to call another user even if they are set to 'do not disturb'. Priority calls to a user without DND will follow forwarding and follow me settings but will not go to voicemail.

Details

Telephone Number: ✓ Extension number.

Default Short Code: ✗

Programmable Button Control: ✓ PCall

See also: DialPhysicalExtensionByNumber, DialPhysicalNumberByID.

Release: 1.0+.

Example

N represents the extension number to be called, despite the extension being set to 'do not disturb'. For example, if extension 201 has 'do not disturb' enabled, a user can dial *71*201# and still get through. This short code is useful for companies that frequently use the 'do not disturb' feature and can be given to Managing Directors or people who may need to get through to people regardless of their 'do not disturb' status.

Short Code: *71*N#

Telephone Number: N

Feature: PriorityCall

Record Message

This short code feature is used to record hunt group announcements on Embedded Voicemail, see Hunt Group | Announcements. Release 5.0+: It is also used to record mailbox user name prompts for the auto attendant **Dial by Name** function.

Details

Telephone Number: ✓

For a hunt group queue announcement, use the hunt group extension number followed by **".1"**.

For a hunt group still queue announcement, use the hunt group extension number followed by **".2"**.

For a mailbox user name prompt, use the user extension number followed by **".3"**.

Default Short Code: ✓ *91N; and *92N; (not on Server Edition)

Programmable Button Control: ✗

Release: 4.0+.

Example

For a hunt group with extension number 300, the default short codes ***91N;/Record Message/N".1"** and ***92N;/Record Message/N".2"** can be used to allow recording of the announcements by dialing ***91300#** and ***92300#**.

To allow users to record their own name prompt, the short code ***89#/Record Message/E."3"** can be used. The **E** is replace by the extension number of the dialing user.

Relay On

This feature closes the specified switch in the system's external output (EXT O/P) port.

This feature is not supported on Linux based systems. For Server Edition, this option is only supported on Expansion System (V2) units.

Details

Telephone Number: ✓ Switch number (1 or 2).

Default Short Code: ✓ *39 (Switch 1), *42 (Switch 2), *9000*.

Programmable Button Control: ✓ Rely+

See also: Relay Off, Relay Pulse.

Release: 1.0+.

Example

This short code is a default within the system configuration. This short code is useful for companies that have external devices, such as door controls, connected to the system. Based on this sample short code, a user dialing *42 is closing switch number 2 to activate an external device.

Short Code: *42

Telephone Number: 2

Feature: RelayOn

Analog Modem Control

On systems with an analog trunk card in the control unit, the first analog trunk can be set to answer V.32 modem calls. This is done by either selecting the Modem Enabled option on the analog line settings or using the default short code *9000* to toggle this service on or off. This short code uses the **RelayOn** feature with the Telephone Number set to "MAINTENANCE". Note that the short code method is always returned to off following a reboot or if used for accessing the system date and time menu.

IP500 ATM4 Uni Trunk Card Modem Support It is not required to switch the card's modem port on/off. The trunk card's V32 modem function can be accessed simply by routing a modem call to the RAS service's extension number. The modem call does not have to use the first analog trunk, instead the port remains available for voice calls.

Relay Off

This feature opens the specified switch in the system's external output (EXT O/P) port.

Details

Telephone Number: ✓ Switch number (1 or 2).

Default Short Code: ✓ *40 (Switch 1), *43 (Switch 2)

Programmable Button Control: ✓ Rely-

See also: Relay On, Relay Pulse.

Release: 1.0+.

Example

This short code is a default within the system configuration. This short code is useful for companies that have external devices, such as door controls, connected to the system. Based on this sample short code, a user dialing *43 is opening switch number 2 to activate an external device.

Short Code: *43

Telephone Number: 2

Feature: RelayOff

Relay Pulse

This feature closes the specified switch in the system's external output (EXT O/P) port for 5 seconds and then opens the switch.

Details

Telephone Number: ✓ Switch number (1 or 2).

Default Short Code: ✓ *41 (Switch 1), *44 (Switch 2)

Programmable Button Control: ✓ Relay

See also: Relay On, Relay Off.

Release: 1.0+.

Example

This short code is a default within the system configuration. This short code is useful for companies that have external devices, such as door controls, connected to the system. Based on this sample short code, a user dialing *44 is opening switch number 2 to activate an external device.

Short Code: *44

Telephone Number: 2

Feature: RelayPulse

Resume Call

Resume a call previously suspended to the specified ISDN exchange slot. The suspended call may be resumed from another phone/ISDN Control Unit on the same line.

Details

Telephone Number: ✓ Exchange suspend slot number.

Default Short Code: ✓ *23*N# (A-Law only) (not on Server Edition)

Programmable Button Control: ✓ Resum

See also: Suspend Call.

Release: 1.0+.

Example

Below is sample short code using the Resume Call feature. N represents the exchange slot number from which the call has been suspended. For example, if a user has suspended a call on slot number 4, this user can resume that call by dialing *23*4#.

Short Code: *23*N#

Telephone Number: N

Feature: ResumeCall

Retrieve Call

Retrieves a call previously held to a specific ISDN exchange slot.

Details

Telephone Number: ✓ Exchange hold slot number.

Default Short Code: ✓ *25*N# (A-Law only) (not on Server Edition)

Programmable Button Control: ✓ Retriv

See also: Hold Call.

Release: 1.0+.

Example

Below is sample short code using the Retrieve Call feature. N represents the exchange slot number from which the call has been placed on hold. For example, if a user has placed a call hold on slot number 4, the user can resume that call by dialing *25*4#.

Short Code: *25*N#

Telephone Number: N

Feature: RetrieveCall

Ring Back When Free

This feature sets a ringback on the specified extension. This sets a 'ringback when free' on an extension currently on a call or a 'ringback when next used' for an extension that is free but does not answer.

When the target extension is next used or ends its current call, the users is rung and when they answer a call is made to the target extension.

Details

Telephone Number: ✓ Target extension number.

Default Short Code: ✗

Programmable Button Control: ✓ RBak+

See also: Cancel Ring Back When Free.

Release: 1.0+.

Example

N represents the target extension from which you want to receive the callback. For example, if you call extension 201 but the line is busy, hang up and then dial *71*201#. When extension 201 disconnects from its current call, your phone will ring. Once you pick up the phone, extension 201's line will start ringing to indicate an incoming call.

Short Code: *71*N#

Telephone Number: N

Feature: RingBackWhenFree

Secondary Dial Tone

Secondary dial tone is a system feature to generate a secondary dial tone after the user has begun dialing an external number. This dial tone is then played until the number dialing and an external trunk seized.

Pre-Release 4.0: Secondary dial tone is triggered through the use of the secondary dial tone short code feature.

Release 4.0+: The use of this short code feature has been replaced by the Secondary Dial Tone check box option on ARS forms.

Details

Telephone Number: ✓ Digit which triggers secondary dial tone.

Default Short Code: ✓ 9 (U-Law only)

Programmable Button Control: ✗

Release: 1.0+.

Example

For pre-4.0 systems secondary dial tone works in two parts. The following system short code will trigger secondary dial tone. To use it to trigger secondary dial tone and then continue dialing, other user, user rights and system short codes should begin with [9].

Short Code: 9

Telephone Number: .

Feature: Secondary Dial Tone

Set Absent Text

This feature can be used to select the user's current absence text. This text is then displayed to internal callers who have suitable display phones or applications. It doesn't changes the users status. The absence text message is limited to 128 characters. Note however that the amount displayed will depend on the caller's device or application.

The text is displayed to callers even if the user has forwarded their calls or is using follow me. Absence text is supported across a multi-site network.

Details

Telephone Number: ✓ The telephone number should take the format **"y,n,text"** where:

- **y** = 0 or 1 to turn this feature on or off.
- **n** = the number of the absent statement to use, see the list below:

0 = None.	4 = Meeting until.	8 = With cust. til.
1 = On vacation until.	5 = Please call.	9 = Back soon.
2 = Will be back.	6 = Don't disturb until.	10 = Back tomorrow.
3 = At lunch until.	7 = With visitors until.	11 = Custom.

text = any text to follow the absent statement.

Default Short Code: ✗

Programmable Button Control: ✓ Absnt

Release: 1.0+.

Example

The following short code can be used to turn an absent text message on:

- **Short Code**: *88
- **Telephone Number**: "1,5,me on 208"
- **Line Group ID**: 0
- **Feature**: SetAbsentText

Example

The following short code could be used to turn this facility off. In the Telephone Number the first 0 is used to turn this facility off and the second 0 is used to select the absent statement "None".

Short Code: *89

Telephone Number: "0,0"

Line Group ID: 0

Feature: SetAbsentText

Set Account Code

This short code feature is used to allow system users to enter a valid account code prior to making a phone call. Once this short code is set up, any existing account code in the system configuration can be used in conjunction with it.

This short code feature is essential for allowing analog phone users to enter account codes as they cannot enter account code through the phone during a call or after dial a number.

Details

Telephone Number: ✓ A valid account code.

Default Short Code: ✗

Programmable Button Control: ✓ Acct.

Release: 2.1+.

Example

In this example, N represents any valid account code. For the purpose of this example, we will imagine the account code to be 1234. Once this short code is created, a user can dial 11*1234# to get a dial tone for dialing the restricted telephone number or the phone number needing to be tracked for billing purposes.

Short code: 11*N#

Telephone Number: N

Feature: SetAccountCode

Set Authorization Code

This short code feature is only available on systems configured to use authorization codes. See Authorization Codes. The feature is used to allow a user to enter a valid authorization code prior to making a phone call.

This short code feature is essential for allowing analog phone users to enter authorization codes. Note that the authorization code must be associated with the user or the user rights to which the user belongs.

Details

Telephone Number: ✓ A valid authorization code.

Default Short Code: ✗

Programmable Button Control: ✗

Release: 3.2+.

Set Fallback Twinning Off

This feature can be used by users to disable fallback twinning operation. This feature requires the user to have a mobile twinning number set.

Fallback twinning redirects calls to the user's configured mobile twinning number when the system cannot detect a connection to the user's normal registered extension. This feature can be used without mobile twinning itself being enabled.

Details

- **Telephone Number:** ✗
- **Default Short Code:** ✗
- **Programmable Button Control:** ✗

Set Fallback Twinning On

This feature can be used by users to enable fallback twinning operation. This feature requires the user to have a mobile twinning number set.

Fallback twinning redirects calls to the user's configured mobile twinning number when the system cannot detect a connection to the user's normal registered extension. This feature can be used without mobile twinning itself being enabled.

Details

- **Telephone Number:** ✗

- **Default Short Code:** ✗
- **Programmable Button Control:** ✗

Set Hunt Group Night Service

This feature puts the specified hunt group into Night Service mode.

Setting and clearing hunt group night service can be done using either manual controls or using a system time profile. The use of both methods to control the night service status of a particular hunt group is not supported.

This function is not supported between systems in a multi-site network. It can only be used by a user currently logged onto the same system as hosting the hunt group.

Details

Telephone Number: ✓ Hunt group extension number. If left blank, the short code will affect all hunt groups of which the user is a member.

The **Set Hunt Group Night Service** and **Clear Hunt Group Night Service** short code and button features can be used to switch an SSL VPN service off or on respectively. The service is indicated by setting the service name as the telephone number or action data. Do not use quotation marks.

Default Short Code: ✓ *20*N#

Programmable Button Control: ✓ HGNS+

See also: Set Hunt Group Out Of Service, Clear Hunt Group Night Service, Clear Hunt Group Out Of Service.

Release: 1.0+.

Example

This short code is a default within the system configuration. N represents the telephone number of the hunt group to be placed into "Night Service" mode. For example, when *20*201# is dialed, the hunt group associated with extension 201 will be placed into "Night Service" mode.

Short Code: *20*N#

Telephone Number: N

Feature: SetHuntGroupNightService

Set Hunt Group Out Of Service

This feature manually puts the specified hunt group into Out of Service mode. If a time profile has also been defined to control hunt group night service, the action may vary:

Set Hunt Group Out of Service can be used to override a time profile and change a hunt group from night service to out of service.

Details

Telephone Number: ✓ Hunt group extension number. For Release 4.0+, if left blank, the short code will affect all hunt groups of which the user is a member.

Default Short Code: ✗

Programmable Button Control: ✓ HGOS+

Release: 1.0+.

Example

Below is a sample short code using the **Set Hunt Group Out Of Service** feature. N represents the telephone number of the hunt group to be placed into "Out of Service" mode. For example, when *56*201# is dialed, the hunt group associated with extension 201 will be placed into "Out of Service" mode.

Short Code: *56*N#

Telephone Number: N

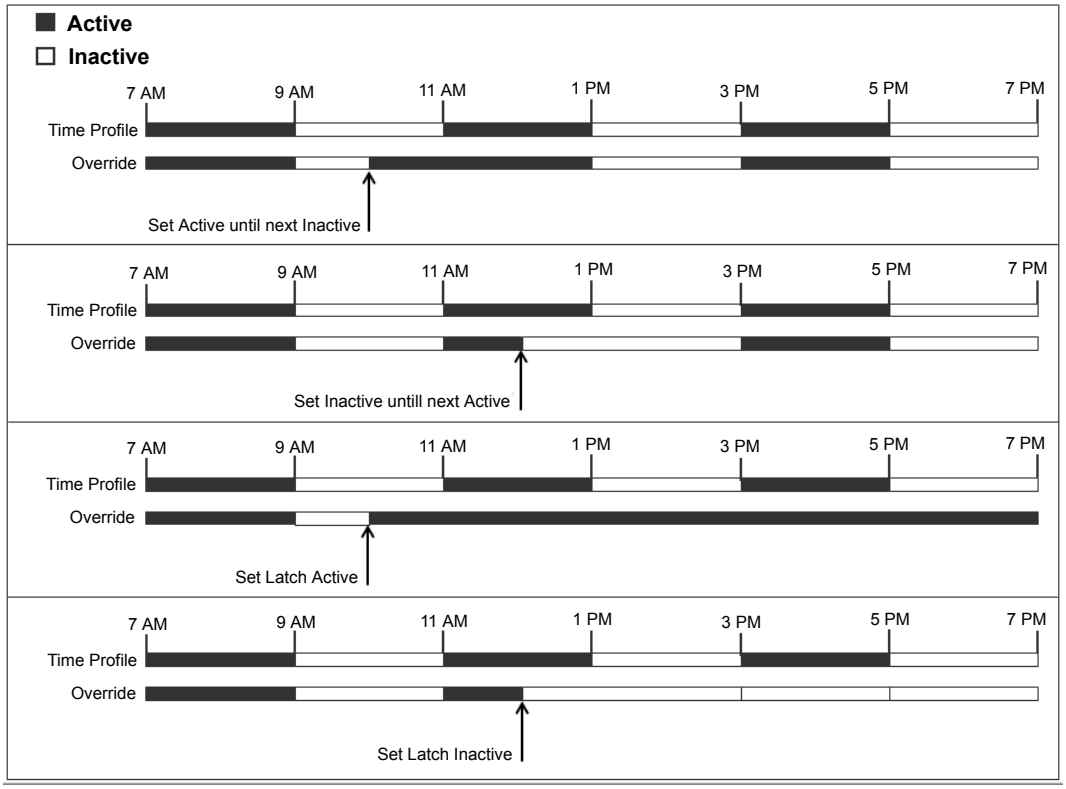
Feature: SetHuntGroupOutOfService

Set Time Profile

You can manually override a time profile. The override settings allow you to mix timed and manual settings.

Five short codes can be configured.

Short Code Name	Description
Set Time Profile Timed Operation	No override. The time profile operates as configured.
Set Time Profile Active Until Next Timed Inactive	Use for time profiles with multiple intervals. Select to make the current timed interval active until the next inactive interval.
Set Time Profile Inactive Until Next Timed Active	Use for time profiles with multiple intervals. Select to make the current active timed interval inactive until the next active interval.
Set Time Profile Latch Active	Set the time profile to active. Timed inactive periods are overridden and remain active.
Set Time Profile Latch Inactive	Set the time profile to inactive. Timed active periods are overridden and remain active.



Telephone Number: Time profile name.

Default Short Code: No.

Programmable Button Control: Yes: Time Profile

Speed Dial

Each system directory and personal directory number stored in the configuration can be optionally assigned an index number. That index number can then be used by M-Series and T-Series phone users to dial the directory number. This short code feature allows the creation of short codes to perform the same function. However, the short code is diallable from any type of telephone extension on the system.

For example:

- If **Feature 0** is followed by a 3-digit index number in the range 000 to 999, the system directory record with the matching index number is dialed.

- If **Feature 0** is followed by * and a 2-digit index number in the range 00 to 99, the personal directory record with the matching index number is dialed. Alternatively Feature 0 can be followed by 00# to 99#. Note: Release 10.0 allows users to have up to 250 personal directory entries. However, only 100 of those can be assigned index numbers.

Details

Telephone Number: ✓ System directory entry index number (000 to 999) or personal directory entry index number (00 to 99).

Default Short Code: ✗

Programmable Button Control: ✗

Release: 8.1.

Example

Using the example below, a user is able to dial *0 and then either a 2 digit code for an indexed personal directory entry or a 3 digit code for an indexed system directory entry.

Short Code: *0N#

Telephone Number: N

Feature: Speed Dial

Shutdown Embedded Voicemail

Allows the Embedded Voicemail service provided by an Avaya memory card in a control unit to be shut down. To restart the service, a **Startup Embedded Voicemail** short code should be used.

The short code has the following effects:

1. Immediately disconnect all current users within Embedded Voicemail. This is not a polite shutdown.
2. Mark the Embedded Voicemail as inactive so that it will not receive any new calls.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✗

Release: 4.0+ (Added in the Release 4.0 Q2 2007 maintenance release).

Stamp Log

The stamp log function is used to insert a line into any System Monitor trace that is running. The line in the trace indicates the date, time, user name and extension plus additional information. The line is prefixed with **LSTMP: Log Stamped** and a log stamp number. When invoked from a Avaya phone with a display, **Log Stamped#** is also briefly displayed on the phone. This allows users to indicate when they have experienced a particular problem that the system maintainer want them to report and allows the maintainer to more easily locate the relevant section in the monitor trace.

The log stamp number is set to 000 when the system is restarted. The number is then incremented after each time the function is used in a cycle between 000 and 999. Alternately if required, a specific stamp number can be assigned to the button or short code being used for the feature.

Details

Telephone Number: Optional. If not set, a number in the sequence 000 to 999 is automatically used. If set, the number set is used.

Default Short Code: ✓ *55

Programmable Button Control: ✓ Stamp Log

Release: 8.1+

Startup Embedded Voicemail

Restarts the Embedded Voicemail service provided by an Avaya Memory in a control unit.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✗

Release: 6.0+

Suspend Call

This feature uses the Q.931 Suspend facility. It suspends the incoming call at the ISDN exchange, freeing up the ISDN B channel. The call is placed in exchange slot 0 if a slot number is not specified.

Details

Telephone Number: ✓ Exchange slot number or blank (slot 0).

Default Short Code: ✗

Programmable Button Control: ✓ Suspe

See also: Resume Call.

Release: 1.0+.

Suspend CW

This feature uses the Q.931 Suspend facility. Suspends the incoming call at the ISDN exchange and answer the call waiting. The call is placed in exchange slot 0 if a slot number is not specified. Only available when supported by the ISDN exchange.

Details

Telephone Number: ✓ Exchange slot number or blank (slot 0).

Default Short Code: ✓ *28*N# (A-Law only) (not on Server Edition)

Programmable Button Control: ✓ SusCW

See also: Resume Call.

Release: 1.0+.

Example

Sample short code using the Suspend CW feature.

Short Code: *28*N#

Feature: Suspend CW

Start After Call Work

This feature can be used by users who have been configured as CCR agents. It allows them to dial a short code to enter the After Call Work (ACW) state as reported by the Customer Call Reporter (CCR) application.

Note:

CCR is not supported in IP Office release 9.1 and later.

Details

Telephone Number: ✗

Default Short Code: ✗

Programmable Button Control: ✓ ACWrk

See also: Clear After Call Work.

Release: 4.2 4Q 2008 Maintenance release+.

Toggle Calls

This feature cycles through each call that the user has on hold on the system. This feature is useful when a user with a single-line telephone has several calls on hold and needs to respond to each one in turn.

Details

Telephone Number: ✗

Default Short Code: ✓ *29

Programmable Button Control: ✓ Toggl

Release: 1.0+.

Example

Below is sample short code using the Toggle Calls feature.

Short Code: *29

Feature: ToggleCalls

Unpark Call

Retrieve a parked call from a specified system park slot.

Details

Telephone Number: ✓ System park slot number.

Default Short Code: ✓ *38*N#

Programmable Button Control: ✓ Ride

See also: Call Park.

Release: 1.0+.

Example

Below is a sample short code using the Unpark Call feature. N represents the park slot number in which the call you want to retrieve was parked. For example, if a user parked a call to slot number 9, you can retrieve that call by dialing *38*9#.

Short Code: *38*N#

Telephone Number: N

Feature: Unpark Call

Voicemail Collect

This feature connects to the voicemail system. Normally the telephone number field is used to indicate the name of the mailbox to be accessed, for example "?Extn201" or "#Extn201".

? indicates 'collect messages'.

# indicates 'leave a message'. It also instructs the voicemail server to give a brief period of ringing before connecting the caller. This is useful if the short code is used for functions like call transfers as otherwise the voicemail server can start playing prompts before the transfer is completed. However, the # can be omitted for immediate connection if required.

" " quotation marks must be used to enclose any information that needs to be sent to the voicemail server as is. Any text not enclosed by quote marks is checked by the telephone system for short code character matches which will be replaced before being sent to the voicemail server.

Manager will automatically add quotation marks to the Telephone Number field if there are no manually added quotation marks. Care should be taken to ensure that special characters that you want replaced by the telephone system, such as **U**, **N** or **X**, are not enclosed by the quotation marks. For scenarios where the telephone number only contains short code characters, an empty pair of quotation marks, for example **""N**.

When using Voicemail Pro, names of specific call flow start points can directly access those start points via a short code. In these cases, ? is not used and # is only used if ringing is required before the start point's call flow begins.

Short codes using the Voicemail Collect feature, with either "Short Codes.name" and "#Short Codes.name" records in the Telephone Number field are automatically converted to the Voicemail Node feature and name.

Note:

CallPilot voicemail is used for IP Office Branch deployments with CS 1000.

Users can access their CallPilot voicemail by dialing the Voicemail Collect short code. Access to CallPilot voicemail from Auto Attendant cannot be enabled by setting a Normal Transfer action to point to the Voicemail Collect short code. If desired, it can be enabled by setting a Normal Transfer action to point to the CallPilot number.

Details

Telephone Number: ✓ See the notes above.

Default Short Code: ✓ *17

Programmable Button Control: ✓ VMCol

See also: Voicemail On, Voicemail Off, Voicemail Node.

Release: 1.0+.

Example: Retrieve Messages from Specific Mailbox

This short code allows a user to retrieve messages from the mailbox of the hunt group 'Sales'. This usage is not supported on Voicemail Pro running in Intuity emulation mode unless a custom call flow has been created for the hunt group, refer to the Voicemail Pro help.

Short Code: *89

Telephone Number: "?Sales"

Feature: VoicemailCollect

Example: Record Message to Specific Mailbox

To allow users to deposit a message directly to Extn201's Voicemail box. This short code is useful when you know the person is not at her/his desk and you want to immediately leave a message rather than call the person and wait to be redirected to voicemail.

Short Code: *201

Telephone Number: "#Extn201"

Feature: VoicemailCollect

Example: Accessing a Specific Voicemail Pro Module

This short code can be used in instances where you have a conference bridge set up on the system and a module has been created via Voicemail Pro to access this conference bridge. A short code can be created for internal access to the module. In the sample short code below, the telephone number field contains the name of the module. In this example, if a short burst of ringing is required before connecting the module, "#conferenc" would be used as the telephone number.

Short Code: *100

Telephone Number: "conferenc"

Feature: VoicemailCollect

Example: Record Voicemail Pro Messages for Outbound Contact Express

Short Code: *99

Telephone Number: "edit_messages"

Feature: VoicemailCollect

This short code allows users to record Voicemail Pro messages used by the Outbound Contact Express solution. For example:

- Queuing messages.
- A message intended for an answering machine.
- Messages an agent can play for a customer.
- On hold messages. (Always specify message number “0” for the hold treatment message.)
- Messages played by a Virtual Agent.

Recorded message files are stored in the folder /opt/vmpro/Wavs/Modules/CPAPrompts.

When invoked, the user is prompted to enter a number to associate with the message. The Outbound Contact Express Proactive Contact component ships with the following default English messages:

- 0: Hold message
- 1: First outbound queue message – Female
- 2: Second outbound queue message - Female
- 3: Third outbound queue message - Female
- 4: Fourth outbound queue message – Female
- 9: First outbound queue message – Male
- 10: Second outbound queue message - Male
- 11: Third outbound queue message - Male
- 12: Fourth outbound queue message - Male
- 17: Message to play to an answering machine or message to play by a virtual agent - Female
- 18: Message to play to an answering machine or message to play by a virtual agent – Male
- 19: Message played when default F6 agent key is pressed (Release the Line, completion Code 20)

Voicemail Node

Similar to Voicemail Collect but used for calls being directed to a Voicemail Pro Short Codes start point. Useful if you have set up a short code start point with Voicemail Pro and want to give direct internal access to it.

Details

Telephone Number: ✓ Voicemail Pro Short Code start point name without quotation marks.

Default Short Code: ✗

Programmable Button Control: ✗

See also: Voicemail Collect.

Release: 2.0+.

Example

Having created a short codes start point call flow called Sales, the following system short code can be used to route calls to that call flow:

- **Short Code:** *96
- **Telephone Number:** Sales
- **Feature**: VoicemailNode

Voicemail On

This feature enables the user's voicemail mailbox to answer calls which ring unanswered or arrive when the user is busy.

Details

Telephone Number: ✗ None.

Default Short Code: ✓ *18

Programmable Button Control: ✓ VMOn

See also: Voicemail Off.

Release: 1.0+.

Example

This short code can be used to toggle the feature on.

Short Code: *18

Feature: VoicemailOn

Voicemail Off

This feature disables the user's voicemail mailbox box from being used to answer calls. It does not disable the voicemail mailbox being used as the target for other functions such as call recording or messages forwarded from other mailboxes.

Details

Telephone Number: ✗ None.

Default Short Code: ✓ *19

Programmable Button Control: ✓ VMOff

See also: Voicemail On.

Release: 1.0+.

Example

Below is a sample of the short code setup.

Short Code: *19

Feature: VoicemailOff

Voicemail Ringback On

This feature enables voicemail ringback to the user's extension. Voicemail ringback is used to call the user when they have new voicemail messages. The ringback takes place each time the extension is used. This feature is useful for users who do not have voicemail light/button indicators on their telephone.

If the user has been configured to receive message waiting indication for any hunt groups, a separate voicemail ringback will occur for each such group and for the users own mailbox.

Details

Telephone Number: ✗

Default Short Code: ✓ *48

Programmable Button Control: ✓ VMRB+

See also: Voicemail Ringback Off.

Release: 1.0+. For Release 3.2, the Voicemail On and Voicemail Ringback On short code features toggled. For Release 4.0 and higher, they no longer toggle.

Example

This short code can be used to turn the feature on.

Short Code: *48

Feature: VoicemailRingbackOn

Voicemail Ringback Off

This feature disables voicemail ringback to the user's extension.

Details

Telephone Number: ✗

Default Short Code: ✓ *49

Programmable Button Control: ✓ VMRB-

See also: Voicemail Ringback On.

Release: 1.0+.

Example

Below is a sample of the short code setup.

Short Code: *49

Feature: VoicemailRingbackOff

Whisper Page

This feature allows you to intrude on another user and be heard by them without being able to hear the user's existing call which is not interrupted. For example: User A is on a call with user B. When user C intrudes on user A, they can be heard by user A but not by user B who can still hear user A. Whisper page can be used to talk to a user who has enabled private call.

The ability to intrude and be intruded is controlled by two configuration settings, the Can Intrude (User | Telephony | Supervisor Settings) setting of the user intruding and the Cannot Be Intruded (User | Telephony | Supervisor Settings) setting of target being intruded on. The setting of any other internal party is ignored. By default, no users can intrude and all users are set to cannot be intruded.

The system support a range of other call intrusion methods in addition to this feature.

Details

Telephone Number: ✓ Target extension number.

Default Short Code: ✗

Programmable Button Control: ✓ Whisp.

See also: Call Intrude, Call Listen, Coaching Intrusion, Dial Inclusion.

Release: 8.0+.

Chapter 16: Button Programming Overview

This section provides an overview of system actions that can be assigned to programmable buttons on Avaya phones.

Button assignment can be done through the system configuration using Manager and for some functions using the phone itself. Using Manager, if only button programming changes are required, the configuration changes can be merged back to the system without requiring a reboot.

Appearance Functions The functions **Call Appearance**, **Bridged Appearance**, **Coverage** and **Line Appearance** are collectively known as "appearance functions". For full details of their operation and usage refer to the Appearance Button Operation section. The following restrictions must be observed for the correct operation of phones.

Phone Support Note that not all functions are supported on all phones with programmable buttons. Where possible exceptions, have been indicated. Those buttons will typically play an error tone when used on that phone. Programming of those features however is not restricted as users may hot desk between different types of phones, including some where the feature is supported.

Actions that use status feedback are only supported on buttons that provide that feedback through lamps or icons.

Related links

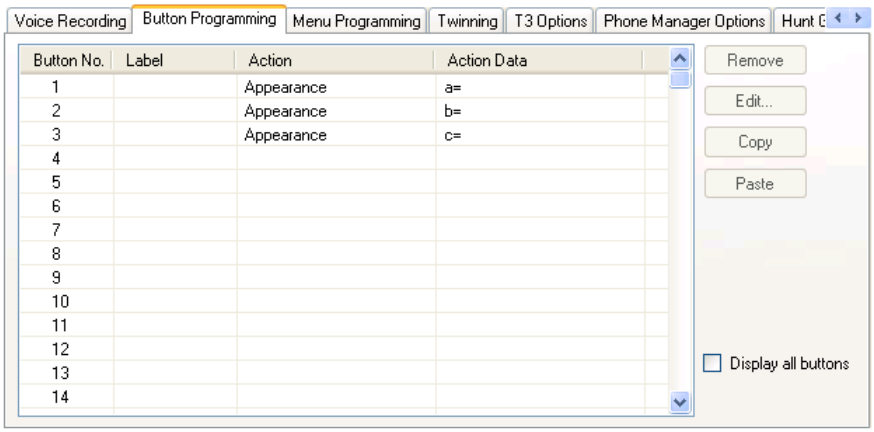
Programming Buttons with Manager on page 789
Programming Button via the Menu Key on page 791
Programming Button via an Admin Button on page 793
BST Button Programming on page 795
T3 Self-Administration on page 797
Interactive Button Menus on page 799
Label Templates on page 799

Programming Buttons with Manager

About this task

Procedure

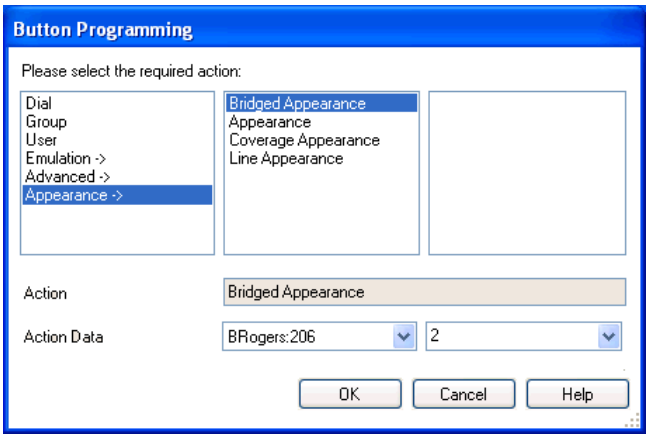
1. Select the  **User** required to display their configuration details.
2. Select **Button Programming**.



The number of button displayed is based on the phone associated with the user when the configuration was loaded. This can be overridden by selecting **Display All Buttons**. This may be necessary for users who switch between different phones using hot desking or have an expansion unit attached to their phone.

3. For the required button, either select the button and then click **Edit**or double-click the button.
4. Edit the settings as required.

   Use the **...** button to display the menu for selecting the required button action. Select the action and set the action data, then click **OK**.



5. Click **OK**.

   Repeat for any other buttons.
6. Click **OK**.

Result

An alternate method for the above programming is to right-click on the various fields. To do this start with the **Action** field, then **Action Data** and then **Label** if required.

Related links

Button Programming Overview on page 789

Programming Button via the Menu Key

On 4412D+, 4424D+, 4612IP, 4624IP, 6408D, 6416D, 6424D phones the **Menu** button can be used to program some functions against other buttons. This programming also includes programmable buttons on any associated add-on units associated with the phone. Buttons already programmed as appearance buttons cannot be altered using these methods.

A Self-Administer button can also be added to allow the phone user to program the functions on their other buttons, see Self-Administer.

T3 phone users can also program buttons using a Menu function, see T3 Self-Administration.

Related links

Button Programming Overview on page 789

Setting a Button to Dial a Number

About this task

This process sets the selected programmable button to the Dial function in the system configuration.

Procedure

1. With the phone idle and on-hook, press MENU.
2. Press ▸ and select **PROG**.
3. Enter the number required.

   The left-most display button can be used to backspace and the right-most display button can be used to **Clear** the whole number.
4. Press the programmable button against which the number should be set.
5. If the button is already programmed, options to replace (**Repla**), keep (**Keep**) or delete (**Delet**) the buttons existing programming appear.

   Select the option required.
6. The message **BUTTON PROGRAMMED!** indicates that the button is now programmed.

   Select **Cont** and then press Exit.

Setting a Button to a Switch Function

About this task

This process allows users to program there own Group, User, and Park slot monitor buttons. It also allows the programming of Dial and Flash Hook buttons.

Procedure

1. With the phone idle and on-hook, press Menu twice.
2. Press ▶ and select **ProgA**.
3. Press ▶ and select **DSS**.
4. Use the ◀ and ▶ buttons to display the function required. Press the display button below the function to select it.
5. If the function requires a telephone number value set, enter the number.

   The left-most display button can be used to backspace and the right-most display button can be used to **Clear** the whole number.
6. Press the programmable button against which the number should be set.
7. If the button is already programmed, options to replace (**Repla**), keep (**Keep**) or delete (**Delet**) the buttons existing programming appear.

   Select the option required.
8. The message **BUTTON PROGRAMMED!** indicates that the button is now programmed.

   Select **Cont** and then press Exit.

Setting Buttons to Admin Function

About this task

Phones with a **Menu** key can program a range of self-administer functions onto their programmable buttons. These are:

Dir - Directory.

Drop - Drop.

HFAns - Internal Auto-Answer.

Timer - Timer.

AutCB - Automatic Callback.

Prog - Abbreviated Dial Program.

CFrwd - Call Forwarding All.

CPark - Call Park.

SAC - Send All Calls.

TmDay - Time of Day.

Admin - Self-Administer.

Acct - Account Code Entry.

AD - Abbreviated Dial.

Call Park

GrpPg - Group Paging.

CPkUp - Call Pickup.

DPkUp - Directed Call Pickup.

RngOf - Ringer Off.

Spres - AD Suppress.

HdSet - Headset Toggle.

HGNS+ - Set Hunt Group Night Service.

This is the same set of functions that can be programmed by users with a button set to Self-Administer (see Self-Administer).

Procedure

1. With the phone idle and on-hook, press Menu.
2. Press ▶ twice and select **Admin**.
3. Use the ◀ and ▶ keys to display the function required and then select it by pressing the display button below the feature.

   Selecting **Expl?** changes the display from short name mode to long name mode. In this mode the full names of the features are displayed. Select **SHORTMODE** to return to that mode.
4. If the function requires a telephone number value set, enter the number.

   The left-most display button can be used to backspace and the right-most display button can be used to **Clear** the whole number.
5. Press the programmable button against which the number should be set.
6. If the button is already programmed, options to replace (**Repla**), keep (**Keep**) or delete (**Delet**) the buttons existing programming appear.

   Select the option required.
7. The message **BUTTON PROGRAMMED!** indicates that the button is now programmed.

   Select **Cont** and then press Exit.

Programming Button via an Admin Button

The Admin (also called Self-Administer) function can be assigned to a programmable button on a user's phone. That button then allows the user to program functions against other programmable buttons on their phone, except those already set as appearance buttons.

Admin buttons are only supported on **2410**, **2420**, **4406D+**, **4412D+**, **4424D+**, **4606IP**, **4612IP**, **4624IP**, **5410**, **5420**, **6408D**, **6416D** and **6424D**.

On **4412D+, 4424D+, 4612IP, 4624IP, 6408D, 6416D, 6424D** phones:

- **Admin** can be permanently accessed via **Menu**, ▸, ▸, **Admin**.
- **Admin1** can be permanently accessed via **Menu**, **Menu**, ▸, **ProgA**, , ▸, **DSS**.

Related links

Button Programming Overview on page 789

Using an Admin Button

About this task

Procedure

1. With the phone idle and on-hook, press the button programmed to **Admin** or **Admin1**.

   The list of available functions is shown.

2. Use the ◂ and ▸ buttons to move through the list.

   Selecting **Expl?** changes the display from short name mode to long name mode. In this mode the full names of the features are displayed. Select **SHORTMODE** to return to that mode.

3. Select the function required.

4. If the function requires a telephone number value set, enter the number.

   The left-most display button can be used to backspace and the right-most display button can be used to Clear the whole number.

5. Press the programmable button against which the number should be set.

   On phones with multiple pages of buttons use the ◂ and ▸ button to select the required page before pressing the button to program.

6. If the button is already programmed, options to replace, keep or delete the button's existing programming appear.

   Select the option required.

7. The message **BUTTON PROGRAMMED!** indicates that the button is now programmed.

8. Select **Cont**. and then press `Exit`or lift the handset to go off-hook.

BST Button Programming

About this task

The process below can be used to assign functions to programmable buttons on T-Series and M-Series phones. Existing button can be overwritten except buttons set to appearance functions.

Procedure

1. Press `Feature *3`.

   If a security code is requested, enter your phone login code and press #.

2. Use one of the processes below.

   Press * to switch between processes (or **More** if displayed). On T7000 phones, only the first process is supported.

3. Select Button and then Function
   a. Press the button to program.
   b. Enter the feature code of the function required (the only * function supported is *7 for contrast).
   c. If the button has an existing function it is displayed and the option to replace the button or return to function selection.

4. Select Function and then Button.

   Enter the number for the feature required or use the volume buttons to move through the list of functions.

   01. Speed dial
   02. Ring Again
   03. Conference
   04. Call Forward All
   05. Last Number Redial
   06. Page Group
   07. Voicemail
   08. Automatic Intercom
   09. Priority Call
   10. Transfer
   11. Call Park
   12. Group Pickup
   13. Direct Pickup
   14. Timer

15. Do Not Disturb On
16. Contrast
17. Group Listen On
18. Time of Day
17. Call Log
18. Self-Administer
19. Account Code
20. Forward on Busy
21. Forward on No Answer
22. Pickup
23. Directory
24. Flash Hook
25. Internal Auto Answer
26. Set Hunt Group Night Service
27. Twinning
28. Ringer Off

    a. Press `Hold`to select a currently displayed function.

    b. Press the button to which the function should be assigned.

    c. If the button has an existing function it is displayed and the option to replace the button or return to function selection.

5. When **Default Buttons** is displayed, press `Hold`(or the **Prog** softkey if displayed).

   The phone buttons are defaulted to those appropriate to the phone type. Note that only buttons that have a default function on the phone type are defaulted. It does not affect the functions assigned to any buttons that do not have default functions.

   Default Buttons

   For T-Series and M-Series phones, default button functions are assigned to buttons when a phone is first connected to the extension port. The functions assigned depend on the particular phone model.

   The default functions for the phone model are also assigned when **Feature *3** is used to default the phone's buttons. Buttons without a default function are not overwritten when the buttons are defaulted.

Related links

Button Programming Overview on page 789

T3 Self-Administration

Note:

IP Office R11 does not support T3 and T3 IP Phones.

Release 4.2+ supports functions for T3 phone users to be able to program their own buttons. This is similar to the existing Self-Administer button supported on other phones but is configured and accessed via different methods.

The user accesses button programming through **Menu | Settings | Button programming**. This function is not available by default, instead it must be configured as available for the user using the method detailed below.

Once enabled, the user is able to configure the following functions on buttons:

Function	Description
empty	Returns the button to it normal default function.
Account Code	Allows the user to enter an account code before or during a call. The account code can be preset or entered after the button press. See the Account Code Entry function.
Callback	Set a callback from the currently dialed extension number. See the Automatic Callback function.
Call list	Displays a list of calls received. See the Call List function.
Call Tracing	Activate malicious call tracing. See the MCID Activate function and Malicious Call Tracing (MCID).
Dial	Dial a preset number or partial number that can be completed after the button press. See the Dial function.
Dial Intercom	Make a page call to the selected target if it supports handsfree answer. See Dial Intercom.
Directory	Display the system directory. See the Directory function.
Do not disturb	Toggle the phone between do not distrub on and off. See the Send All Calls function.
Follow me here	Activate/cancel follow me here. See the Follow Me Here function.
Forward unconditional	Activate/cancel forward all calls. See the Forward Unconditional On function.
Group Paging	Page a group of phones. See the Group Paging function.
Group Membership	Enable/disable the user membership of a group or all groups. See the Hunt Group Enable function.

Table continues…

Group State	Change a hunt group's out of service status. See the Set Hunt Group Out of Service function.
Headset	Switch between handset and headset modes. See the Headset Toggle function.
Internal Auto-Answer	Auto connect internal calls after a single tone. See the Internal Auto-answer function.
Login	Access the menu for phone log in. See the Extn Login function.
Logout	Log out from the phone. See the Extn Logout function.
Night Service	Change a hunt group's night service status. See the Set Hunt Group Night Service function.
Paging	Page an extension or group. See the Dial Paging function.
Pickup	Answer a call alerting on the system. See the Call Pickup function.
Pickup Member	Answer a call alerting the hunt group of which the user is a member. See the Call Pickup Members function.
Twinning	Switch mobile twinning on/off and set the twinning destination. Also used to pull a call answered at the twinned number back to the users primary extension. See the Twinning function.
User	Monitor the status of a user. Also used to call them or to pickup calls alerting them. See the User function.
Visual Voice	Create a visual voice access button. See Visual Voice.
Voicemail	Equivalent to the Voicemail Collect function.
Voicemail on/off	Switch the use of the user's mailbox to answer unanswered calls calls on/off. See the Voicemail On function.

The user will need to be made aware of which physical buttons can be programmed as this varies between the different T3 phones. See T3 Compact, T3 Classic and T3 Comfort.

Configuring a T3 User for Button Programming

1. Using Manager, receive the configuration from the system.
2. Select the T3 user and then select **Menu Programming**.
3. Set the action for one of the menus to **Self-Administer**.
4. Send the configuration back to the system.
5. The user will now be able to access button programming from their phone via **Menu | Settings | Button programming**.

Related links

Button Programming Overview on page 789

Interactive Button Menus

For certain functions, on display phones where a button has been configured without a specific number, a menu for number entry is displayed. The menu includes a **Dir** option for selecting a number from the directories held by the system.

Functions that use the interactive menu are:

Feature	Directory lists...		Feature	Directory lists...
Automatic Intercom	Users		Follow Me Here Cancel	Users
Acquire Call/Call Steal	Users		Follow Me Here	Users
Call Forwarding All	Users		Follow Me To	Users
Call Intrude	Users		Forward Number	Users/Groups
Call Park To Other Extension	Users		Forward Busy Number	Users/Groups
Dial Inclusion	Users		Group Paging	Users/Groups
Dial Intercom	Users		Leave Word Calling	Users/Groups
Directed Call Pickup	Users/Groups		Priority Calling	Users/Groups

User and Group buttons can be used to indicate the required user or hunt group only if those buttons are on an associated button module. **User** and **Group** buttons on the users extension are not accessible while the interactive button menu is being displayed.

For functions supported across a multi-site network, the directory will include remote users and advertised hunt groups.

For M-Series and T-Series phone, the volume buttons are used to scroll through the list of matching names. If this is done during a call or while a call is alerting, this will also adjust the call or ring volume.

Related links

Button Programming Overview on page 789

Label Templates

The attached zip file below contains Word document templates for the paper programmable key labels on various phones supported by the system. Two templates are provided, one for A4 size paper, the other for US Letter sized paper.

DSS Key Label Template File (Microsoft Word .dot Files)

For ETR, M-Series, T-Series, 1400 and 1600 phones, a number of tools and perforated printable labels are available. For further details visit http://support.avaya.com and search for information on DESI. Alternatively visit http://www.desi.com.

Manager is able to pass user button information to a DESI application on the same PC. This allows printing of labels using the label text set within the system configuration. Currently only ETR, M-Series, T-Series, 1400 and 1600 phonesphones are supported by DESI.

Related links

Button Programming Overview on page 789

Chapter 17: Button Programming Actions

The following sections provide details for each of the button actions supported by system. Note that this does not include buttons on phones on a system running in Partner Edition mode.

For each the following details are listed:

- **Action** Indicates the selection path to the action from within the list of actions displayed in Manager.
- **Action Data** Indicates the type of data required by the action. For some actions no data is required while for others action data may be optional. The option to enter the data after pressing the button is not available for all phones, see Interactive Button Menus.
- **Default Label** This is the default text label displayed on phones which provide a display area next to programmable buttons. Alternate labels can be specified in the system configuration or entered by the phone user (refer to the telephone user guide). Note that for buttons with action data set, the action data may also be displayed as part of the default label. Depending on the display capacity of the particular phone, either a short or long label is displayed.
- **Toggles** Indicates whether the action toggles between two states, typically on or off.
- **Status Indication** Indicates whether the button provides status indication relevant to the feature if the button has status lamps or display. If the **Status Indication** is listed as **Required** it indicates that the button action is only supported on programmable buttons that can provide status indication.
- **User Admin** This item indicates that users with a Self-Administer button can assign the action to other buttons themselves.
- Phone Support This is only a general indication of support or otherwise of an action by phones within particular series. On phones with 3 or less programmable buttons those button can only be used for the Call Appearance action. In addition some actions are only supported on phones where the programmable buttons provide status indication and or a display for data entry once the feature is invoked.

Table of Button Programming Actions

The following tables list the actions available for programmable buttons on system.

Login Code Required Some function may require the user to enter their log in code. This typically applies when the action data is left blank for entry when the button is pressed.

General

Action	Action Data	Default Label
Dial	Any number.	Dial
Group	"Group name" in quote marks.	<Group name>
User	"User name" in quote marks.	<User name>

Appearance

Action	Action Data	Default Label
Appearance	None.	**a=**
Bridged Appearance	User name and call appearance button number.	<user name><appearance label>
Coverage Appearance	User name.	<user name>
Line Appearance	Line appearance ID.	**Line**

Emulation

Action	Action Data	Short Label	Long Label
Abbreviated Dial	Any number.	**AD**	**Abbreviate Dial**
Abbreviated Dial Pause	None.	**Pause**	**–**
Abbreviated Dial Program	None.	**Prog**	**–**
Abbreviated Dial Stop	None.	**Stop**	**–**
Account Code Entry	Account code or blank for entry when pressed.	**Acct**	**Account Code**
ACD Agent Statistics	None.	**Stats**	**–**
ACD Stroke Count	None.	**Count**	**–**
AD Special Function Mark	None.	**Mark**	**–**
AD Special Function Wait	None.	**Wait**	**–**
AD Special Functions	None.	**Sfunc**	**–**
AD Suppress	None.	**Spres**	**Suppress Digits**
Automatic Callback	None.	**AutCB**	**Auto Callback**
Automatic Intercom	User number or name.	**Iauto**	**Auto Intercom**
Call Forwarding All	Any number or blank for entry when pressed.	**CFrwd**	**Call Forward All**
Call Park	Park slot ID (alphanumeric) or blank for menu of slots in use.	**CPark**	**Call Park**
Call Park To Other Extension	User number.	**RPark**	**Call Park to Other**

Table continues…

Action	Action Data	Short Label	Long Label
Call Pickup	None.	**CpkUp**	**Call Pickup Any**
Cancel Leave Word Calling	None.	**CnLWC**	**–**
Consult	None.	**CnsIt**	**–**
Dial Intercom	User number or name or blank for entry when pressed.	**Idial**	**Auto Intercom**
Directed Call Pickup	User number or name or group number or name or or blank for entry when pressed..	**DpkUp**	**Call Pickup**
Directory	None.	**Dir**	**–**
Drop	None.	**Drop**	**Drop Call**
Group Paging	User or group number or name or blank for entry when pressed.	**GrpPg**	**Page**
Headset Toggle	None or FF	**HdSet**	**–**
Inspect	None.	**Inspt**	**–**
Internal Auto-Answer	None.	**HFAns**	**Auto Answer**
Leave Word Calling	None.	**LWC**	**–**
Manual Exclude	None.	**Excl**	**–**
Priority Calling	None.	**Pcall**	**–**
Ringer Off	None.	**RngOf**	**Ringer Off**
Self-Administer	Blank or 1 or 2	**Admin**	**Self Administer**
Send All Calls	None.	**SAC**	**Send All Calls**
Stored Number View	None.	**BtnVu**	**–**
Time of Day	None.	**TmDay**	**–**
Timer	None.	**Timer**	**–**
Twinning	None.	**Twinning**	**Twinning**
Visual Voice	None.	**Voice**	**Voice**

Advanced

Action	Action Data	Category	Short Label	Long Label
Acquire Call	User number or blank for last call transferred.	Call	**Acquir**	**Acquire**

Table continues…

Action	Action Data	Category	Short Label	Long Label
Break Out	System name or IP address or blank for selection when pressed.	Dial	**BkOut**	**Breakout**
Busy	None.	Busy	**Busy**	**–**
Busy On Held	0 (off) or 1 (on).	Busy	**BusyH**	**–**
Call Intrude	User number or blank for entry when pressed.	Call	**Intru**	**Call Intrude**
Call List	None.	Call	**LIST**	**–**
Call Listen	User number.	Call	**Listn**	**Listen**
Call Log	None.	Call		**Call Log**
Call Pickup Any	None.	Call	**PickA**	**Pickup Any**
Call Pickup Group	Group number or name.	Call	**PickG**	**Pickup Group**
Call Pickup Members	Group number or name.	Call	**PickM**	**Pickup Members**
Call Queue	User number.	Call	**Queue**	**Queue**
Call Record	None.	Call	**Recor**	**Record**
Call Screening	None.	Call	**CallScreen**	**Call Screening**
Call Steal	User number or blank for last call transferred.	Call	**Steal**	**–**
Call Waiting Off	None.	Call	**CWOff**	**–**
Call Waiting On	None.	Call	**CWOn**	**–**
Call Waiting Suspend	None.	Call	**CWSus**	**–**
Cancel All Forwarding	None.	Call	**FwdOf**	**Call Forward Off**
Cancel Ring Back When Free	None.	Miscellaneous	**RBak-**	**–**
Channel Monitor	Channel number.	Call	**ChMon**	**–**
Clear Call	None.	Call	**Clear**	**Clear**
Clear CW	None.	Call	**ClrCW**	**–**
Clear Hunt Group Night Service	Group number.	Call	**HGNS-**	**–**
Clear Hunt Group Out Of Service	Group number.	Call	**HNOS-**	**–**

Table continues…

Action	Action Data	Category	Short Label	Long Label
Clear Quota	"Service name" within quote marks or "" for all services.	Call	**Quota**	**–**
Coaching Intrusion	User number or name or blank for entry when pressed.	Call	**Coach**	**Coaching Intrusion**
Conference	Invoke the conference process. (M and T-Series phones only)	Call	**Conf**	**–**
Conference Add	None.	Call	**Conf+**	**Conference Add**
Conference Meet Me	Conference name or number.	Call	**CnfMM**	**Conf. Meet Me**
Dial 3K1	Any number.	Dial	**D3K1**	**Dial 3K1**
Dial 56K	Any number.	Dial	**D56K**	**Dial 56K**
Dial 64K	Any number.	Dial	**D64K**	**Dial 64K**
Dial CW	User number.	Dial	**DCW**	**Dial Call Waiting**
Dial Direct	User number or name or blank for entry when pressed.	Dial	**Dirct**	**Auto Intercom**
Dial Emergency	Any number.	Dial	**Emrgy**	**Dial Emergency**
Dial Inclusion	User number or name or blank for entry when pressed.	Dial	**Inclu**	**Dial Inclusion**
Dial Paging	User or group number or name or blank for entry when pressed.	Dial	**Page**	**Page**
Dial Physical Extn by Number	Extension port Base Extension number.	Dial	**PhyEx**	**Dial Physical Extn**
Dial Physical Extn by Id	Extension port ID number. (Release 1.4+)	Dial	**DialP**	**Dial Extn by Id**
Dial Speech	Any number.	Dial	**DSpch**	**Dial Speech**
Dial V110	Any number.	Dial	**DV110**	**Dial V110**
Dial V120	Any number.	Dial	**DV120**	**Dial V120**
Dial Video	Any number.	Dial	**Dvide**	**Dial Video**

Table continues…

Action	Action Data	Category	Short Label	Long Label
Display Msg	Command string.	Dial	**Displ**	**–**
Do Not Disturb Auto-Intercom Deny	None	Do Not Disturb	**NoAI**	**No Auto Int Calls**
Do Not Disturb Exception Add	Any number.	Do Not Disturb	**DNDX+**	**–**
Do Not Disturb Exception Delete	Any number.	Do Not Disturb	**DNDX-**	**–**
Do Not Disturb Off	None.	Do Not Disturb	**DNDOf**	**–**
Do Not Disturb On	None.	Do Not Disturb	**DNDOn**	**Do Not Disturb**
Extn Login	None.	Extension	**Login**	**Login**
Extn Logout	None.	Extension	**Logof**	**Logout**
Flash Hook	None.	Miscellaneous	**Flash**	**Flash Hook**
Follow Me Here	User number.	Follow Me	**Here+**	**Follow Me Here**
Follow Me Here Cancel	User number or blank for entry when pressed.	Follow Me	**Here-**	**Follow Me Here-**
Follow Me To	User name or user number or blank for entry when pressed.	Follow Me	**FolTo**	**Follow Me To**
Forward Hunt Group Calls On	None.	Forward	**FwdH+**	**–**
Forward Hunt Group Calls Off	None.	Forward	**FwdH-**	**Fwd HG Calls**
Forward Number	Any number or blank for entry when pressed.	Forward	**FwdNo**	**Fwd Number**
Forward On Busy Number	Any number or blank for entry when pressed.	Forward	**FwBNo**	**Fwd Busy Number**
Forward On Busy Off	None.	Forward	**FwBOf**	**–**
Forward On Busy On	None.	Forward	**FwBOn**	**Fwd Busy**
Forward On No Answer Off	None.	Forward	**FwNOf**	**–**
Forward On No Answer On	None.	Forward	**FwNOn**	**Fwd No Answer**
Forward Unconditional Off	None.	Forward	**FwUOf**	**–**

Table continues…

Action	Action Data	Category	Short Label	Long Label
Forward Unconditional On	None.	Forward	**FwUOn**	**Fwd Unconditional**
Group Listen On	None.	Extension	**GroupListenOn**	**–**
Hold Call	ISDN Exchange slot number.	Hold	**Hold**	**–**
Hold CW	None.	Hold	**HoldCW**	**–**
Hold Music	None.	Hold	**Music**	**Hold Music**
Hunt Group Disable	Group number or name or blank for all groups.	Hunt Group	**HGDis**	
Hunt Group Enable	Group number or name or blank for all groups.	Hunt Group	**HGEna**	**HG Enable**
Last Number Redial	Redial the last number dialed. (M and T-Series phones only)	Call	**Again**	**–**
MCID Activate	None.	Miscellaneous	**MCID**	**Malicious Call**
Monitor Analogue Trunk MWI	Line appearance ID.	Voicemail	**TrkMW**	**Trunk MWI**
Off Hook Station	None.	Miscellaneous	**OHStn**	**–**
Pause Recording	None.	Call	**PauseRec**	**Pause Recording**
Priority Call	User number or name.	Call	**PCall**	**Priority Call**
Private Call	None. (Release 4.0+)	Call	**PrivC**	**Private Call**
Relay Off	1 or 2.	Relay	**Rely-**	**–**
Relay On	1 or 2.	Relay	**Rely+**	**Relay On**
Relay Pulse	1 or 2.	Relay	**Relay**	**Relay Pulse**
Resume Call	ISDN Exchange slot number.	Call	**Resum**	**–**
Retrieve Call	ISDN Exchange slot number.	Call	**Retriv**	**–**
Ring Back When Free	None.	Miscellaneous	**RBak+**	**Auto Callback**
Set Absent Text	String for selected message and custom text.	Set	**Absnt**	**Absence Text**

Table continues…

Action	Action Data	Category	Short Label	Long Label
Set Account Code	Blank or valid account code. (Release 2.1+)	Set	**Acct**	**Account Code**
Set Hunt Group Night Service	Group number.	Set	**HGNS+**	**HG Night Service**
Set Hunt Group Out Of Service	Group number.	Set	**HGOS+**	**HG Out of Service**
Set Inside Call Seq	Value 0 to 10.	Set	**ICSeq**	**–**
Set Night Service Group	Group number. (Release 4.2+)	Set	**SetNSG**	**HG NS Group**
Set No Answer Time	Time in seconds (range 6 to 99999).	Set	**NATim**	**No Answer Time**
Set Outside Call Seq	Value 0 to 10.	Set	**OCSeq**	**–**
Set Out of Service Group	Group number. (Release 4.2+)	Set	**SetOOSG**	**HG OS Group**
Set Ringback Seq	Value 0 to 10.	Set	**RBSeq**	**–**
Set Wrap Up Time	Time in seconds (range 0 to 99999).	Set	**WUTim**	**Wrap-up Time**
Speed Dial	Initiate the speed dial selection process. (M and T-Series phones only)	Dial	**SpdDial**	**–**
Stamp Log	None.	Miscellaneous	**StmpL**	**Stamp Log**
Suspend Call	ISDN Exchange slot number.	Suspend	**Suspe**	**–**
Suspend CW	ISDN Exchange slot number.	Suspend	**SusCW**	**–**
Toggle Calls	None.	Call	**Toggl**	**–**
Transfer	Initiate the call transfer process. (M and T-Series phones only)	Call	**Xfer**	**–**
Unpark Call	Park slot ID (alphanumeric).	Call	**Ride**	**–**
Voicemail Collect	See notes.	Voicemail	**VMCol**	**VMail Collect**
Voicemail Off	None.	Voicemail	**VMOff**	**–**
Voicemail On	None.	Voicemail	**VMOn**	**VMail On**
Voicemail Ringback Off	None.	Voicemail	**VMRB-**	**–**

Table continues…

Action	Action Data	Category	Short Label	Long Label
Voicemail Ringback On	None.	Voicemail	**VMRB+**	**VMail Ringback**
Whisper Page	User number or name or blank for entry when pressed.	Call	**Whisp**	**Whisper Page**

Abbreviated Dial

This function allows quick dialing of a stored number.

Action: Emulation | Abbreviated Dial.

Action Data:

- **Full Number** The number is dialled.
- **Partial Number** The partial number is dialled and the user can then complete dialing the full number.

Default Label: AD or Abbreviate Dial.

Toggles: No.

Status Indication: No.

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** Yes	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes **[1]**	**3700 Series:** No	**5400 Series:** Yes [1]	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes **[1]**	**3810:** No	**5600 Series:** Yes [1]	**9600:** No	

[1] Not 1403, 1603, 2402, 4601, 4602, 5402, 5601 and 5602 models.

Abbreviated Dial Pause

Not supported. Provided for CTI emulation only. Allows a user to enter a pause character when programming an abbreviated dial.

Action: Emulation | Abbreviated Dial Pause.

Action Data: None.

Default Label: Pause.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. May have limited support on some specific T3 phone models if detailed below.

Abbreviated Dial Program

Not supported. Provided for CTI emulation only. Allows a user to program abbreviated dialing numbers against other programmable buttons. This function cannot be used to overwrite call appearance buttons.

Action: Emulation | Abbreviated Dial Program.

Action Data: None.

Default Label: Prog.

Toggles: No.

Status Indication: No.

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series**	**4100 Series:** No	**6400 Series:** No	**D100:** No
1100 Series: No	**2400 Series:** No	**4400 Series:** No	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** No	**9040:** No	**T-Series:** No
1400 Series: No	**3700 Series:** No	**5400 Series:** No	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: No	**3810:** No	**5600 Series:** No	**9600 Series:** No	

Abbreviated Dial Stop

Not supported. Provided for CTI emulation only. Allows a user to enter a stop character when programming an abbreviated dial.

Action: Emulation | Abbreviated Dial Stop.

Action Data: None.

Default Label: Stop.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. May have limited support on some specific T3 phone models if detailed below.

Account Code Entry

Enter an account code for a call. This button can be used before dialing a number or during a call.

Action: Emulation | Account Code Entry.

Action Data: Optional. If an code is set it must match an account code set in the account codes list. If no account code is set, the phone display will request entry of a valid code. This option is not supported on XX02 phones and the T7000 phone.

Default Label: Acct or Account Code.

Toggles: No.

Status Indication: No.

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0 DT software.
2. May have limited support on some specific T3 phone models if detailed below.

T3 Phones:

- **Classic/Comfort icon**: Displays **1234**.
- **DSS Link LED**: None.

ACD Agent Statistics

Not supported. Provided for CTI emulation only.

Action: Emulation | ACD Agent Statistics.

Action Data: None.

Default Label: Stats.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. May have limited support on some specific T3 phone models if detailed below.

ACD Stroke Count

Not supported. Provided for CTI emulation only.

Action: Emulation | ACD Stroke Count.

Action Data: None.

Default Label: Count.

Toggles: No.

Status Indication: No.

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No

Table continues…

1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0 DT software.
2. May have limited support on some specific T3 phone models if detailed below.

Acquire Call

See Call Steal.

AD Special Functions

Not supported. Provided for CTI emulation only. Allows a user to enter a special character (mark, pause suppress, wait) when entering an abbreviated dial.

Action: Emulation | AD Special Functions.

Action Data: None.

Default Label: Sfunc.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

AD Special Function Mark

Not supported. Provided for CTI emulation only. Allows a user to enter a mark character when programming abbreviated dial.

Action: Emulation | AD Special Function Mark.

Action Data: None.

Default Label: Mark.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

AD Special Function Wait

Not supported. Provided for CTI emulation only. Allows a user to enter a Wait for Dial Tone character when programming an abbreviated dial.

Action: Emulation | AD Special Function Wait.

Action Data: None.

Default Label: Wait.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T3/T3 IP Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

No

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

AD Suppress

Suppresses the display of dialed digits on the telephone display. Dialed digits are replaced with an **s** character.

Action: Emulation | AD Suppress.

Action Data: None.

Default Label: Spres or Suppress Digits.

Toggles: Yes.

Status Indication: Yes.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>** ◀	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No

Table continues…

1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series**: No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

After Call Work

This button is used by users configured as a Customer Call Reporter (CCR) Agent (**User | Telephony | Supervisor Settings**) and working with the CCR application. It shows the CCR agent their current After Call Work (ACW) status and allow them to manually change status. While in ACW state, the agent will not receive hunt group calls.

CCR Agents can be automatically put into and taken out of ACW by the system if the user is configured for Automatic After Call Work (User | Telephony | Supervisor Settings). Those users must have an **After Call Work** button.

Note:

CCR is not supported in IP Office release 9.1 and later.

Action: Advanced | Miscellaneous | After Call Work

Action Data: None.

Default Label: ACWrk or After Call Work.

Toggles: Yes.

Status Indication: Yes. Required.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>**	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** No	**4100 Series:** No	**6400 Series:** No	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** No	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** No	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes [1]	**9500 Series:** Yes	
1600 Series: Yes [1]	**3810:** No	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 2402, 4601, 4602, 5402, 5601 and 5602.

Appearance

Creates a call appearance button. This can be used to answer and make calls. Users with multiple call appearance buttons can handle multiple calls.

Call appearance functions, assigned to buttons that do not have status lamps or icons, are automatically disabled until the user logs in at a phone with suitable buttons.

Appearance buttons can be set with a ring delay if required or to not ring. This does not affect the visual alerting displayed next to the button. The delay uses the user's Ring Delay (**User | Telephony | Multi-line Options**) setting.

Details

Action: Appearance | Appearance.

Action Data: Optional text label.

Default Label: a=.

Toggles: No.

Status Indication: Yes, required. See “Call Appearance Button Indication” in *Administering IP Office with Manager*.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** No	**4100 Series:** Yes [1]	**6400 Series:** Yes	**D100:** No

Table continues…

1100 Series: No	**2400 Series:** Yes	**4400 Series:** Yes	**7400 Series:** Yes [1]	**M-Series:** Yes [1]
1200 Series: No	**3600 Series:** Yes	**5400 Series:** Yes	**9040:** Yes	**T-Series:** Yes [1]
1400 Series: Yes	**3700 Series:** No	**4600 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes	**3810:** Yes	**5600 Series:** Yes	**9600 Series:** Yes	

1. 4100 Series and 7400 Series phones support virtual call appearance button operation. This also applies to T7000, T7100, M7100 and M7100N phones and the Audio Conferencing Unit (ACU).

Virtual Call Appearances

4100 Series and 7400 Series phones support virtual call appearance button operation. This also applies to T7000, T7100, M7100 and M7100N phones and the Audio Conferencing Unit (ACU).

Virtual call appearance operation is similar to an analog phone with call waiting enabled. However, it does not use the call waiting on/off settings, instead it uses call appearance buttons.

The number of virtual call appearances is set by the call appearance buttons programmed in the user's settings. These must be programmed as a single block start from button 1. It is recommended that only a maximum of 3 call appearances are used, however the user must have at least 1 call appearance programmed in order to make and receive calls.

Virtual Call Appearance Usability

If the user goes off-hook, they are connected to the alerting call if any, else to dial tone in order to make an outgoing call. This uses one of their virtual call appearance buttons.

With a call connected:

- If another call arrives on another virtual call appearance, the user will hear a call waiting tone on the set. The display, if the phone has one, will switch between details of the current and the waiting caller.
- If the user presses **Hold**, the connected call is placed on hold and:

If there are any available virtual call appearances, dial tone is heard. This allows the user to make a call or to use short codes that may affect the held or waiting calls. The following are some of the default short codes that can be used:

- ***26: Clear CW** Drop the previous call and answer the waiting call.
- ***52: Clear Call** Drop the previous call.
- ***47: Conference Add** Start a conference between the user and any held calls.
- Else, if there is a call waiting, that call is answered.
- Else, if there is a call on hold, that call is reconnected.

If the user presses **Release** or **Drop** or goes on-hook during a call, the current call is ended and the user's phone returns to idle. If there is a waiting call, it starts ringing. The user can answer the call by going off hook or pressing **Hold**.

With the phone idle:

If the user goes off hook:

- The first alerting call appearance is answered if any.
- Else, the first idle call appearance is seized and the user hears dial tone.
- The user can press `Hold`to switch between virtual call appearances. This will answer or retrieve any call on next virtual call appearance or else hear dial tone to make a call.

With the phone idle but a call alerting:

Going off-hook or pressing Hold will answer the call.

When all the users virtual call appearances are in use, they are busy to any further calls. Calls will follow forward on busy if set, else go to voicemail is available or else get busy indication.

The only other appearance button controls applied and supported are

Reserve Last CA This setting can be enabled for the extension user. When selected, the last available call appearance is reserved for outgoing calls only. For example, for a user with 3 call appearances, they return busy to any further calls when 2 virtual appearances are in use. The extension user can press hold to get dial tone on the reserved call appearance. An available call appearance is also required when using **Feature 70** to initiate a call transfer.

Coverage Appearances Other users can have Coverage Appearance buttons set to provided coverage to the virtual call appearance user. The virtual appearance users **Individual Coverage Time** setting is applied.

Automatic Callback

Sets a ringback on the extension being called. When the target extension ends its current call, the ringback user is rung (for their set **No Answer Time**) and if they answer, a new call is made to the target extension.

Ringback can also be cleared using the Cancel Ring Back When Free function.

Action: Emulation | Automatic Callback.

Action Data: None.

Default Label: AutCB or Auto Callback.

Toggles: Yes.

Status Indication: Yes.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>** ◀	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Auto-Intercom Deny

Use the Auto-Intercom Deny function to block automatic intercom calls.

Action: Advanced | Do Not Disturb | Auto Intercom Deny.

Action Data: Blank.

Default Label: NoAI or No Auto Int Calls.

Toggles: Yes.

Status Indication: Yes.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>** ◀	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	▲ On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes

Table continues…

1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Automatic Intercom

Automatic intercom functions allow you to call an extension and have the call automatically answered on speaker phone after 3 beeps. The extension called must support a handsfree speaker. If the extension does not have a handsfree microphone then the user must use the handset if they want to talk. If the extension is not free when called, the call is presented as a normal call on a call appearance button if available.

This feature can be used as part of handsfree announced transfers.

Action: Emulation | Automatic Intercom.

Action Data: User number or name.

This field can be left blank for number entry when pressed.

On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.

Default Label: Iauto or Auto Intercom.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes

Table continues…

1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. May have limited support on some specific T3 phone models if detailed below.

T3 Phones:

- **Classic/Comfort icon**: Displays followed by the set number.
- **DSS Link LED**: None.

Break Out

This feature is usable within a system multi-site network. It allows a user on one system in the network to specify that the following dialing be processed by another system on the network as if the user dialed it locally on that other system.

On phones with a multi-line display, if the target system is not specified in the button settings, a menu of the available systems in the network is displayed from which a selection can be made.

Action: Advanced | Dial | Break Out.

Action Data: Optional. The system name or IP address of the required system can be specified. If no system name or IP address is set, on display phones a list of systems within the network is displayed when the button is pressed.

Default Label: BkOut or Breakout.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**M-Series:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**T-Series:** No
1200 Series: No	**3600 Series:** Yes	**4600 Series:** Yes [1]	**9040:** Yes	**T3/T3 IP Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes [1]	**9500 Series:** Yes	

Table continues…

1600 Series: Yes [1]	**3810:** No	**5600 Series:** Yes [1]	**D100:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5402, 5601 and 5602 models.

Bridged Appearance

Creates an appearance button that follows the state of another user's call appearance button. The bridged appearance can be used to make and answer calls on behalf of the call appearance user.

The bridged appearance button user must also have at least one call appearance button programmed.

Bridged appearance functions, assigned to buttons that do not have status lamps or icons, are automatically disabled until the user logs in at a phone with suitable buttons.

Appearance buttons can be set with a ring delay if required or to not ring. This does not affect the visual alerting displayed next to the button. The delay uses the user's Ring Delay (User | Telephony | Multi-line Options) setting.

Action: Appearance | Bridged Appearance.

Action Data: User name and call appearance button number.

Default Label: <user name><call appearance label>.

Toggles: No.

Status Indication: Yes. Required. See Bridge Appearance Button Indication.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** No	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes [1]
1200 Series: No	**3600 Series:** Yes	**4600 Series:** Yes	**9040:** Yes	**T-Series:** Yes [1]
1400 Series: Yes	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes	**3810:** Yes	**5600 Series:** Yes	**9600 Series:** Yes	

1. Not supported on T7000, T7100, M7100, M7100N and the Audio Conferencing Unit (ACU).

Busy

Not used.

Busy On Held

When on, busy on held returns busy to new calls while the user has an existing call on hold. While this feature can be used by users with appearance keys, it is not recommended as this overrides the basic call handling intent of appearance keys.

Action: Advanced | Busy | Busy on Held.

Action Data: 1 for on, 0 for off.

Default Label: BusyH.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Call Forwarding All

Switches forward unconditional on and sets the forward number to the number specified or prompts the user to enter a number if none is specified.

Action: Emulation | Call Forwarding All.

Action Data: Telephone number or blank for entry when pressed.

If blank, user's with a log in code will be prompted to enter that code to use this function.

On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.

Default Label: CFrwd or Call Forward All.

Toggles: Yes.

Status Indication: Yes.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>** ◀	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Call Intrude

This feature allows you to intrude on the existing connected call of the specified target user. All call parties are put into a conference and can talk to and hear each other. A **Call Intrude** attempt to a user who is idle becomes a Priority Call.

The ability to intrude and be intruded is controlled by two configuration settings, the Can Intrude (User | Telephony | Supervisor Settings) setting of the user intruding and the Cannot Be Intruded (User | Telephony | Supervisor Settings) setting of target being intruded on. The setting of any

other internal party is ignored. By default, no users can intrude and all users are set to cannot be intruded.

The system support a range of other call intrusion methods in addition to this feature.

Action: Advanced | Call | Call Intrude.

Action Data: User number or blank for entry when pressed.

On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.

Default Label: Intru or Intrude.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Call List

This function is only supported for T3 phones. It provides access to a list of received calls.

Action: Advanced | Call | Call List.

Action Data: None.

Default Label: LIST.

Toggles: No.

Status Indication: Yes Required.

User Admin: No.

Phone Support This function is only supported for T3 phones.

T3 Phones:

- **Classic/Comfort icon**: Displays **LIST**.
- **DSS Link LED**: On when calls are in the list. Flashes when new calls are in the list.

Call Listen

This feature allows you to monitor another user's call without being heard. Monitoring can be accompanied by a tone heard by all parties. Use of the tone is controlled by the Beep on Listen setting on the System | Telephony | Tones & Music tab. The default for this setting is on. If enabled, this is the only indication of monitoring given to the monitored user. There is no phone display indication of monitoring.

Warning:

The use of features to listen to a call without the other call parties being aware of that monitoring may be subject to local laws and regulations. Before enabling the feature you must ensure that you have complied with all applicable local laws and regulations. Failure to do so may result in severe penalties.

The use of call listen is dependant on:

The target being a member of the group set as the user's Monitor Group (User | Telephony | Supervisor Settings). The user does not have to be a member of the group.

The ability to intrude and be intruded is controlled by two configuration settings, the Can Intrude (User | Telephony | Supervisor Settings) setting of the user intruding and the Cannot Be Intruded (User | Telephony | Supervisor Settings) setting of target being intruded on. The setting of any other internal party is ignored. By default, no users can intrude and all users are set to cannot be intruded.

This feature uses system conference resources. If insufficient conference resource are available it will not be possible to use this feature.

A number of features are supported for call listening:

- Users can be given privacy features that allow them to indicate that a call cannot be monitored. See Private Calls.
- IP extensions can be monitored including those using direct media. Previously the monitoring of IP extensions could not be guaranteed.
- The monitoring call can be initiated even if the target user is not currently on a call and remains active until the monitoring user clears the monitoring call.
- The user who initiated the call listen can also record the call.

Intruding onto an a user doing silent monitoring (Call Listen) is turned into a silent monitoring call.

1400, 1600, 9500 and 9600 Series phones with a user button can initiate listening using that button if the target user meets the criteria for listening.

The system support a range of other call intrusion methods in addition to this feature.

Action: Advanced | Call | Call Listen.

Action Data: User number.

Default Label: Listn or Listen.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Call Log

This function provides access to a list of received calls.

Action: Advanced | Call | Call Log.

Action Data: None.

Default Label: Call Log.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support This function is only supported on M-Series and T-Series phones with a display. Not supported on phones on a DECT systems.

Call Park

Allows the user to park and unpark calls. The button can be used in two ways, either associated with a specified park slot number or unspecified.

When associated with a specific park slot number, the button will park and unpark calls from that park slot and indicate when a call is parked in that park slot. Similarly the Park buttons within application (for example SoftConsole and one-X Portal) can be used to park, retrieve and indicate parked calls.

When not associated with a specific park slot number, the button will park calls by assigning them a park slot number based on the users extension number. For example, for extension XXX, the first parked call is assigned to park slot XXX0, the next to XXX1 and so on up to XXX9. The button will indicate when there are parked calls in any of those slots. On the T7000 phone, only a single automatic part slot XXX0 is supported.

- With a call connected, pressing the button will park that call using a park slot number assigned by the system based on the extension number.
- With no call connected, pressing the button will display details of any calls parked by the extension and allow their retrieval.

Action: Emulation | Call Park.

Action Data: Optional. Either blank or a specific park slot number. Name ca

Park slot IDs can be up to 15 digits in length. Names can also be used for application park slots.

Default Label: CPark or Call Park.

Toggles: ✓.

Status Indication: ✓.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- Calls parked by extension	**CPark** ◆	**CPark**	Green flash	Red flash	Green flash	Blue	Slow flash
- Call Parked by other extension	**CPark**	**CPark**	Red flash	**Red on**	Red flash	**Green**	Slow flash
- No parked calls	**CPark**	**CPark**	Off	Off	Off	Grey	Off

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes [2]
1200 Series: No	**3600 Series:** Yes	**5400 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes [2]
1400 Series: Yes [1]	**3700 Series:** No	**4600 Series:** Yes [1]	**9500 Series:** Yes	
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 2402, 4601, 4602, 5402, 5601 and 5602.
2. M-Series/T-Series: The button is equivalent to **Feature 74**.

Call Park and Page

Parks the user's current call into the park slot number specified on the **System | Telephony | Park & Page** tab, in the **Central Park Range** field.

On M/T-series phones, 14xx/16xx phones, and the 9504 phone, the user is presented with up to three Page Target Groups. On other 95xx/96xx phones, the Page action displays a scrolling list of possible Page Target Groups. The user may also directly enter a Page target number, or use the system Directory to find a Page target.

A call Parked within the Central Park Range (regardless of the origin of the Park action) can be retrieved by directly dialing the desired Central Park Range slot on which that call is Parked.

Action: Emulation | Call Park and Page.

Action Data: None.

Default Label: ParkPage

Toggles: No.

Status Indication: No.

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** No	**4100 Series:** No	**6400 Series:** No	**D100:** Yes
1100 Series: Yes	**2400 Series:** No	**4400 Series:** No	**7400 Series:** No	**M-Series:** Yes [1]
1200 Series: Yes	**3600 Series:** No	**5400 Series:** No	**9040:** Yes	**T-Series:** Yes [1]

Table continues…

1400 Series: Yes	**3700 Series:** No	**4600 Series:** No	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes	**3810:** No	**5600 Series:** No	**9600 Series:** Yes	

1. M-Series/T-Series: **Feature 74** is equivalent to this button when a Central Park Range is defined. On an M7000 phone, if this feature is invoked, the call always attempts to Park on the highest defined Central Park Range slot. See the Call Park and Page short code description for details.

Call Park To Other Extension

Allows the user to park their current call against another user's extension. The parked call indication on that extension is then activated according to the telephone type.

If the target extension has a Call Park button with no specific park slot number, the parked call will be indicated by that button and can be unparked from the list of parked calls shown when that button is pressed.

The park slot number assigned to the parked call is based on the number of the extension parking the call. For example, calls parked by extension 201 are assigned the park slot ID 2010, 2011 and so on up to 2019 depending on the number of calls parked.

Action: Emulation | Call Park To Other Extension.

Action Data: User number. This field can be left blank for number entry when pressed.

On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.

Default Label: RPark or Call Park to Other.

Toggles: Yes .

Status Indication: Yes. This is the status indication on the extension parking the call.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- Parked call	**RPark** ◆	**RPark**	Green flash	Red flash	Green flash	Blue	Slow flash
- No parked call	**RPark**	**RPark**	Off	Off	Off	Grey	Off

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**5400 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**4600 Series:** Yes [1]	**9500 Series:** Yes	
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 2402, 4601, 4602, 5402, 5601 and 5602.

Call Pickup

Answer an alerting call on the system.

Action: Emulation | Call Pickup.

Action Data: None.

Default Label: CpkUp or Call Pickup Any.

Toggles: No.

Status Indication: No.

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** Yes	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

2. **T3 Phones**: Displays a menu for entry of the extension number from which to pickup a call.
   - **Classic/Comfort icon**: Displays .
   - **DSS Link LED**: None.

Call Pickup Any

Pick up the first available ringing call on the system.

Action: Advanced | Call | Call Pickup Any.

Action Data: None.

Default Label: PickA or Pickup Any.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. **T3 Phones**: Displays a list of call ringing from which the user can select a call to answer.
   - **Classic/Comfort icon**: Displays .
   - **DSS Link LED**: None.

Call Pickup Group

Pick up a call ringing any hunt group of which the user is a member or set to pick up calls from a specific group.

The user can use this feature even if their membership of the group is currently set as disabled.

Action: Advanced | Call | Call Pickup Group.

Action Data: Optional. To pick up calls from a specific group, use the group number or name.

Default Label: PickG or Pickup Group.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. May have limited support on some specific T3 phone models as detailed below.

T3 Phones: Displays a list of calls ringing the hunt group from which the user can select which call to answer.

- **Classic/Comfort icon**: Displays followed by group name.
- **DSS Link LED**: None.

M-Series/T-Series: The button is equivalent to **Feature 75**.

Call Pickup Members

This feature can be used to pick up any call to an extension that is a member of the hunt group specified. The call picked up does not have to be a hunt group call. The call picked up does not have to be a hunt group call. The function includes group members even if their membership of the group is currently disabled.

Action: Advanced | Call | Call Pickup Members.

Action Data: Group number or name.

Default Label: PickM or Pickup Members.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. May have limited support on some specific T3 phone models as detailed below.

T3 Phones: Displays a list of calls ringing the hunt group from which the user can select which call to answer.

- **Classic/Comfort icon**: Displays followed by group name.
- **DSS Link LED**: None.

Call Queue

Transfer the call to the target extension if free or busy. If busy, the call is queued to wait for the phone to become free. This is similar to transfer except it allows you to transfer calls to a busy phone.

Action: Advanced | Call | Call Queue.

Action Data: User number.

Default Label: Queue.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Call Record

This feature allows you to record a conversation and requires Voicemail Pro to be installed. An advice of recording warning will be given if configured on the voicemail system. The recording is placed in the mailbox specified by the user's **Manual Recording Mailbox** setting. Call recording also requires available conference resources similar to a three-party conference.

Action: Advanced | Call | Call Record.

Action Data: None.

Default Label: Recor or Record.

Toggles: Yes.

Status Indication: Yes.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No

Table continues…

1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Call Screening

This function is used to enable or disable call screening. While enabled, when a caller is presented to the user's voicemail mailbox, if the user's phone is idle they will hear through the phone's handsfree speaker the caller leaving the message and can select to answer or ignore the call.

This feature is supported on 1408, 1416, 1608, 1616, 9500 Series, 9600 Series, M7310, M7310N, M7208, M7208N, M7324, M7324N, T7208, T7316 and T7316E phones. It can be used with both Embedded Voicemail and Voicemail Pro.

Call screening is only applied as follows:

- It is only applied to calls that have audible alerted at the user's extension before going to voicemail. This requires the user to have both voicemail coverage and call screening enabled and the phone's ringer not set to silent. However it is not applied if the user transfers the call to voicemail.
- It is only applied if the user's phone is idle, ie. not on a call or with a call held pending transfer or conference.
- Calls that ring the user, are then rerouted (for example follow a forward on busy setting) and then return to the user's mailbox are screened.

While a call is being screened, the phone can be used to either answer or ignore the screened call. Auto answer options are ignored.

Answering a screened call

A screened call can be answered by pressing the **Answer** soft key (if displayed) or lifting the handset. Pressing the call appearance or line button on which the call is indicated will also answer the call.

When answered:

- The phone's microphone is unmuted and a normal call between the user and caller now exists.
- The voicemail recording stops but that portion of the call already recorded is left as a new message in the user's mailbox.

Ignoring a screened call

A screened call can be ignored by pressing the Ignore soft key if displayed. On 1400, 1600, 9500 and 9600 Series phones, pressing the **SPEAKER** button will ignore the call. On M-Series and T-Series phones, pressing the **Release** key will ignore the call.

When ignored:

- The call continues to be recorded until the caller hangs up or transfers out of the mailbox.
- The user's phone returns to idle with call screening still enabled. However any other call that has already gone to voicemail is not screened.

Screened call operation

While a call is being screened:

- The mailbox greeting played and the caller can be heard on the phone's speakerphone. The caller cannot hear the user.
- The user is regarded as being active on a call. They will not be presented with hunt group calls and additional personal calls use abbreviated ringing.
- 1400/1600/9500/9600 Series phones: If the phone's default audio path is set to headset or the phone is idle on headset, then the screened call is heard through the headset.
- Any additional calls that go to the user's mailbox when they are already screening a call, remain at the mailbox and are not screened even if the existing call being screened is ended.
- Making or answering another call while listening to a screened call is treated as ignoring the screened call. For users with **Answer Pre-Select** enabled (User | Telephony | Multi-line Options), pressing an appearance button to display details of a call is also treated as ignoring the screened call.
- Other users cannot access a call that is being screened. For example they cannot use call pickup, bridged appearance or line appearance buttons, call intrude or call acquire functions.
- Phone based administration cannot be accessed and the hold, transfer and conference buttons are ignored.
- The screened caller using DTMF breakout ends the call screening.

Enabling do not disturb overrides call screening except for calls from numbers in the user's do not disturb exceptions list.

Locking the phone overrides call screening.

Manual call recording cannot be applied to a call being screened.

While a call is being screened, it uses one of the available voicemail channels. If no voicemail channels are available, call screening does not occur.

Warning:

The use of features to listen to a call without the other call parties being aware of that monitoring may be subject to local laws and regulations. Before enabling the feature you must ensure that you have complied with all applicable local laws and regulations. Failure to do so may result in severe penalties.

Details

Action: Advanced | Call | Call Screening.

Action Data: None.

Default Label: CallScreen or Call Screening.

Toggles: Yes.

Status Indication: Yes.

Status	2400, 5400 Series	4600, 5600 Series	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	T-Series, M-Series
- On.	**<Label>** ◀	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** No	**4100 Series:** No	**6400 Series:** No	**D100:** No
1100 Series: No	**2400 Series:** No	**4400 Series:** No	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** No	**9040:** No	**T-Series:** Yes [1]
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** No	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** No	**5600 Series:** No	**9600 Series:** Yes	

1. Not 1403, 1603, T7406E.

Call Steal

This function can be used with or without a specified user target.

If the target has alerting calls, the function will connect to the longest waiting call.

If the target has no alerting calls but does have a connected call, the function will take over the connected call, disconnecting the original user. This usage is subject to the **Can Intrude** setting of the **Call Steal** user and the **Cannot Be Intruded** setting of the target.

If no target is specified, the function attempts to reclaim the user's last ringing or transferred call if it has not been answered or has been answered by voicemail.

Action: Advanced | Call | Call Steal.

Action Data: User number or blank for last call transferred.

Default Label: Aquir or Aquire.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. May have limited support on some specific T3 phone models if detailed below.

Call Waiting Off

Switches call waiting off for the user. This button function is obsolete. The Call Waiting On button function toggles on/off and indicates current status.

Action: Advanced | Call | Call Waiting Off.

Action Data: None.

Default Label: CWOff.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No [2]

Table continues…

1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. May have limited support on some specific T3 phone models if detailed below.

Call Waiting On

Enables call waiting on the user's extension. When the user is on a call and another call arrives, they will hear a call waiting tone.

Note:

Call waiting does not operate for user's with call appearance buttons. See Call Waiting.

Details

Action: Advanced | Call | Call Waiting On.

Action Data: None.

Default Label: CWOn or Call Waiting On.

Toggles: Yes.

Status Indication: Yes.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>**	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No

Table continues…

1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Call Waiting Suspend

Disables call waiting, if on, for the duration of the extension's next call.

Action: Advanced | Call | Call Waiting Suspend.

Action Data: None.

Default Label: CWSus.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Cancel All Forwarding

Cancels forward unconditional, forward on busy, forward on no answer, follow me and do not disturb if any of those are active on the user's extension.

Action: Advanced | Call | Cancel All Forwarding.

Action Data: None.

Default Label: FwdOf or Call Forward Off.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Cancel Leave Word Calling

Not supported. Provided for CTI emulation only. Cancels the last Leave Word Calling message originated by the user.

Action: Emulation | Cancel Leave Word Calling.

Action Data: None.

Default Label: CnLWC.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No

Table continues…

1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Cancel Ring Back When Free

Cancels any existing ring back set by the user, see Ring Back When Free. Note that the Ring Back When Free button toggles to set or cancel ring back when free and also indicates the current status.

Action: Advanced | Miscellaneous | Cancel Ring Back When Free.

Action Data: None.

Default Label: RBak-.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. May have limited support on some specific T3 phone models if detailed below.

M-Series/T-Series: The button is equivalent to **Feature #2**.

Clear Call

This feature can be used to end the last call put on hold. This can be used in scenarios where a first call is already on hold and simply ending the second call will cause an unsupervised transfer of the first call.

Action: Advanced | Call | Clear Call.

Action Data: None.

Default Label: Clear.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Clear CW

End the user's current call and answer any call waiting. Requires the user to also have call waiting indication on. This function does not work for users with multiple call appearance buttons.

Action: Advanced | Call **|** Clear CW.

Action Data: None.

Default Label: ClrCW.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Clear Hunt Group Night Service

Changes the specified hunt group from Night Service mode to 'In Service' mode. This button function is obsolete. The Set Hunt Group Night Service function can be used to toggle a group in/out of service and provides lamp status indication.

Setting and clearing hunt group night service can be done using either manual controls or using a system time profile. The use of both methods to control the night service status of a particular hunt group is not supported.

This function is not supported between systems in a multi-site network. It can only be used by a user currently logged onto the same system as hosting the hunt group.

Action: Advanced | Call | Clear Hunt Group Night Service.

Action Data: Group number.

If left blank, the button will affect all hunt groups of which the user is a member.

The **Set Hunt Group Night Service** and **Clear Hunt Group Night Service** short code and button features can be used to switch an SSL VPN service off or on respectively. The service is indicated by setting the service name as the telephone number or action data. Do not use quotation marks.

Default Label: HGNS-.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Clear Hunt Group Out Of Service

Changes the specified hunt groups status from Out of Service mode to 'In Service' mode. This button function is obsolete. The Set Hunt Group Out Of Service function can be used to toggle a group in/out of service and provides lamp status indication.

This function is not supported between systems in a multi-site network. It can only be used by a user currently logged onto the same system as hosting the hunt group.

Action: Advanced | Call | Clear Hunt Group Out of Service.

Action Data: Group number.

If left blank, the button will affect all hunt groups of which the user is a member.

Default Label: HGOS-.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No

Table continues…

1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Clear Quota

Quotas can be assigned on outgoing calls to data services such as internet connections. The quota defines the number of minutes available for the service within a time frame set within the service, for example each day, each week or each month.

The Clear Quota function can be used to reset the quota for a specific service or for all services.

Action: Advanced | Call | Clear Quota.

Action Data: Service name" or "" (all services).

Default Label: Quota.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Coaching Intrusion

This feature allows the you to intrude on another user's call and to talk to them without being heard by the other call parties to which they can still talk. For example: User A is on a call with user B. When user C intrudes on user A, they can hear users A and B but can only be heard by user A.

The ability to intrude and be intruded is controlled by two configuration settings, the Can Intrude (User | Telephony | Supervisor Settings) setting of the user intruding and the Cannot Be Intruded (User | Telephony | Supervisor Settings) setting of target being intruded on. The setting of any other internal party is ignored. By default, no users can intrude and all users are set to cannot be intruded.

Warning:

The use of features to listen to a call without the other call parties being aware of that monitoring may be subject to local laws and regulations. Before enabling the feature you must ensure that you have complied with all applicable local laws and regulations. Failure to do so may result in severe penalties.

The system support a range of other call intrusion methods in addition to this feature.

Action: Advanced | Call | Coaching Intrusion.

Action Data: User number or name or blank for entry when pressed.

Default Label: Coach or Coaching Intrusion.

Toggles: No.

Status Indication: No.

User Admin: No feedback provided..

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No.	**20 Series:** No.	**4100 Series:** No	**6400 Series:** No	**D100:** No
1100 Series: No.	**2400 Series:** No	**4400 Series:** No	**7400 Series:** No	**M-Series:** No
1200 Series: No.	**3600 Series:** No	**4600 Series:** No	**9040:** No	**T-Series:** No
1400 Series: Yes [1][2]	**3700 Series:** No	**5400 Series:** No	**9500 Series:** Yes [2]	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** No	**5600 Series:** No	**9600 Series:** Yes	

1. Not 1403, 1603.
2. Not supported on non-IP telephones when using a headset.

Conference

This function is intend for use with Avaya M-Series and T-Series phones only. When pressed, the button invokes the same conference process as dialing **Feature 3**.

Action: Advanced | Call | Conference.

Action Data: None.

Default Label: Conf or Conference Add.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support This function is only supported on Avaya M-Series and T-Series phones.

M-Series/T-Series: The button is equivalent to **Feature 3**.

Conference Add

Conference add controls can be used to place the user, their current call and any calls they have on hold into a conference. When used to start a new conference, the system automatically assigns a conference ID to the call. This is termed ad-hoc (impromptu) conferencing.

If the call on hold is an existing conference, the user and any current call are added to that conference. This can be used to add additional calls to an ad-hoc conference or to a meet-me conference. Conference add can be used to connect two parties together. After creating the conference, the user can drop from the conference and the two incoming calls remain connected.

For further details refer to the Conferencing section.

Action: Advanced | Call | Conference Add.

Action Data: None.

Default Label: Conf+ or Conference Add.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No

Table continues…

1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Conference Meet Me

Conference meet-me refers to features that allow a user or caller to join a specific conference by using the conference's ID number (either pre-set in the control or entered at the time of joining the conference).

Note:

Conference Meet Me features can create conferences that include only one or two parties. These are still conferences that are using resources from the host system's conference capacity.

Conference ID Numbers

By default, ad hoc conferences are assigned numbers starting from 100 for the first conference in progress. Therefore, for conference Meet Me features specify a number away from this range ensure that the conference joined is not an ad hoc conference started by other users. It is not possible to join a conference using conference Meet Me features when the conference ID is in use by an ad-hoc conference.

User Personal Conference Number Each user's own extension number is treated as their own personal conference number. Only that user is able to start a conference using that number as the conference ID. Any one else attempting to start a conference with that number will find themselves in a conference but on hold until the owner also joins. Personal conferences are always hosted on the owner's system.

Note:

When a user calls from their mobile twinned number, the personal conference feature will only work if they access the conference using an FNE 18 service.

Multi-Site Network Conferencing

Meet Me conference IDs are now shared across a multi-site network. For example, if a conference with the ID 500 is started on one system, anyone else joining conference 500 on any system will join the same conference. Each conference still uses the conference resources of the system on which it was started and is limited by the available conference capacity of that system.

Previously separate conferences, each with the same conference ID, could be started on each system in a multi-site network.

Other Features

Transfer to a Conference ButtonA currently connected caller can be transferred into the conference by pressing **TRANSFER**, then the Conference Meet Me button and **TRANSFER** again to complete the transfer. This allows the user to place callers into the conference specified by the button without being part of the conference call themselves. This option is only support on Avaya phones with a fixed **TRANSFER** button (excluding T3 and T3 IP phones).

Conference Button Status Indication When the conference is active, any buttons associated with the conference ID indicate the active state.

Details

Action: Advanced | Call | Conference Meet Me.

Action Data: Conference number. This can be an alphanumeric value up to 15 characters.

User Personal Conference Number Each user's own extension number is treated as their own personal conference number. Only that user is able to start a conference using that number as the conference ID. Any one else attempting to start a conference with that number will find themselves in a conference but on hold until the owner also joins. Personal conferences are always hosted on the owner's system.

Note:

When a user calls from their mobile twinned number, the personal conference feature will only work if they access the conference using an FNE18 service.

Default Label: CnfMM <conference number> or Conf. Meet Me <conference number>.

Toggles: No.

Status Indication: Yes

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Consult

Not supported. Provided for CTI emulation only.

Action: Emulation | Consult.

Action Data: None.

Default Label: Cnslt.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Coverage Appearance

Creates a button that alerts when a call to the specified covered user is unanswered after that users **Individual Coverage Timer** expires.

The call coverage appearance button user must also have at least one call appearance button programmed. The covered user does not need to be using call appearance buttons.

Coverage appearance functions, assigned to buttons that do not have status lamps or icons, are automatically disabled until the user logs in at a phone with suitable buttons.

IP Office: Appearance buttons can be set with a ring delay if required or to not ring. This does not affect the visual alerting displayed next to the button. The delay uses the user's Ring Delay (User | Telephony | Multi-line Options) setting.

Action: Appearance | Coverage Appearance.

Action Data: User name.

Default Label: <user name>.

Toggles: No.

Status Indication: Yes. See Coverage Button Indication.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** No	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes [1]
1200 Series: No	**3600 Series:** Yes	**4600 Series:** Yes	**9040:** Yes	**T-Series:** Yes [1]
1400 Series: Yes	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes	**3810:** Yes	**5600 Series:** Yes	**9600 Series:** Yes	

1. Not supported on T7000, T7100, M7100, M7100N and the Audio Conferencing Unit (ACU).

Dial

This action is used to dial the number contained in the Telephone Number field. A partial number can be enter for the user to complete. On buttons with a text label area, **Dial** followed by the number is shown.

Action Data: Telephone number or partial telephone number.

Default Label: Dial.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** Yes	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No [2]

Table continues…

1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. T3 Phones
   - **Classic/Comfort icon**: Displays the telephone number set.
   - **DSS Link LED**: None.

Dial 3K1

The call is presented to local exchange as a "3K1 Speech Call". Useful in some where voice calls cost less than data calls.

Action: Advanced | Dial | Dial 3K1.

Action Data: Telephone number.

Default Label: D3K1 or Dial 3K1.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Dial 56K

The call presented to local exchange as a "Data Call".

Action: Advanced | Dial | Dial 56K.

Action Data: Telephone number.

Default Label: D56K or Dial 56K.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Dial 64K

The call is presented to local exchange as a "Data Call".

Action: Advanced | Dial | Dial 64K.

Action Data: Telephone number.

Default Label: D64K or Dial 64K.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Dial CW

Call the specified extension number and force call waiting indication on if the extension is already on a call. The call waiting indication will not work if the extension called has multiple call appearance buttons in use.

Action: Advanced | Dial | Dial CW.

Action Data: User number.

Default Label: DCW or Dial Call Waiting.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Dial Direct

Automatic intercom functions allow you to call an extension and have the call automatically answered on speaker phone after 3 beeps. The extension called must support a handsfree speaker. If the extension does not have a handsfree microphone then the user must use the handset if they want to talk. If the extension is not free when called, the call is presented as a normal call on a call appearance button if available.

This feature can be used as part of handsfree announced transfers.

Action: Advanced | Dial | Dial Direct.

Action Data: User number or name or blank for entry when pressed.

If left blank, the **Dial Direct** button can be used with User buttons to specify the target.

Default Label: Dirct or Auto Intercom.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes
1100 Series: No	**2400 Series:** Yes [1]	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1200 Series: No	**3600 Series:** No	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1400 Series: Yes [1]		**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1600 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Dial Emergency

Dials the number specified regardless of any outgoing call barring applicable to the user.

Action: Advanced | Dial | Dial Emergency.

Action Data: Telephone number.

Default Label: Emrgy or Dial Emergency.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Dial Inclusion

This feature allows you to intrude on another user's call to talk to them. Their current call is put on hold while you talk and automatically reconnected when you end the intrusion. The intruder and the target extension can then talk but cannot be heard by the other party. This can include intruding into a conference call, where the conference will continue without the intrusion target.

During the intrusion all parties hear a repeated intrusion tone. When the intruder hangs-up the original call parties are reconnected. Attempting to hold a dial inclusion call simply ends the intrusion. The inclusion cannot be parked.

The ability to intrude and be intruded is controlled by two configuration settings, the Can Intrude (User | Telephony | Supervisor Settings) setting of the user intruding and the Cannot Be Intruded (User | Telephony | Supervisor Settings) setting of target being intruded on. The setting of any other internal party is ignored. By default, no users can intrude and all users are set to cannot be intruded.

The system support a range of other call intrusion methods in addition to this feature.

Action: Advanced | Dial | Dial Inclusion.

Action Data: User number or name or blank for user selection when pressed.

On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.

Default Label: Inclu or Dial Inclusion.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Dial Intercom

Automatic intercom functions allow you to call an extension and have the call automatically answered on speaker phone after 3 beeps. The extension called must support a handsfree speaker. If the extension does not have a handsfree microphone then the user must use the handset if they want to talk. If the extension is not free when called, the call is presented as a normal call on a call appearance button if available.

This feature can be used as part of handsfree announced transfers.

Action: Emulation | Dial Intercom.

Action Data: User number or name or blank for number entry when pressed.

On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.

Default Label: Idial or Auto Intercom.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   T3 Phones:

   - **Classic/Comfort icon**: Displays followed by the set number.
   - **DSS Link LED**: None.

   M-Series/T-Series: The button is equivalent to **Feature 66 <number>**.

Dial Paging

Makes a paging call to an extension or group specified. If no number is specified, this can be dialed after pressing the button. The target extension or group members must be free and must support handsfree auto-answer in order to hear the page.

On Avaya phones with a **CONFERENCE** button, a paged user can convert the page call into a normal call by pressing that button.

Action: Advanced | Dial | Dial Paging.

Action Data: User number or name or group number or name or blank for number entry when pressed.

Default Label: Page.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   T3 Phones:

   - **Classic/Comfort icon**: Displays 🕪 followed by target number if set.
   - **DSS Link LED**: None.

Dial Physical Extn by Number

Call the specified extension using its Base Extension number setting. This is regardless of the current user logged in at that extension and any forwarding, follow me or do not disturb settings applied by the extension user. This function requires the extension to be assigned a default extension number in the system configuration. If the extension does not have a default extension number, Dial Physical Extn by Id should be used.

Action: Advanced | Dial | Dial Physical Extn by Number.

Action Data: Extension port base extension number.

Default Label: PhyEx or Dial Physical Extn.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes

Table continues…

1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Dial Physical Number by ID

Call the specified extension, if free, regardless of the current user logged in at that extension and any forwarding, follow me or do not disturb settings applied by the extension user. This function uses the port ID shown in the system configuration.

Action: Advanced | Dial | Dial Physical Extn by Id.

Action Data: Extension port ID number.

Default Label: DialP or Dial Extn by Id.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Dial Speech

This feature allows a short code to be created to force the outgoing call to use the Speech bearer capability.

Action: Advanced | Dial | Dial Speech.

Action Data: Telephone number.

Default Label: DSpch or Dial Speech.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Dial V110

The call is presented to local exchange as a "Data Call".

Action: Advanced | Dial | Dial V110.

Action Data: Telephone number.

Default Label: DV110 or Dial V110.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Dial V120

The call is presented to local exchange as a "Data Call".

Action: Advanced | Dial | Dial V120.

Action Data: Telephone number.

Default Label: DV120 or Dial V120.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Display Msg

Allows the sending of text messages to digital phones on the local system.

Action: Advanced | Dial | Display Msg.

Action Data: The telephone number takes the format N";T" where:

- **N** is the target extension.
- **T** is the text message. Note that the **";** before the text and the **"** after the text are required.

Default Label: Displ.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Dial Video

The call is presented to the local exchange as a "Video Call".

Action: Advanced | Dial | Dial Video.

Action Data: Telephone number.

Default Label: Dvide or Dial Video.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Directed Call Pickup

Pickup a call ringing at a specific extension or hunt group.

Action: Emulation | Directed Pickup.

Action Data: User number or name or group number or name or blank for number entry when pressed.

On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.

Default Label: DpkUp or Call Pickup.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No [2]

Table continues…

1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   M-Series/T-Series: The button is equivalent to **Feature 76**.

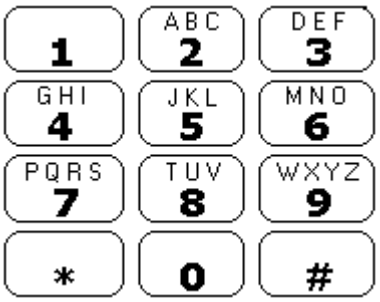
Directory

A **Dir** button provides access to various directories and allows telephone number selection by dialed name matching. The directories available for searching depend on the phone type, see User Directory Access. Once they user has selected a directory, dialing on the dial pad letter keys is used to display matching names, with controls for scrolling through the matching names and for calling the currently displayed name.

The method of name matching is controlled by the Dial by Name (System | Telephony | Telephony) setting in the system configuration:

- **With Dial By Name on** Matching is done against all the dial keys pressed. For example, dialing 527 matches names starting with JAS (for example "Jason") and KAR (for example "Karl"). Only the first 50 matches are displayed.
- **With Dial By Name off** Matching is done against the first letter only. For example pressing 5 displays names beginning with J. Press 5 again displays names beginning with K. Only the first 50 matches are displayed. This mode is not supported by Release 5.0+.

Name dialing functions on the system assume that the phone is using the standard ITU keypad as follows:



Dialing Spaces

To enter a name with a space, the 0 key is used for the space. For example "John S..." is dialed as 564607.

Details

Action: Emulation | Directory.

Action Data: None.

Default Label: Dir.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**3600 Series:** No	**5400 Series:** Yes [1]	**9040:** No	**T3/T3 IP Series:** Yes
1400 Series: No	**3700 Series:** No	**4600 Series:** Yes [1]	**9500 Series:** No	
1600 Series: Yes [1]	**3810:** Yes	**5600 Series**: Yes [1]	**9600 Series:** No	
20 Series: Yes	**4100 Series:** No	**6400 Series:** Yes	**M-Series:** Yes	
2400 Series: Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**T-Series:** Yes [1]	

1. Not 1603, 2402, 4601, 4602, 5402, 5601, 5602 and T7100 models.

T3 Phones:

- **Classic/Comfort icon**: Displays 🕮.
- **DSS Link LED**: None.

Do Not Disturb Exception Add

Adds a number to the user's "Do Not Disturb Exception List". This can be the number of an internal user or a number to match the CLI of a particular external caller.Calls from that number, except hunt group calls, will ignore the user's Do Not Disturb setting. For further details see Do Not Disturb (DND).

Action: Advanced | Do Not Disturb | Do Not Disturb Exception Add.

Action Data: Telephone number or CLI. Up to 31 characters. For CLI numbers any prefix added by the system must also be included.

Default Label: DNDX+.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Do Not Disturb Exception Delete

Removes a number from the user's "Do Not Disturb Exception List". This can be the number of an internal user or a number to match the CLI of a particular external caller.

Action: Advanced | Do Not Disturb | Do Not Disturb Exception Delete.

Action Data: Telephone number or CLI.

Default Label: DNDX-.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Do Not Disturb Off

Cancels the user's 'do not disturb' mode if set. This button function is obsolete as the do not disturb on function toggles on/off and indicates the button status.

Action: Advanced | Do Not Disturb | Do Not Disturb Off.

Action Data: None.

Default Label: DNDOf.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   M-Series/T-Series: The button is equivalent to **Feature #85**.

Do Not Disturb On

Enables the user's 'do not disturb' mode.

For CCR Agents, using this function button on the following phones will be requested the user to select a reason code - 1400, 1600, 2400, 4600, 5400, 5600, 9500 and 9600 Series phones with available programmable buttons.

Note:

CCR is not supported in IP Office release 9.1 and later.

Action: Advanced | Do Not Disturb | Do Not Disturb On.

Action Data: None.

Default Label: DNDOn or Do Not Disturb.

Toggles: Yes.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   M-Series/T-Series: The button is equivalent to **Feature 85**.

Drop

This action is supported on phones which do not have a permanent **Drop** button.

For a currently connected call, pressing **Drop** disconnects the call. When drop is used to end a call, silence is returned to the user rather than dial tone. This is intended operation, reflecting that **Drop** is mainly intended for use by call center headset users.

If the user has no currently connected call, pressing **Drop** will redirect a ringing call using the user's **Forward on No Answer** setting if set or otherwise to voicemail if available.

For a conference call, on phones with a suitable display, **Drop** can be used to display the conference parties and allow selection of which party to drop from the conference.

Action: Emulation | Drop.

Action Data: None.

Default Label: Drop or Drop Call.

Toggles: No.

Status Indication: No.

User Admin: ✓.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** No	**D100:** No
1100 Series: No	**2400 Series:** No	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** Yes	**5400 Series:** Yes	**9040:** Yes	**T-Series:** No
1400 Series: No	**3700 Series:** No	**4600 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: No	**3810:** Yes	**5600 Series:** Yes	**9600 Series:** Yes	

Extn Login

Extn Login allows a user who has been configured with a **Login Code** (User | Telephony | Supervisor Settings) to take over ownership of any extension. That user's extension number becomes the extension number of the extension while they are logged. This is also called ‘hot desking’.

Hot desking is not supported for H175, E129 and J129 telephones.

When used, the user is prompted to enter their extension number and then their log in code. Login codes of up to 15 digits are supported with **Extn Login** buttons. Login codes of up to 31 digits are supported with **Extn Login** short codes.

When a user logs in, as many of their user settings as possible are applied to the extension. The range of settings applied depends on the phone type and on the system configuration.

By default, on 1400 Series, 1600 Series, 9500 Series and 9600 Series phones, the user's call log and personal directory are accessible while they are logged in. This also applied to M-Series and T-Series telephones.

On other types of phone, those items such as call logs and speed dials are typically stored locally by the phone and will not change when users log in and log out.

If the user logging in was already logged in or associated with another phone, they will be automatically logged out that phone.

Action: Advanced | Extension | Extn Login.

Action Data: None.

Default Label: Login.

Toggles: Yes.

Status Indication: Yes.

Status	2400, 5400 Series	4600, 5600 Series	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	T-Series, M-Series
- On.	**<Label>**	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Extn Logout

Logs out a user from the phone. The phone will return to its normal default user, if an extension number is set against the physical extension settings in the configuration. Otherwise it takes the setting of the **NoUser** user. This action is obsolete as Extn Login can be used to log out an existing logged in user.

If the user who logged out was the default user for an extension, dialing *36 will associate the extension with the user unless they are set to forced log in.

This feature cannot be used by a user who does not have a log in code.

Action: Advanced | Extension | Extn Logout.

Action Data: None.

Default Label: Logof or Logout.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. May have limited support on some specific T3 phone models if detailed below.

Flash Hook

Sends a hook flash signal to the currently connected line if that line is an analog line.

Action: Advanced | Miscellaneous | Flash Hook.

Action Data: Optional. Normally this field is left blank. It can contain the destination number for a Centrex Transfer for external calls on a line from a Centrex service provider.

Default Label: Flash or Flash Hook.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No

Table continues…

1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Follow Me Here

Causes calls to the extension number specified, to be redirected to this user's extension. User's with a log in code will be prompted to enter that code when using this function.

Action: Advanced | Follow Me | Follow Me Here.

Action Data: User name or user number.

If a user name or user number has been entered in the **Action Data** field, when the interactive menu opens, press `Enter`to activate Follow Me Here for the number displayed on the screen.

This field can be left blank for number entry when pressed.

On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.

Default Label: Here+ or Follow Me Here.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

T3 Phones:

- **Classic/Comfort icon**: Displays followed by the user name.
- **DSS Link LED**: On when active.

Follow Me Here Cancel

Cancels any 'Follow Me Here' set on the specified extension. Only works if entered at the extension to which the extension's calls are being sent by the follow me action.

Action: Advanced | Follow Me | Follow Me Here Cancel.

Action Data: User number or blank for number entry when pressed.

If a user name or user number has been entered in the **Action Data** field, when the interactive menu opens, press `Enter`to deactivate Follow Me Here for the number displayed on the screen.

On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.

Default Label: Here- or Follow Me Here-.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Follow Me To

Leaving the extension blank prompts the user to enter the extension to which their calls should be redirected. User's with a log in code will be prompted to enter that code when using this function.

Action: Advanced | Follow Me | Follow Me To.

Action Data: User name or user number or blank for number entry when pressed.

If a user name or user number has been entered in the **Action Data** field, when the interactive menu opens, press `Enter`to activate Follow Me To for the number displayed on the screen.

On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.

Default Label: FolTo or Follow Me To.

Toggles: Yes.

Status Indication: Yes. On/off status indication is provided if the button is programmed with a user name or number.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>** ◀	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	▲ On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Forward Hunt Group Calls Off

Cancels the forwarding of the user's hunt group calls. This function is obsolete since the button function Forward Hunt Group Calls On toggles on/off and indicates status.

Action: Advanced | Forward | Forward Hunt Group Calls Off.

Action Data: None.

Default Label: FwdH-.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Forward Hunt Group Calls On

Forward the user's hunt group calls (internal and external). This function only works when forward unconditional is also on and uses the same forwarding number as forward unconditional.

This option is only applied for calls to **Sequential** and **Rotary** type hunt groups. Calls from other hunt group types are not presented to the user when they have Forward Unconditional active. Note also that hunt group calls cannot be forwarded to another hunt group.

Action: Advanced | Forward | Forward Hunt Group Calls On.

Action Data: None.

Default Label: FwdH+ or Fwd HG Calls.

Toggles: Yes.

Status Indication: Yes.

Status	2400, 5400 Series	4600, 5600 Series	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	T-Series, M-Series
- On.	**<Label>**	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Forward Number

Sets the number to which calls are forwarded when the user has forwarding on. Used for all forwarding options unless a separate **Forward On Busy Number** is also set. Forwarding to an external number is blocked if **Inhibit Off-Switch Transfers** is selected within the system configuration.

Action: Advanced | Forward | Forward Number.

Action Data: Telephone number.

The field to be left blank to prompt the user for entry when the button is pressed. If blank, users with a log in code will be prompted to enter that code.

On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.

Default Label: FwdNo or Fwd Number.

Toggles: No.

Status Indication: Yes. For a button with a prefixed number, status indication will indicate when that number matches the users current set number. For a button with a no number, status indication will show when a number has been set.

Status	2400, 5400 Series	4600, 5600 Series	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	T-Series, M-Series
- On.	**<Label>**	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Forward On Busy Number

Sets the number to which calls are forwarded when using 'Forward on Busy' and/or 'Forward on No Answer'. Forwarding to an external number is blocked if **Inhibit Off-Switch Transfers** is selected within the system configuration.

Action: Advanced | Forward | Forward on Busy Number.

Action Data: Telephone number.

The field to be left blank to prompt the user for entry when the button is pressed. If blank, users with a log in code will be prompted to enter that code.

On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.

Default Label: FwBNo or Fwd Busy Number.

Toggles: No.

Status Indication: Yes. For a button with a prefixed number, status indication will indicate when that number matches the users current set number. For a button with a no number, status indication will show when a number has been set.

Status	2400, 5400 Series	4600, 5600 Series	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	T-Series, M-Series
- On.	**<Label>**	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Forward On Busy Off

Switches forward on busy off. This button function is obsolete, as Forward On Busy On can be used to switch forward on busy on/off and provides status indication.

Action: Advanced | Forward | Forward on Busy Off.

Action Data: None.

Default Label: FwBOf.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗

Table continues…

1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Forward On Busy On

Enables forwarding when the user's extension is busy. For users with call appearance buttons, they will only return busy when all call appearance buttons are in use. Uses the **Forward Number** as its destination unless a separate **Forward on Busy Number** is set.

Forward Internal (**User | Forwarding**) can also be used to control whether internal calls are forwarded.

Action: Advanced | Forward | Forward on Busy On.

Action Data: None.

Default Label: FwBOn or Fwd Busy.

Toggles: Yes.

Status Indication: Yes.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J69, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>** ◀	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	▲ On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Forward On No Answer Off

Switches forward on no answer off. This button function is obsolete, as Forward On No Answer On can be used to switch forward on no answer on/off and provides status indication.

Action: Advanced | Forward | Forward on No Answer Off.

Action Data: None.

Default Label: FwNOf.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Forward On No Answer On

Switches forward on no answer on/off. The time used to determine the call as unanswered is the user's no answer time. Uses the **Forward Number** as its destination unless a separate **Forward on Busy Number** is set.

Forward Internal (**User | Forwarding**) can also be used to control whether internal calls are forwarded.

Action: Advanced | Forward | Forward on No Answer On.

Action Data: None.

Default Label: FwNOn or Fwd No Answer.

Toggles: Yes.

Status Indication: Yes.

Status	2400, 5400 Series	4600, 5600 Series	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	T-Series, M-Series
- On.	**<Label>**	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Forward Unconditional Off

Switch 'forward all calls' off. This does not affect 'Forward on No Answer' and/or 'Forward on Busy' if also on. This function is obsolete as a button set to Forward Unconditional On toggles on/off and indicates when on.

Action: Advanced | Forward | Forward Unconditional Off.

Action Data: None.

Default Label: FwUOf.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗

Table continues…

1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Forward Unconditional On

This function is also known as 'divert all' and 'forward all'. It forwards all calls, except hunt group and page calls, to the forward number set for the user's extension. To also forward hunt group calls to the same number 'Forward Hunt Group Calls On' must also be used.

Forward Internal (**User | Forwarding**) can also be used to control whether internal calls are forwarded.

In addition to the lamp indication shown below, most phones display **D** when forward unconditional is on.

Action: Advanced | Forward | Forward Unconditional On.

Action Data: None.

Default Label: FwUOn or Fwd Unconditional.

Toggles: Yes.

Status Indication: Yes.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>** ◀	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	▲ On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗ [2]

Table continues…

1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   T3 Phones:

   - **Classic/Comfort icon**: Displays followed by the user name.
   - **DSS Link LED**: On when active.

   M-Series/T-Series: The button is equivalent to **Feature 4 <number>**.

Group

Monitors the status of a hunt group queue. This option is only supported for hunt groups with queuing enabled. The user does not have to be a member of the group.

Depending on the users button type, indication is given for when the group has alerting calls and queued calls (queued in this case is defined as more calls waiting than there are available group members).

Pressing a **Group** button answers the longest waiting call.

The definition of queued calls include group calls that are ringing. However, for operation of the **Group** button, ringing calls are separate from other queued calls.

Action: Group.

Action Data: Group name enclosed in " " double-quotes or group number.

Default Label: <group name>.

Toggles: No.

Status Indication: Yes, Required.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- No calls	**Main**	**Main**	Off	Off	Off	Grey	Off
- Call alerting	**Main** ◆	**Main** ◆	Green flash	Red flash	Green flash	Blue	▲ Slow flash
- Calls queued	**Main**	**Main**	Red flash	**Red on**	Red flash	**Green**	▲ Slow flash

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** Yes	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Group Listen On

Using group listen allows callers to be heard through the phone's handsfree speaker but to only hear the phone's handset microphone. This enables listeners at the user's phone to hear the connected party whilst limiting the connected party to hear only what is communicated via the phone handset

When group listen is enabled, it modifies the handsfree functionality of the user's phone in the following manner

When the user's phone is placed in handsfree/speaker mode, the speech path from the connected party is broadcast on the phone speaker but the phone's base microphone is disabled.

The connected party can only hear speech delivered via the phone's handset microphone.

Group listen is not supported for IP phones or when using a phone's **HEADSET** button.

For T-Series and M- Series phones, this option can be turned on or off during a call. For other phones, currently connected calls are not affected by changes to this setting, instead group listen must be selected before the call is connected.

Group listen is automatically turned off when the call is ended.

Action: Advanced | Extension | Group Listen On.

Action Data: None.

Default Label: Group Listen On.

Toggles: Yes.

Status Indication: Yes.

Status	2400, 5400 Series	4600, 5600 Series	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	T-Series, M-Series
- On.	**<Label>**	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✗	**4100 Series:** ✗	**6400 Series:** ✓	**96x1 Series:**✓
1100 Series: ✗	**2400 Series:** ✓	**4400 Series:** ✓	**7400 Series:** ✗	**D100:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓	**9040:** ✗	**M-Series:** ✓ [2]
1400 Series: ✓[1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T-Series:** ✓ [2]
1600 Series: ✓	**3810:** ✗	**5600 Series:** ✓	**9600 Series:** ✗	**T3/T3 IP Series:** ✗

1. Not 1403.
2. M-Series/T-Series: The button is equivalent to **Feature 802** (On) and **Feature #802** (Off).

Group Paging

Makes a paging call to an extension or group specified. If no number is specified, this can be dialed after pressing the button. The target extension or group members must be free and must support handsfree auto-answer in order to hear the page.

On Avaya phones, a paged user can convert the page call into a normal call by pressing the **Conference** button.

Action: Emulation | Group Paging.

Action Data: User number or name or group number or name.

On large display phones, if configured without a preset target, this type of button will display an interactive button menu for target selection.

Default Label: GrpPg.

Toggles: No.

Status Indication: Yes.

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** Yes
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** ✓	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   T3 Phones:

   - **Classic/Comfort icon**: Displays 🕪 followed by target number if set.
   - **DSS Link LED**: None.

   M-Series/T-Series: The button is equivalent to **Feature 60 <number>**.

Headset Toggle

This function is intended for use with Avaya phones that have separate handset and headset sockets but do not provide a dedicated Headset button, for example older style 4400 Series and 4600 Series phones. On phones without a headset socket or with a dedicated headset button this control will have no effect.

Action: Miscellaneous | Headset Toggle.

Action Data: None.

Default Label: HdSet.

Toggles: Yes.

Status Indication: Yes.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✗	**T3/T3 IP Series:** ✓ [2]
1400 Series: ✗	**3700 Series:** ✗	**5400 Series:** ✗	**9500 Series:** ✗	

Table continues…

1600 Series: ✗	**3810:** ✗	**5600 Series:** ✗	**9600 Series:** ✗	
20 Series: ✗	**4100 Series:** ✗	**6400 Series:** ✗	**M-Series:** ✗	
2400 Series: ✗	**4400 Series:** ✓	**7400 Series:** ✗	**T-Series:** ✗	

1. 4606, 4612 and 4624 only.
2. T3 Phones
   - **Classic/Comfort icon**: Displays **HdSet**.
   - **DSS Link LED**: On when active.

:

Hold Call

This uses the Q.931 Hold facility, and "holds" the incoming call at the ISDN exchange, freeing up the ISDN B channel. The Hold Call feature "holds" the current call to a slot. The current call is always automatically placed into slot 0 if it has not been placed in a specified slot. Only available if supported by the ISDN exchange.

Action: Advanced | Hold | Hold Call.

Action Data: ISDN Exchange hold slot number or blank (slot 0).

Default Label: Hold.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Hold CW

Place the user's current call on hold and answers the waiting call. This function is not supported on phones which have multiple call appearance buttons set.

Action: Advanced | Hold | Hold CW.

Action Data: None.

Default Label: HoldCW.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Hold Music

This feature allows the user to listen to the system's music on hold. See Music On Hold for more information.

Action: Advanced | Hold | Hold Music.

Action Data: Optional. Systems can support multiple hold music sources. However only the system source is supported for **Hold Music** buttons.

Default Label: Music or Hold Music.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Hunt Group Enable

An individual users membership of any particular hunt groups is programmed through the system configuration. This control allows the user to enable or disable that membership. While enabled, the user can receive hunt group calls when logged in.

In addition to the lamp indication below, phones display **G** when any group membership is enabled.

Action: Advanced | Hunt Group | Hunt Group Enable.

Action Data: Group number or name or blank for all groups of which the user is a member.

Default Label: HGEna or HG Enable.

Toggles: Yes.

Status Indication: Yes. Required.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>** ◀	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	▲ On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓

Table continues…

1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗ [2]
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   T3 Phones:

   - **Classic/Comfort icon**: Displays [🔔] followed by the group number or * for all if programmed with no specific group number.
   - **DSS Link LED**: On when active.

Hunt Group Disable

This function is obsolete, the Hunt Group Enable function being able to toggle membership between enabled and disabled and providing lamp indication of when membership is enabled.

An individual user's membership of any particular hunt groups is programmed through the system configuration. This control allows the user to disable that membership. They will no longer receive calls to that hunt group until their membership is enabled again.

Action: Advanced | Hunt Group | Hunt Group Disable.

Action Data: Group number or blank for all groups of which the user is a member.

Default Label: HGDis.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Inspect

Not supported. Provided for CTI emulation only. Allows users on display phones to determine the identification of held calls. Allows users on an active call to display the identification of incoming calls.

Action: Emulation | Inspect.

Action Data: None.

Default Label: Inspt.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Internal Auto-Answer

This function is also known as handsfree auto-answer. It sets the user's extension to automatically connect internal calls after a single tone. This function should only be used on phones that support handsfree operation.

Action: Emulation | Internal Auto-Answer.

Action Data: Optional.

- If left blank this function acts as described above for internal auto-answer.
- **FF** can be entered. In that case the button will enable/disable headset force feed operation for external calls. In this mode, when headset mode is selected but the phone is idle, an incoming external call will cause a single tone and then be automatically connected. This operation is only supported on Avaya phones with a fixed **HEADSET** button. Ring delay is applied if set on the appearance button receiving the call before the call is auto-connected.

Default Label: HFAns or Auto Answer.

Toggles: Yes.

Status Indication: Yes. Required.

Status	2400, 5400 Series	4600, 5600 Series	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	T-Series, M-Series
- On.	**<Label>**	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗ [2]
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   T3 Phones:

   - **Classic/Comfort icon**: Displays **HFAns**.
   - **DSS Link LED**: On when active.

Last Number Redial

This function is intend for use with Avaya M-Series and T-Series phones only. When pressed, the button invokes the same last number redial process as dialing **Feature 5**.

Action: Advanced | Call | Last Number Redial.

Action Data: None.

Default Label: Again.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support This function is only supported on Avaya M-Series and T-Series phones.

M-Series/T-Series: The button is equivalent to **Feature 5**.

Leave Word Calling

Not supported. Provided for CTI emulation only. Leaves a message for the user associated with the last number dialed to call the originator.

Action: Emulation | Leave Word Calling.

Action Data: None.

Default Label: LWC.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Line Appearance

Creates an line appearance button linked to the activity of a specified line appearance ID number. The button can then be used to answer and make calls on that line.

The line appearance button user must also have at least one call appearance button programmed before line appearance buttons can be programmed.

Line appearance functions, assigned to buttons that do not have status lamps or icons, are automatically disabled until the user logs in at a phone with suitable buttons.

Release 3.2+: Appearance buttons can be set with a ring delay if required or to not ring. This does not affect the visual alerting displayed next to the button. The delay uses the user's Ring Delay (User | Telephony | Multi-line Options) setting.

Release 4.2+: Line appearances are supported on T3 and T3 IP phones. These phones do not require (or support) call appearance buttons in order to use line appearances.

Action: Appearance | Line Appearance.

Action Data: Line ID number.

Default Label: Line <Line ID number>.

Toggles: No.

Status Indication: Yes. See Line Appearance Button Indication.

User Admin: No.

Phone Support: The following table indicates phones which support the programmable button:

Analog: ✗	**20 Series:** ✗	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓ [1]
1200 Series: ✗	**3600 Series:** ✓	**4600 Series:** ✓	**9040:** ✓	**T-Series:** ✓ [1]
1400 Series: ✓	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓	**3810:** ✓	**5600 Series:** ✓	**9600 Series:** ✓	

1. Not supported on T7000, T7100, M7100, M7100N and the Audio Conferencing Unit (ACU).

MADN Call Appearance

With the Multiple Appearance Directory Number (MADN) feature, a Directory Number (DN) can be configured to appear on more than one telephone. You can have up to 30 appearances of the same DN. These appearances can be on single-line or multiline telephones. MADN is an Avaya Communication Server 1000 key and lamp style feature.

To use MADN features in IP Office environment, the MADN number must be configured as one of the user’s number. The user associated with the MADN number does not need to have a license or an active extension. However, the user must have an extension number for the feature to work. The system considers the user’s records when the user makes a call using the MADN buttons.

- MADN Single Call Appearance (SCA)

  The core behavior of Bridge Appearance to a MADN user emulates MADN Single Call Appearance by providing the following behaviors for incoming and outgoing calls:

  - For incoming calls, the button offers Birdge Appearance like behavior to the specified MADN Number.

- For outgoing calls, the button offers Call Appearance like behavior that presents the call as originating from the user but with the MADN Number and the name of the user in the calling party information.

- MADN Multiple Call Appearance (MCA)

  The core behavior of Coverage Appearance to a MADN user emulates MADN Multiple Call Appearance by providing the following behaviors for incoming and outgoing calls:

  - For incoming calls, the button offers Coverage Appearance like behavior to the specified MADN Number.
  - For outgoing calls, the button offers Call Appearance like behavior that presents the call as originating from the user but with the MADN Number in the calling party information.

Action Any one of the following:

- Appearance | MADN Single Call Appearance
- Appearance | MADN Multiple Call Appearance

Action Data:

- MADN Single Call Appearance: User Name, Call Appearance button number and Ring Delay.
- MADN Multiple Call Appearance: User Name and Ring Delay.

Default Label:

- MADN SCA: <MADN number S=>
- MADN MCA: <MADN number M=>

Toggles: No.

Status Indication:

- MADN SCA: Yes. See Bridge Appearance Button Indication.
- MADN MCA: Yes. See Coverage Button Indication.

User Admin: No.

Phone Support: The following table indicates phones which support the programmable button:

Analog: ✗	**20 Series:** ✗	**4100 Series:** ✗	**6400 Series:** ✗	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✗	**4400 Series:** ✗	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✗	**9040:** ✗	**T-Series:** ✗
1400 Series: ✓	**3700 Series:** ✗	**5400 Series:** ✗	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓	**3810:** ✗	**5600 Series:** ✗	**9600 Series:** ✓	

MCID Activate

This action is used with ISDN Malicious Caller ID call tracing. It is used to trigger a call trace at the ISDN exchange. The call trace information is then provided to the appropriate legal authorities.

This option requires the line to the ISDN to have MCID enabled at both the ISDN exchange and on the system. The user must also be configured with **Can Trace Calls** (**User | Telephony | Supervisor Settings**) enabled.

Note:

Currently, in Server Edition network, MCID is only supported for users using an MCID button and registered on the same IP500 V2 Expansion system as the MCID trunks.

Action: Advanced | Miscellaneous | MCID Activate.

Action Data: None.

Default Label: MCID or Malicious Call.

Toggles: No.

Status Indication: Yes.

User Admin: No.

Phone Support: Note that support for particular phone models is also dependant on the system software level.

Analog: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T3/T3 IP Series:** No
1400 Series: Yes	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	
20 Series: No	**4100 Series:** No	**6400 Series:** No	**M-Series:** Yes	
2400 Series: Yes	**4400 Series:** Yes	**7400 Series:** No	**T-Series:** Yes	

1. Not 1603, 4601, 4602, 5601 and 5602.

Monitor Analogue Trunk MWI

Enables a user to receive message waiting indicator (MWI) signals from analog trunks terminating on the ATM4U-V2 card. MWI is a telephone feature that turns on a visual indicator on a telephone when there are recorded messages.

Action: Advanced | Voicemail | Monitor Analogue Trunk MWI.

Action Data: The line appearance ID of the analog line for which MWI will be received.

Default Label: Trunk MWI.

Toggles: No.

Status Indication: No.

User Admin: No.

Off Hook Station

Enables the user's extension to be controlled by an application, for example SoftConsole. Calls can then be answered and cleared through the application without having to manually go off or on hook. Requires the phone to support full handsfree operation.

Action: Advanced | Miscellaneous | Off Hook Station.

Action Data: None.

Default Label: OHStn.

Toggles: Yes.

Status Indication: Yes.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>**	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T3/T3 IP Series:** ✗
1400 Series: ✓	**3700 Series:** ✗	**5400 Series:** ✓ [1]	**9500 Series:** ✓	
1600 Series: ✓	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	
20 Series: ✓	**4100 Series:** ✗	**6400 Series:** ✓	**M-Series:** ✓	
2400 Series: ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**T-Series:** ✓	

1. Not 2402, 4601, 4602, 5402, 5601 and 5602 models.

Pause Recording

This feature can be used to pause any call recording. It can be used during a call that is being recorded to omit sensitive information such as customer credit card information. This feature can be used with calls that are recorded both manually or calls that are recorded automatically.

The button status indicates when call recording has been paused. The button can be used to restart call recording. The system **Auto Restart Paused Recording** (System | Voicemail) setting can be used to set a delay after which recording is automatically resumed.

If the voicemail system is configured to provide advice of call recording warnings, then pausing the recording will trigger a "Recording paused" prompt and a repeat of the advice of call recording warning when recording is resumed.

Action: Advanced | Call | Pause Recording.

Action Data: None.

Default Label: PauseRec or Pause Recording.

Toggles: Yes.

Status Indication: Yes.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✗	**4100 Series:** ✗	**6400 Series:** ✗	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✗	**4400 Series:** ✗	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✗	**9040:** ✗	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✗	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✗	**5600 Series:** ✗	**9600 Series:** ✓	

1. Not 1403, 1603.

Priority Call

This feature allows the user to call another user even if they are set to 'do not disturb'. A priority call will follow forward and follow me settings but will not go to voicemail.

Action: Advanced | Call | Priority Call.

Action Data: User number or name.

Default Label: PCall or Priority Call.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support: The following table indicates phones which support the programmable button:

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Priority Calling

Not supported. Provided for CTI emulation only.

Action: Emulation | Priority Calling.

Action Data: None.

Default Label: Pcall.

Toggles: No.

Status Indication: No.

Phone Support: The following table indicates phones which support the programmable button:

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Private Call

When on, any subsequent calls cannot be intruded on until the user's private call status is switched off. The exception is Whisper Page which can be used to talk to a user on a private call.

Note that use of private calls is separate from the user's intrusion settings. If the user's **Cannot be Intruded** (User | Telephony | Supervisor Settings) setting is enabled, switching private calls off does not affect that status. To allow private calls to be used to fully control the user status, **Cannot be Intruded** (User | Telephony | Supervisor Settings) should be disabled for the user.

If enabled during a call, any current recording, intrusion or monitoring is ended.

Action: Advanced | Call | Private Call.

Action Data: None.

Default Label: PrivC or Private Call.

Toggles: Yes.

Status Indication: Yes.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>**	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✗	**4100 Series:** ✗	**6400 Series:** ✗	**D100:** ✓
1100 Series: ✓	**2400 Series:** ✓	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✓	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1603, 4601, 4602, 5601 and 5602.

Relay Off

Opens the specified switch in the system's external output port (**EXT O/P**).

This feature is not supported on Linux based systems. For Server Edition, this option is only supported on Expansion System (V2) units.

Action: Advanced | Relay | Relay Off.

Action Data: Switch number (1 or 2).

Default Label: Rely-.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Relay On

Closes the specified switch in the system's external output port (**EXT O/P**).

This feature is not supported on Linux based systems. For Server Edition, this option is only supported on Expansion System (V2) units.

Action: Advanced | Relay | Relay On.

Action Data: Switch number (1 or 2).

Default Label: Rely+ or Relay On.

Toggles: Yes.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✓
1100 Series: ✓	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✓	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗

Table continues…

1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Relay Pulse

Closes the specified switch in the system's external output port (**EXT O/P**) for 5 seconds and then opens the switch.

This feature is not supported on Linux based systems. For Server Edition, this option is only supported on Expansion System (V2) units.

Action: Advanced | Relay | Relay Pulse.

Action Data: Switch number (1 or 2).

Default Label: Relay or Relay Pulse.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✓
1100 Series: ✓	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✓	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗ [12]
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   T3 Phones:

   - **Classic/Comfort icon**: Displays **S1** or **S2** dependant on switch number.
   - **DSS Link LED**: None.

Resume Call

Resume a call previously suspended to the specified ISDN exchange slot. The suspended call may be resumed from another phone/ISDN Control Unit on the same line.

Action: Advanced | Call | Resume Call.

Action Data: ISDN Exchange suspend slot number.

Default Label: Resum.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Request Coaching Intrusion

This feature allows a user to request that another user intrude on a call and talk to them without being heard by the other call parties to which they can still talk.

The ability to intrude and be intruded is controlled by two configuration settings, the Can Intrude (User | Telephony | Supervisor Settings) setting of the user intruding and the Cannot Be Intruded (User | Telephony | Supervisor Settings) setting of target being intruded on. The setting of any other internal party is ignored. By default, no users can intrude and all users are set to cannot be intruded.

Warning:

The use of features to listen to a call without the other call parties being aware of that monitoring may be subject to local laws and regulations. Before enabling the feature you must ensure that you have complied with all applicable local laws and regulations. Failure to do so may result in severe penalties.

The system support a range of other call intrusion methods in addition to this feature.

Action: Advanced | Call | Request Coaching Intrusion.

Action Data: None.

Default Label: Request Coach or Request Coaching Intrusion.

Toggles: Yes.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✗	**4100 Series:** ✗	**6400 Series:** ✗	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✗	**4400 Series:** ✗	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✗	**9040:** ✗	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✗	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✗	**5600 Series:** ✗	**9600 Series:** ✓	

1. Not 1403, 1603.

The Request Coaching Intrusion feature exhibits the following behavior:

- A coaching request can be sent to a user or a group.
- While the request is pending, the user can cancel the request by pressing the Request Coach button again.
- Once a coaching session is established, the user that initiated the request can include the coach in the call, transfer the call to the coach, or drop the coach from the call.
- Once a coaching session is established, the coach can join the call or steal the call. The coach cannot transfer or conference the call.
- Once the primary call ends, the coaching call continues.

Retrieve Call

Retrieves a call previously held to a specific ISDN exchange slot. Only available when supported by the ISDN exchange.

Action: Advanced | Call | Retrieve Call.

Action Data: Exchange hold slot number.

Default Label: Retriv.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: Yes	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: Yes	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** ✓	**T-Series:** No
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Ring Back When Free

Sets a ringback on the extension being called. When the target extension ends its current call, the ringback users is rung (for their set No Answer Time) and if they answer, a new call is made to the target extension.

Ringback can be cleared using the Cancel Ring Back When Free function.

Action: Advanced | Miscellaneous | Ring Back When Free.

Action Data: None.

Default Label: AutCB or Auto Callback.

Toggles: No.

Status Indication: Yes.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>** ◀	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	▲ On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗ [2]
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

Ringer Off

Switches the phone's call alerting ring on/off.

Action: Emulation | Ringer Off.

Action Data: None.

Default Label: RngOf or Ringer Off.

Toggles: Yes.

Status Indication: Yes Required.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>** ◀	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	▲ On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Self-Administer

Allows a user to program features against other programmable buttons themselves.

Appearance can no longer be used to create call appearance buttons. Similarly, existing call appearance button cannot be overwritten using any of the other Admin button functions.

User's with a log in code will be prompted to enter that code when they use this button action.

T3 phone users can access a similar set of functions for button programming, see T3 Phone Self-Administration.

On 4412D+, 4424D+, 4612IP, 4624IP, 6408D, 6416D, 6424D phones:

- **Admin** can be permanently accessed via **Menu**, ▶, ▶, Admin. See Using a Menu Key.
- **Admin1** can be permanently accessed via **Menu**, Menu, ▶, **ProgA**, ▶, **DSS**.

Action: Emulation | Self-Administer.

Action Data: See below.

Value	T-Series and M-Series phones	Other Phones
None	The Feature *3 process is started with an alternate set of possible functions.	If no value is set, the button allows user programming of the following emulation actions. Abbreviated Dial. Abbreviated Dial Program. Account Code Entry. AD Suppress. Automatic Callback. Break Out. Call Forwarding All. Call Park. Call Park and Page Call Park To Other Extension Call Pickup. Call Pickup Any Conference Meet Me Dial Paging Directed Call Pickup. Directory. Drop. Group Paging. Headset Toggle. Hook Flash. Internal Auto-Answer. Ringer Off. Self-Administer. Send All Calls. Set Absent Text Set Hunt Group Night Service. Time of Day. Timer. Twinning
1	The **Feature *1** process is started for assigning **Abbreviated Dial** button.	If **1** is entered as the telephone number, allows user programming of the following system functions. Abbreviated Dial. Group. CPark. User. Flash Hook.

Table continues…

Value	T-Series and M-Series phones	Other Phones
2	The Feature ***6** process is started for setting the ring type.	If **2** is entered, the button can be used for viewing details of the control unit type and its software version. This option is available. If the user has a log in code set, they will be prompted to enter that code. System phone users can also use the button to manually set the system's date and time.
3	The option **3** is used with M-Series and T-Series sets to enable display contrast control.	Not used.

Default Label: Admin or Self Administer.

Toggles: No.

Status Indication: No.

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T3/T3 IP Series:** ✓ [2]
1400 Series: ✓	**3700 Series:** ✗	**5400 Series:** ✓ [1]	**9500 Series:** ✓	
1600 Series: ✓	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	
20 Series: ✓	**4100 Series:** ✗	**6400 Series:** ✓	**M-Series:** ✓	
2400 Series: ✓	**4400 Series:** ✓	**7400 Series:** ✗	**T-Series:** ✓	

1. Not 1403, 1603, 2402, 5402, 4601, 4602, 5601 and 5602.
2. See T3 Phone Self-Administration.

Send All Calls

Sets the user's extension into 'Do Not Disturb' mode. Callers, other than those on the user's do not disturb exception list, receive busy or are diverted to the users voicemail mailbox. Note that with a call already connected and other calls already alerting, enabling Do Not Disturb will not affect those calls already existing. For full details of see Do Not Disturb.

When on, most phones display an **N** on the display. This function and the Do Not Disturb On function work in parallel, ie. setting one sets the other.

Action: Emulation | Send All Call.

Action Data: None.

Default Label: SAC or Send All Calls.

Toggles: Yes.

Status Indication: Yes.

Status	2400, 5400 Series	4600, 5600 Series	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	T-Series, M-Series
- On.	**<Label>**	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗ [2]
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   T3 Phones:

   - **Classic/Comfort icon**: Displays **[ ]**.
   - **DSS Link LED**: On when active.

Set Absent Text

This feature can be used to select the user's current absence text. This text is then displayed to internal callers who have suitable display phones or applications. It doesn't changes the users status. The absence text message is limited to 128 characters. Note however that the amount displayed will depend on the caller's device or application.

The text is displayed to callers even if the user has forwarded their calls or is using follow me. Absence text is supported across a multi-site network.

Note:

The user still has to select **Set** or **Clear** on their phone to display or hide the text.

Action: Advanced | Set | Set Absent Text.

Action Data: Optional.

Note:

On certain phones (1400, 1600, 9500 and 9600), if the button is set without any Action Data, the user is prompted to select their absence text and switch it on/off through a menu shown on the phone display.

The telephone number should take the format "**y,n,text**" where:

- **y** = 0 or 1 to turn this feature off or on repesctively.
- **n** = the number of the absent statement to use:

0 = None.	4 = Meeting until.	8 = With cust. til.
1 = On vacation until.	5 = Please call.	9 = Back soon.
2 = Will be back.	6 = Don't disturb until.	10 = Back tomorrow.
3 = At lunch until.	7 = With visitors until.	11 = Custom.

text = any text to follow the absent statement..

Default Label: Absnt or Absence Text.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** ✓	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** No	**5400 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**4600 Series:** Yes [1]	**9500 Series:** Yes	**T3/T3 IP Series:** No
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 2402, 4601, 4602, 5402, 5601 and 5602.

Set Account Code

Dials an account code and then returns dial tone for the user to dial a number. Can also be used to enter an account code after a call has been connected.

Action: Advanced | Set | Set Account Code..

Action Data: Account code or blank. If blank, the user is prompted to dial an account code after pressing the button. This option is not supported on XX02 phone modules.

Default Label: Acct or Account Code.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗ [2]
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   T3 Phones:

   - **Classic/Comfort icon**: Displays **1234**.
   - **DSS Link LED**: None.

Set Hunt Group Night Service

Puts the specified hunt group into Night Service mode. Calls to a group set to night service, receive busy or are diverted to voicemail if available or are diverted to the group's night service fallback group if set.

Setting and clearing hunt group night service can be done using either manual controls or using a system time profile. The use of both methods to control the night service status of a particular hunt group is not supported.

This function is not supported between systems in a multi-site network. It can only be used by a user currently logged onto the same system as hosting the hunt group.

Action: Advanced | Set | Set Hunt Group Night Service.

Action Data: Hunt group extension number.

Release 4.0+: If left blank, the button will affect all hunt groups of which the user is a member.

The **Set Hunt Group Night Service** and **Clear Hunt Group Night Service** short code and button features can be used to switch an SSL VPN service off or on respectively. The service is indicated by setting the service name as the telephone number or action data. Do not use quotation marks.

Default Label: HGNS+ or HG Night Service.

Toggles: Yes.

Status Indication: Yes Required. If the button is blank (no specific hunt group) it will indicate on if any one of the hunt groups of which the user is a member is set to night service. If the button is set for multiple hunt groups it will indicate on if any one of those groups is set to night service.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>** ◀	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	▲ On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗ [2]
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   T3 Phones: Supported on Avaya T3 Classic, T3 Comfort phones and DSS Link units only.

   - **T3 Classic/T3 Comfort icon**: Displays ☽ followed by the group number. The background uses the same settings as the LED below.
   - **DSS Link LED**: On when all related groups are in night service. Slow flash if related hunt groups are in mixed states.

Set Hunt Group Out Of Service

Puts the specified hunt group into Out of Service mode. Calls to a group set to out of service receive busy or are diverted to voicemail if available or are diverted to the group's out of service fallback group if set.

This function can be used to used to override hunt groups already set to night service mode by an associated time profile.

Action: Advanced | Set | Set Hunt Group Out of Service.

Action Data: Hunt group extension number.

If left blank, the button will affect all hunt groups of which the user is a member.

Default Label: HGOS+ or HG Out of Service.

Toggles: Yes.

Status Indication: Yes Required. If the button is blank (no specific hunt group) it will indicate on if any one of the hunt groups of which the user is a member is set out of service. If the button is set for multiple hunt groups it will indicate on if any one of those groups is set out of service.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>** ◀	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	▲ On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗ [2]
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   T3 Phones:

   - **Classic/Comfort icon**: Displays **–** followed by the group number. The background uses the same settings as the LED below.

- **DSS Link LED**: On when set. On when all related groups are out of service. Slow flash if related hunt groups are in mixed states.

Set Inside Call Seq

This feature allows the user to select the ringing used on their analog extension for internal calls.

The number entered corresponds to the ring pattern required. This is 0 for Default Ring, 1 for RingNormal, 2 for RingType1, etc. For more information on selectable ringing patterns, see Ring Tones. Use of this short code function is applicable to analog phone users only. The distinctive ringing pattern used for other phones is set by the phone type.

Set Night Service Destination

This button allows the user to change the Night Service target of a hunt group. The button user does not have to be a member of the hunt group. In a multi-site network this function can be used for hunt groups on remote systems.

Changing the destination does not affect calls already ringing at the hunt groups previous night service destination.

Action: Advanced | Set | Set Night Service Group.

Action Data: Hunt group extension number. This is the group for which the night service destination is being set.

Default Label: SetNSG or HG NS Group.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗ [2]
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

2. Limited support on some specific T3 phone models as detailed below.

   On T3 phones this option is accessible through the phone's menus.

Set No Answer Time

Allows the user to change their no answer time setting. This is the time calls ring before going to voicemail or following the user's divert on no answer setting if set on.

In situations where call coverage is also being used, the user's no answer time must be greater than their individual coverage time for coverage to occur.

Action: Advanced | Set | Set No Answer Time.

Action Data: Time in seconds.

Default Label: NATim or No Answer Time.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Set Out of Service Destination

This button allows the user to change the Out of Service target of a hunt group. The button user does not have to be a member of the hunt group. In a multi-site network this function can be used for hunt groups on remote systems.

Changing the destination does not affect calls already ringing at the hunt groups previous Out of Service destination.

Action: Advanced | Set | Set Out of Service Group.

Action Data: Hunt group extension number. This is the group for which the night service destination is being set.

Default Label: SetOOSG or HG OS Group.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗ [2]
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   On T3 phones this option is accessible through the phone's menus.

Set Outside Call Seq

This feature allows the user to select the ringing used on their analog extension for external calls.

The number entered corresponds to the ring pattern required. This is 0 for Default Ring, 1 for RingNormal, 2 for RingType1, etc. For more information on selectable ringing patterns, see Ring Tones. Use of this short code function is applicable to analog phone users only. The distinctive ringing pattern used for other phones is set by the phone type.

Set Ringback Seq

This feature allows the user to select the ringing used on their analog extension for ringback calls.

The number entered corresponds to the ring pattern required. This is 0 for Default Ring, 1 for RingNormal, 2 for RingType1, etc. For more information on selectable ringing patterns, see Ring Tones. Use of this short code function is applicable to analog phone users only. The distinctive ringing pattern used for other phones is set by the phone type.

Set Wrap Up Time

Allows users to change their Wrap-up Time (User | Telephony | Call Settings) setting.

Other phones or applications monitoring the user's status will indicate the user as still being busy (on a call).

Hunt group calls will not be presented to the user.

If the user is using a single line set, direct calls also receive busy treatment. If the user is using a mutli-line set (multiple call appearances), direct calls to them will ring as normal.

It is recommended that this option is not set to less than the default of 2 seconds. 0 is used to allow immediate ringing.

For users set as an CCR Agent, the After Call Work Time (User | Telephony | Supervisor Settings) setting should be used.

Note:

CCR is not supported in IP Office release 9.1 and later.

Action: Advanced | Set | Set Wrap Up Time.

Action Data: Time in seconds. Range 0 to 99999 seconds.

Default Label: WUTim or Wrap-up Time.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Speed Dial

When pressed, the button invokes the same process as dialing **Feature 0**.

If **Feature 0** is followed by a 3-digit index number in the range 000 to 999, the system directory entry with the matching index number is dialed.

If **Feature 0** is followed by ***** and a 2-digit index number in the range 00 to 99, the personal directory entry with the matching index number is dialed. Note: Release 10.0 allows users to have up to 250 personal directory entries. However, only 100 of those can be assigned index numbers.

Action: Advanced | Dial | Speed Dial.

Action Data: None.

Default Label: SpdDial.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series**	**4100 Series:** No	**6400 Series:** No	**D100:** No
1100 Series: Yes	**2400 Series:** No	**4400 Series:** No	**7400 Series:** No	**M-Series:** Yes
1200 Series: Yes	**3600 Series:** No	**4600 Series:** No	**9040:** No	**T-Series:** Yes
1400 Series: No	**3700 Series:** No	**5400 Series:** No	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: No	**3810:** No	**5600 Series:** No	**9600 Series:** No	

Stamp Log

The stamp log function is used to insert a line into any System Monitor trace that is running. The line in the trace indicates the date, time, user name and extension plus additional information. The line is prefixed with **LSTMP: Log Stamped** and a log stamp number. When invoked from a Avaya phone with a display, **Log Stamped#** is also briefly displayed on the phone. This allows users to indicate when they have experienced a particular problem that the system maintainer want them to report and allows the maintainer to more easily locate the relevant section in the monitor trace.

The log stamp number is set to 000 when the system is restarted. The number is then incremented after each time the function is used in a cycle between 000 and 999. Alternately if required, a specific stamp number can be assigned to the button or short code being used for the feature.

Action: Advanced | Miscellaneous | Stamp Log.

Action Data: Optional. Blank or any 3 digit number.

Default Label: Stamp Log.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✗	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✓
1100 Series: ✓	**2400 Series:** ✓	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓ [1]
1200 Series: ✓	**3600 Series:** ✓	**4600 Series:** ✓	**9040:** ✓	**T-Series:** ✓ [1]
1400 Series: ✓	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓	**3810:** ✓	**5600 Series:** ✓	**9600 Series:** ✓	

1. Not supported on T7000, T7100, M7100, M7100N and the Audio Conferencing Unit (ACU).

Stored Number View

Not supported. Provided for CTI emulation only. Allows a user to view the contents of any programmed feature button.

Action: Emulation | Stored Number View.

Action Data: None.

Default Label: BtnVu.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Suspend Call

Uses the Q.931 Suspend facility. Suspends the incoming call at the ISDN exchange, freeing up the ISDN B channel. The call is placed in exchange slot 0 if a slot number is not specified. Only available when supported by the ISDN exchange.

Action: Advanced | Suspend | Suspend.

Action Data: Exchange slot number or blank (slot 0).

Default Label: Suspe.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Suspend CW

Uses the Q.931 Suspend facility. Suspends the incoming call at the ISDN exchange and answer the call waiting. The call is placed in exchange slot 0 if a slot number is not specified. Only available when supported by the ISDN exchange.

Action: Advanced | Suspend | Suspend CW.

Action Data: Exchange slot number or blank (slot 0).

Default Label: SusCW.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Time of Day

Displays the time and date on the user's telephone. This function is ignored on those Avaya phones that display the date/time by default.

Action: Emulation | Time of Day.

Action Data: None.

Default Label: TmDay.

Toggles: Yes.

Status Indication: Yes.

Status	2400, 5400 Series	4600, 5600 Series	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	T-Series, M-Series
- On.	**<Label>** ◀	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	▲ On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100: :** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** Yes	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes [1]	**9500 Series:** Yes	**T3/T3 IP Series:** No

Table continues…

1600 Series: Yes [1]	**3810:** No	**5600 Series:** Yes [1]	**9600 Series:** No	

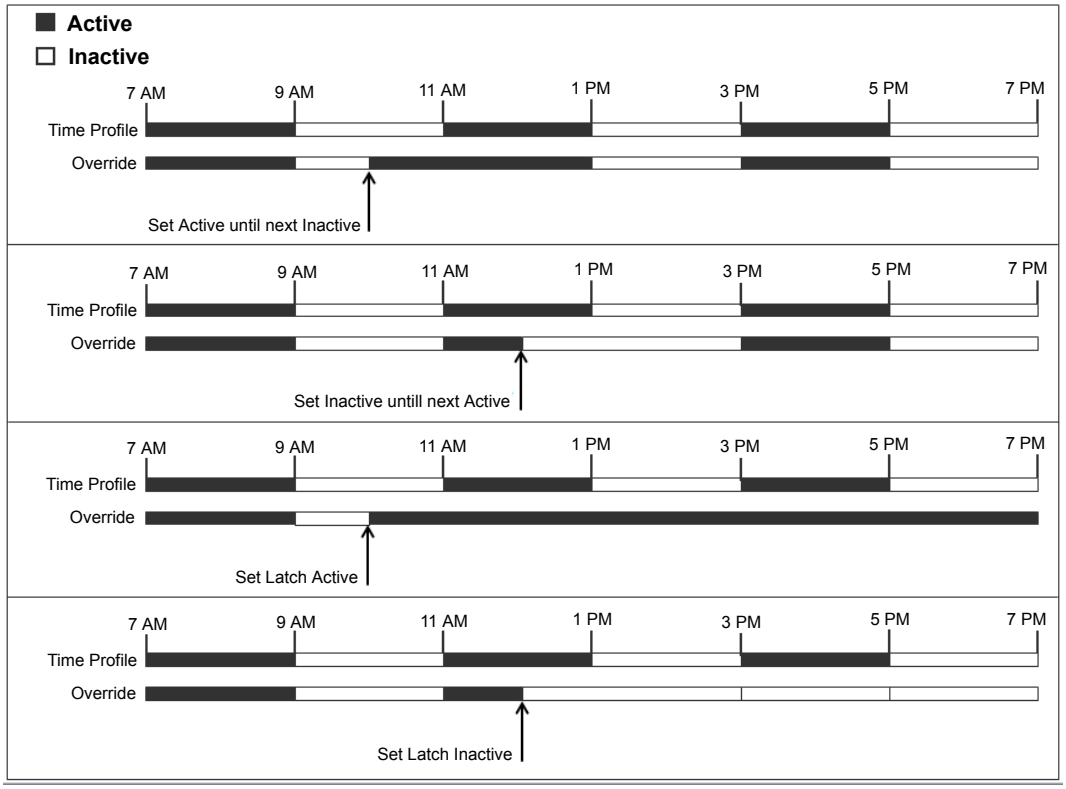
1. Not 1403, 1603, 2402, 4601, 4602, 5402, 5601 and 5602 models.

Time Profile

You can manually override a time profile. The override settings allow you to mix timed and manual settings.

The button indicator will show the Time Profile state and pressing the button will present a menu with five options and an indication of the current state. The menu options are listed below.

Menu Option	Description
Timed Operation	No override. The time profile operates as configured.
Active Until Next Timed Inactive	Use for time profiles with multiple intervals. Select to make the current timed interval active until the next inactive interval.
Inactive Until Next Timed Active	Use for time profiles with multiple intervals. Select to make the current active timed interval inactive until the next active interval.
Latch Active	Set the time profile to active. Timed inactive periods are overridden and remain active.
Latch Inactive	Set the time profile to inactive. Timed active periods are overridden and remain inactive.



Action: Emulation | Time Profile

Action Data: Time profile name.

Default Label: TP or Time Profile

Toggles: No.

Status Indication:

Status	1400, 1600,	9600 Series	9608, 9611, J139, J169, J179	9621, 9641
On	**Green**	**Red on**	**Green On**	**Green**
Off	**Off**	**Off**	**Off**	Grey

User Admin: No

Phone Support: Note that support for particular phone models is also dependant on the system software level.

Analog:	**20 Series:** No	**4100 Series:** No	**6400 Series:** No	**D100:** No

Table continues…

1100 Series: No	**2400 Series:** No	**4400 Series:** No	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** No	**9040:** No	**T-Series:** No
1400 Series: Yes	**3700 Series:** No	**5400 Series:** No	**9500 Series:** No	**T3/T3 IP Series:** No
1600 Series: Yes	**3810:** No	**5600 Series:** No	**9600 Series:** Yes	

Timer

Starts a timer running on the display of the user's extension. The timer disappears when the user ends a call.

This function can be used on Avaya phones (except 9600 Series) that display a call timer next to each call appearance. The button will temporarily turn the call timer on or off for the currently selected call appearance. The change only applies for the duration of the current call.

Action: Emulation | Timer.

Action Data: None.

Default Label: Timer.

Toggles: Yes.

Status Indication: Yes.

Status	**2400, 5400 Series**	**4600, 5600 Series**	4400, 6400 Series	1400, 1600, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>** ◀	**<Label>**	**Green on**	Off	–	–	–	▲ On
- Off.	**<Label>**	**<Label>**	Off	Off	–	–	–	Off

User Admin: Yes.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** Yes	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes [1]	**9500 Series:** Yes	**T3/T3 IP Series:** No

Table continues…

1600 Series: Yes [1]	**3810:** No	**5600 Series:** Yes [1]	**9600 Series:** Yes [2]	

1. Not 1403, 1603, 2402, 4601, 4602, 5402, 5601 and 5602 models.
2. Supported on 96x1, but not 96x0.

Transfer

This function is intend for use with Avaya M-Series and T-Series phones only. When pressed, the button invokes the same transfer process as dialing **Feature 70**.

Action: Advanced | Call | Transfer.

Action Data: None.

Default Label: Xfer.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support This function is only supported on Avaya M-Series and T-Series phones.

Toggle Calls

Cycle between the user's current call and any held calls.

Action: Advanced | Call | Toggle Calls..

Action Data: None.

Default Label: Toggl.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗

Table continues…

1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Twinning

This action can be used by user's setup for mobile twinning. This action is not used for internal twinning.

While the phone is idle, the button allows the user to set and change the destination for their twinned calls. It can also be used to switch mobile twinning on/off and indicates the status of that setting.

When a call has been routed by the system to the user's twinned destination, the **Twinning** button can be used to retrieve the call at the user's primary extension.

In configurations where the call arrives over an IP trunk and the outbound call is on an IP trunk, multi-site network may optimise the routing and in this case the button may not be usable to retrieve the call.

For user's setup for one-X Mobile Client, changes to their Mobile Twinning status made through the system configuration or using a **Twinning** button are not reflected in the status of the **Extension to Cellular** icon on their mobile client. However, changes to the **Extension to Cellular** status made from the mobile client are reflected by the **Mobile Twinning** field in the system configuration. Therefore, for one-X Mobile Client users, it is recommended that they control their Mobile Twinning status through the one-X Mobile Client rather than through a **Twinning** button.

Mobile Twinning Handover When on a call on the primary extension, pressing the **Twinning** button will make an unassisted transfer to the twinning destination. This feature can be used even if the user's **Mobile Twinning** setting was not enabled.

During the transfer process the button will wink.

Pressing the twinning button again will halt the transfer attempt and reconnect the call at the primary extension.

The transfer may return if it cannot connect to the twinning destination or is unanswered within the user's configured **Transfer Return Time** (if the user has no **Transfer Return Time** configured, a enforced time of 15 seconds is used).

Action: Emulation | Twinning.

Action Data: None.

Default Label: Twinning.

Toggles: Yes.

Status Indication: Yes.

Status	2400, 5400 Series	4600, 5600 Series	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	T-Series, M-Series
- On.	**Twinning** ◀	**Twinning**	**Green on**	**Red on**	**Green on**	**Green**	▲ On
- Off.	**Twinning**	**Twinning**	Off	Off	Off	Grey	Off
- Twinned call at secondary	**Twinning** ◀	**Twinning** ◆	**Red on**	Red flash	**Red on**	Blue	[▲ On

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**M-Series:** ✓
1100 Series: ✓	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**T-Series:** ✓
1200 Series: ✓	**3600 Series:** ✓	**4600 Series:** ✓ [1]	**9040:** ✓	**T3/T3 IP Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓ [1]	**9500 Series:** ✓	
1600 Series: ✓ [1]	**3810:** ✗	**5600 Series:** ✓ [1]	**D100:** ✓	

1. Not 1403, 1603, 2402, 4601, 4602, 5402, 5601 and 5602 models.

Unpark Call

This function is obsolete, since the Call Park function can be used to both park and retrieve calls and provides visual indication of when calls are parked. Retrieve a parked call from a specified system park slot.

Action: Advanced | Call | Unpark Call.

Action Data: System park slot number. This must match a park slot ID used to park the call.

Default Label: UnPark.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗ [2]
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

User

Monitors whether another user's phone is idle or in use. The **Telephone Number** field should contain the users name enclosed in double quotes. The button can be used to make calls to the user or pickup their longest waiting call when ringing. On buttons with a text label, the user name is shown.

The actions performed when the button is pressed will depend on the state of the target user and the type of phone being used. It also depend on whether the user is local or on a remote multi-site network system.

Phone	Large display 1400, 1600, 2400, 4600, 5400, 5600, 9500, 9600, M-Series and T-Series Phones	Other Phones or across a multi-site network
Idle	Call the user. Whilst ringing the phone displays options to **Callback** (set an automatic callback) and **Drop** (end the call attempt).	
Ringing	• **Call Pickup:** Pickup the ringing call. • **Call**: Make a call to the user.	Picks up the call.
On a Call	The following options are displayed (name lengths may vary depending on the phone display): • **Call:** Make a call to the user. • **Message:** Cause a single burst of ringing on the target phone. On some phones, when they end their current call their phone will then display PLEASE CALL and your extension number. • **Voicemail:** Call the user's voicemail mailbox. • **Callback:** Set an automatic callback.	No action. For 1400, 1600, 9500 and 9600 Series phones, the **Call**, **Voicemail** and **Callback** options are supported.

Table continues…

	For 1400, 1600, 9500 and 9600 Series phones the following additional options are displayed: • **Drop** Disconnect the user's current call. • **Acquire:** Shown if able to intrude on the user. Take control of the call. • **Intrude:** Shown if able to intrude on the user. Intrude into the call, turning it into a 3-way conference. • **Listen:** Shown if configured to be able to listen to (monitor) the user. Start silent monitoring of the user's call.	

A User button can be used in conjunction with other buttons to indicate the target user when those buttons have been configured with no pre-set user target. In cases where the other button uses the phone display for target selection this is only possible using **User** buttons on an associate button module.

The following changes have been made to the indication of user status via BLF (busy lamp field) indicators such as a User button:

The status shown for a logged out user without mobile twinning will depend on whether they have **Forward Unconditional** enabled.

- If they have **Forward Unconditional** enabled the user is shown as idle.
- If they do not have **Forward Unconditional** enabled they will show as if on DND.

The status shown for a logged out user with mobile twinning will be as follows:

- If there are any calls alerting or in progress through the system to the twinned destination, the user status is shown as alerting or in-use as appropriate. This includes the user showing as busy/in-use if they have such a call on hold and they have **Busy on Held** enabled.
- If the user enables DND through Mobile Call Control or one-X Mobile client, their status will show as DND.
- Calls from the system direct to the user's twinned destination number rather than redirected by twinning will not change the user's status.

Action: User.

Action Data: User name enclosed in "double-quotes".

Default Label: <the user name>.

Toggles: No.

Status Indication: Yes.

Status	2400 Series, 5400 Series	4600 Series, 5600 Series	4400 Series, 6400 Series	1400 Series, 1600 Series, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	T-Series, M-Series
- Idle.	**Extn221**	**Extn221**	Off	Off	Off	Off	Grey	Off
- Alerting.	**Extn221** ◀	**Extn221** ◆	Green flash	Red flash	Red flash	Red flash	Blue	▲ Slow flash
- In Use/ Busy.	**Extn221**	**Extn221**	**Green on**	Red wink	Red wink	Red wink	Blue	▲ Fast flash
- DND	**Extn221**	**Extn221**	**Green on**	**Red on**	**Red on**	**Red on**	**Green**	▲ On

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** Yes	**4100 Series:** No	**6400 Series:** Yes	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** Yes
1200 Series: No	**3600 Series:** Yes	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** Yes
1400 Series: Yes [1]	**3700 Series:** No	**5400 Series:** Yes	**9500 Series:** Yes	**T3/T3 IP Series:** No [2]
1600 Series: Yes [1]	**3810:** Yes	**5600 Series:** Yes [1]	**9600 Series:** Yes	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   T3 Phones:

   - **Classic/Comfort icon**: Displays the user name.
   - **DSS Link LED**: On when busy, flashing when call alerting user.

Visual Voice

This action provides the user with a menu for access to voicemail mailboxes. The menu provides the user with options for listening to messages, leaving messages and managing the mailbox. If no action data is specified, then it is the user's mailbox. Action Data can be used to specify the mailbox of another user or group.

Note:

You can also use the “H” and “U” user source numbers to add another mailbox to your Visual Voice menu. See **Call Management** > **Users** > **Add/Edit Users** > **Source Numbers**

If the Action Data has been configured, pressing the button for an incoming call or while a call is connected sends the call to the user mailbox specified in the action data. If no Action Data is configured, the user is prompted to enter a mailbox.

On phones that have a display but do not support full visual voice operation as indicated below, use of the button for user mailbox access using voice prompts and for direct to voicemail transfer during a call is supported (does not include T3 and T3 IP phones).

Access to Visual Voice on supported phones can be triggered by the phone's **MESSAGES** button rather than requiring a separate Visual Voice programmable button. This is done using the option **System Settings** > **System** > **Voicemail** > **Messages button goes to Visual Voice**.

Action: Emulation | Visual Voice.

Action Data: All local users and groups and all users and groups on systems in the network, except for the user on which the button is being programmed.

Default Label: Voice.

Toggles: No.

Status Indication: When action data is configured, the status lamp provides a message waiting indicator for the monitored mailbox.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: No	**20 Series:** No	**4100 Series:** No	**6400 Series:** No	**D100:** No
1100 Series: No	**2400 Series:** Yes [1]	**4400 Series:** Yes	**7400 Series:** No	**M-Series:** No
1200 Series: No	**3600 Series:** No	**4600 Series:** Yes [1]	**9040:** Yes	**T-Series:** No
1400 Series: Yes	**3700 Series:** No	**5400 Series:** Yes [1]	**9500 Series:** Yes	**T3/T3 IP Series:** Yes [2]
1600 Series: Yes	**3810:** No	**5600 Series:** Yes [1]	**9600 Series:** No	

1. Not 1403, 1603, 2402, 5402, 4601, 4602, 5601 and 5602.
2. Takes the user direct to the listen part of Visual Voice. For the full Visual Voice menu options the user should use **Menu | Settings | Voicemail Settings**.

Visual Voice Controls

The arrangement of options on the screen will vary depending on the phone type and display size.

Listen Access your own voicemail mailbox. When pressed the screen will show the number of **New**, **Old** and **Saved** messages. Select one of those options to start playback of messages in that

category. Use the ▲ up arrow and ▼ arrow keys to move through the message. Use the options below.

Listen Play the message.

Pause Pause the message playback.

Delete Delete the message.

Save Mark the message as a saved message.

Call Call the message sender if a caller ID is available.

Copy Copy the message to another mailbox. When pressed a number of additional options are displayed.

Message Record and send a voicemail message to another mailbox or mailboxes.

Greeting Change the main greeting used for callers to your mailbox. If no greeting has been recorded then the default system mailbox greeting is used.

Mailbox Name Record a mailbox name. This feature is only available on systems using Embedded Voicemail.

Email This option is only shown if you have been configured with an email address for voicemail email usage in the system configuration. This control allows you to see and change the current voicemail email mode being used for new messages received by your voicemail mailbox. Use **Change** to change the selected mode. Press `Done`when the required mode is displayed. Possible modes are:

Password Change the voicemail mailbox password. To do this requires entry of the existing password.

Voicemail Switch voicemail coverage on/off.

Voicemail Collect

Connects to the voicemail server. The telephone number must indicate the name of the Voicemail box to be accessed, eg. "?Extn201" or "#Extn201". The ? indicates "collect Voicemail" and the # indicates "deposit Voicemail". This action is not supported by voicemail using Intuity emulation mode.

When used with Voicemail Pro, names of specific call flow start points can also be used to directly access those start points via a short code. In these cases ? is not used and # is only used if ringing is required before the start points call flow begins.

Action: Advanced | Voicemail | Voicemail Collect.

Action Data: See above.

Default Label: VMCol or VMail Collect.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗ [2]
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

   M-Series/T-Series: For access to the users own mailbox, this button is equivalent to **Feature 65** and **Feature 981**.

Voicemail Off

Disables the user's voicemail box from answering calls that ring unanswered at the users extension. This does not disable the user's mailbox and other methods of placing messages into their mailbox.

This button function is obsolete as the Voicemail On function toggles on/off.

Action: Advanced | Voicemail | Voicemail Off.

Action Data: None.

Default Label: VMOff.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✓
1100 Series: ✓	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✓	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗

Table continues…

1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Voicemail On

Enables the user's voicemail mailbox to answer calls which ring unanswered or arrive when the user is busy.

Action: Advanced | Voicemail | Voicemail On.

Action Data: None.

Default Label: VMOn or VMail On.

Toggles: Yes.

Status Indication: Yes.

Status	**2400, 5400 Series**	**4600, 5600 Series**	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J139, J169, J179	9621, 9641	**T-Series, M-Series**
- On.	**<Label>**	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✓
1100 Series: ✓	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✓	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗ [2]
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.
2. Limited support on some specific T3 phone models as detailed below.

T3 Phones: Supported on Avaya T3 Classic, Comfort and Compact phones for Release 4.2+.

- **Classic/Comfort icon**: Displays . The background uses the same settings as the LED below.
- **DSS Link LED**: On when set.

Voicemail Ringback Off

Disables voicemail ringback to the user's extension. This button function is obsolete as the Voicemail Ringback On function toggles on/off.

Action: Advanced | Voicemail | Voicemail Ringback Off.

Action Data: None.

Default Label: VMRB-

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✗	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✗	

1. Not 1403, 1603, 2402, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Voicemail Ringback On

Enables voicemail ringback to the user's extension. Voicemail ringback is used to call the user when they have new voicemail messages in their own mailbox or a hunt group mailbox for which they have been configured with message waiting indication.

The ringback takes place when the user's phone returns to idle after any call is ended.

Action: Advanced | Voicemail | Voicemail Ringback On.

Action Data: None.

Default Label: VMRB+ or VMail Ringback.

Toggles: Yes.

Status Indication: Yes.

Status	2400, 5400 Series	4600, 5600 Series	1400, 1600, 4400, 6400, 9500 Series	9600 Series	9608, 9611, J169, J179	9621, 9641	T-Series, M-Series
- On.	**<Label>**	**<Label>**	**Green on**	**Red on**	**Green on**	**Green**	On
- Off.	**<Label>**	**<Label>**	Off	Off	Off	Grey	Off

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✓	**4100 Series:** ✗	**6400 Series:** ✓	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✓ [1]	**4400 Series:** ✓	**7400 Series:** ✗	**M-Series:** ✓
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✓ [1]	**9040:** ✓	**T-Series:** ✓
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✓	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✓	**5600 Series:** ✓ [1]	**9600 Series:** ✓	

1. Not 1403, 1603, 4601, 4602, 5601 and 5602 except where 4602 is supported on Release 2.1 and 3.0DT software.

Whisper Page

This feature allows you to intrude on another user and be heard by them without being able to hear the user's existing call which is not interrupted. For example: User A is on a call with user B. When user C intrudes on user A, they can be heard by user A but not by user B who can still hear user A. Whisper page can be used to talk to a user who has enabled private call.

The ability to intrude and be intruded is controlled by two configuration settings, the Can Intrude (User | Telephony | Supervisor Settings) setting of the user intruding and the Cannot Be Intruded (User | Telephony | Supervisor Settings) setting of target being intruded on. The setting of any other internal party is ignored. By default, no users can intrude and all users are set to cannot be intruded.

The system support a range of other call intrusion methods in addition to this feature.

Action: Advanced | Call | Whisper Page.

Action Data: User number or name or blank for entry when pressed.

Default Label: Whisp or Whisper Page.

Toggles: No.

Status Indication: No.

User Admin: No.

Phone Support Note that support for particular phone models is also dependant on the system software level.

Analog: ✗	**20 Series:** ✗	**4100 Series:** ✗	**6400 Series:** ✗	**D100:** ✗
1100 Series: ✗	**2400 Series:** ✗	**4400 Series:** ✗	**7400 Series:** ✗	**M-Series:** ✗
1200 Series: ✗	**3600 Series:** ✗	**4600 Series:** ✗	**9040:** ✗	**T-Series:** ✗
1400 Series: ✓ [1]	**3700 Series:** ✗	**5400 Series:** ✗	**9500 Series:** ✓	**T3/T3 IP Series:** ✗
1600 Series: ✓ [1]	**3810:** ✗	**5600 Series:** ✗	**9600 Series:** ✓	

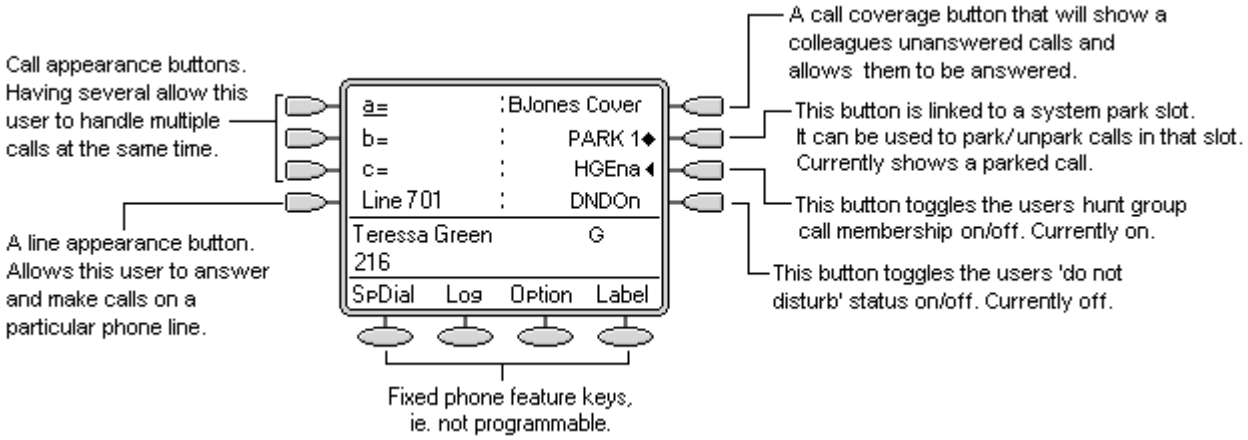
1. Not 1403, 1603.

Chapter 18: Appearance Button Operation

Many Avaya phones supported on system have a programmable keys or buttons (the terms 'key' and 'button' mean the same thing in this context). Various actions can be assigned to each of these keys, allowing the phone user to access that action.

Many of the phones also have indicator lamps next to the programmable buttons. These lamps are used to indicate the status of the button, for example 'on' or 'off'. On other phones the programmable buttons use an adjacent area of the phones display to show status icons and text labels for the buttons.

Example The example below shows the display and programmable buttons on an Avaya 5421 phone where a number of programmable features have been assigned to the user.



This type of phone displays text labels for the programmed features. On other phones a paper label may have to be updated to indicate the programmed feature.

The system supports the following 'appearance' actions - Call Appearance, Bridged Appearance, Line Appearance and Call Coverage Appearance. These actions can be assigned to the programmable buttons on a user's phone. Those 'appearance' buttons can then be used to answer, share, switch between and in some case make calls. This type of call handling is often called 'key and lamp mode'.

This document covers the programming and operation of phones using the appearance functions. Details of the other actions that can be assigned to programmable keys are covered in Button Programming.

Note:

For all the examples within this documentation, it is assumed that **Auto Hold** is on and **Answer Pre-Select** is off unless otherwise stated.

The text shown on phone displays are typical and may vary between phone types, locales and system software releases.

Related links

Appearance Button Features on page 944
Call Appearance Buttons on page 945
Bridged Appearance Buttons on page 945
Call Coverage Buttons on page 946
Line Appearance Buttons on page 947
Selected Button Indication on page 948
Idle Line Preference on page 949
Ringing Line Preference on page 951
Answer Pre-Select on page 953
Auto Hold on page 955
Ring Delay on page 955
Delayed Ring Preference on page 957
Collapsing Appearances on page 959
Joining Calls on page 960
Multiple Alerting Appearance Buttons on page 962
Twinning on page 963
Busy on Held on page 964
Reserving a Call Appearance Button on page 964
Logging Off and Hot Desking on page 964
Applications on page 965
Programming Appearance Buttons on page 965

Appearance Button Features

Appearance functions are only supported on Avaya phones which have programmable buttons and also support multiple calls. Appearance functions are also only supported on those buttons that have suitable adjacent indicator lamps or a display area. Appearance buttons are not supported across a multi-site network.

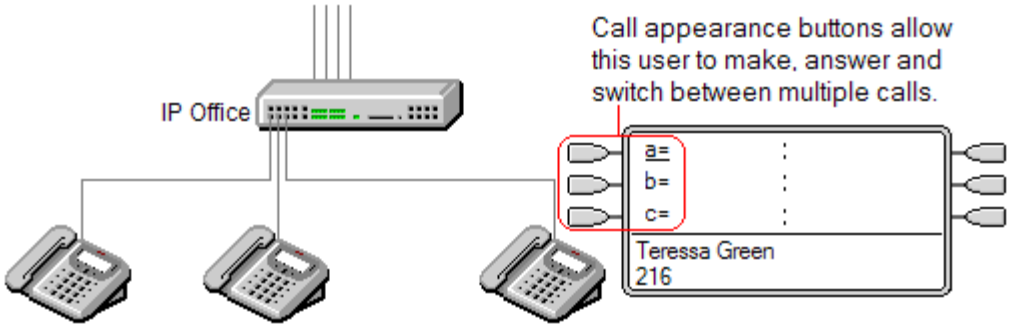
Related links

Appearance Button Operation on page 943

Call Appearance Buttons

Call appearance buttons are used to display alerts for incoming calls directed to a user's extension number or to a hunt group of which they are a member. Call appearance buttons are also used to make outgoing calls.

By having several call appearance buttons, a user is able to be alerted about several calls, select which call to answer, switch between calls and take other actions.



When all the user's call appearance buttons are in use or alerting, any further calls to their extension number receive busy treatment. Instead of busy tone, the user's forward on busy is used if enabled or otherwise voicemail if available.

Call appearance buttons are the primary feature of key and lamp operation. None of the other appearance button features can be used until a user has some call appearance button programmed[1].

There are also addition requirements to programming call appearance buttons:

Call appearance buttons must be the first button programmed for the user.

Programming a single call appearance button for a user is not supported. The normal default is 3 call appearances per user except on phones where only two physical buttons are available.

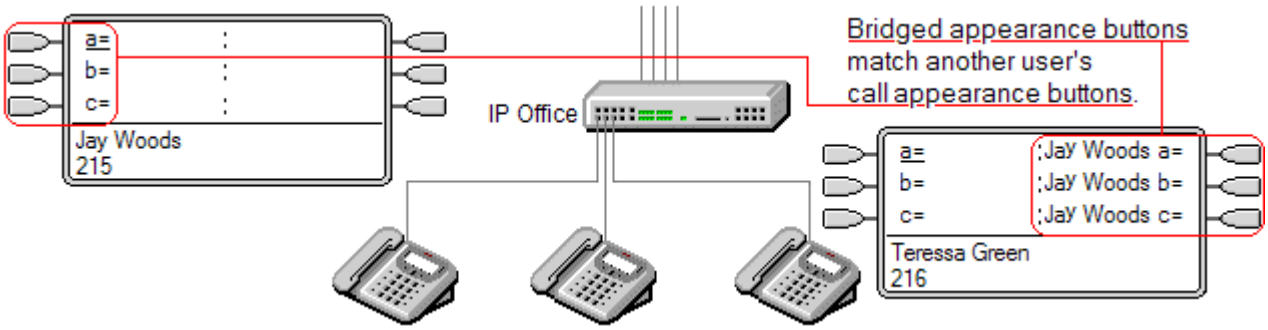
[1] For Release 4.2+, T3 phones support the use of Line Appearance buttons. These can be programmed against buttons on T3 phones without requiring call appearance buttons. See T3 Phone Line Appearances.

Related links

Appearance Button Operation on page 943

Bridged Appearance Buttons

A bridged appearance button shows the state of one of another user's call appearance buttons. It can be used to answer or join calls on that user's call appearance button. It can also be used to make a call that the call appearance user can then join or retrieve from hold.



When the user's call appearance button alerts, any associated bridged appearance buttons on other user's phones also alert. The bridged appearance buttons can be used to answer the call on the call appearance button user's behalf.

When the call appearance button user answers or makes a call, any associated bridged appearance buttons on other users' phones show the status of the call, ie. active, on hold, etc. The bridged appearance button can be used to retrieve the call if on hold or to join the call if active (subject to intrusion permissions).

Note Bridged appearance buttons are different from the action of bridging into a call (joining a call). See Joining Other Calls (Bridging).

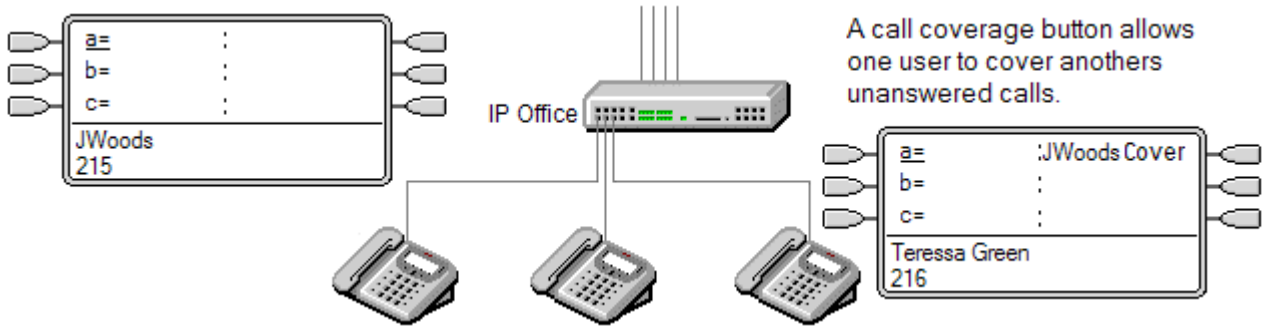
Bridged appearance buttons are not supported between users on different systems in a multi-site network.

Related links

Appearance Button Operation on page 943

Call Coverage Buttons

Call coverage allows a user to be alerted when another user has an unanswered call.



The user being covered does not necessarily have to be a key and lamp user or have any programmed appearance buttons. Their Individual Coverage Time setting (default 10 seconds) sets how long calls will alert at their extension before also alerting on call coverage buttons set to that user.

The user doing the covering must have appearance buttons including a call coverage appearance button programmed to the covered users name.

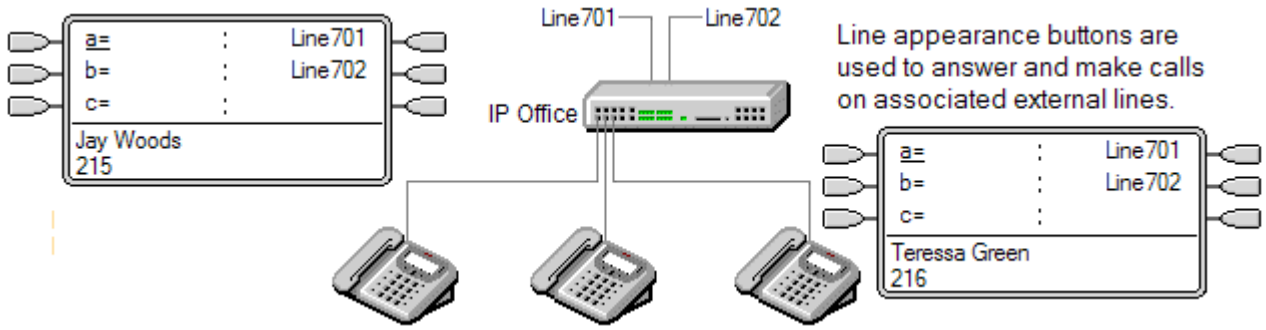
Call coverage appearance buttons are not supported between users on different systems in a multi-site network.

Related links

Appearance Button Operation on page 943

Line Appearance Buttons

Line appearance buttons allow specific individual line to be used when making calls or answered when they have an incoming call. It also allows users to bridge into calls on a particular line.



Incoming call routing is still used to determine the destination of all incoming calls. Line appearance buttons allow a call on a specific line to alert the button user as well as the intended call destination. When these are one and the same, the call will only alert on the line appearance but can still receive call coverage.

When alerting on suitable phones, details of the caller and the call destination are shown during the initial alert.

Individual line appearance ID numbers to be assigned to selected lines on a system. Line appearance buttons are only supported for analog, E1 PRI, T1, T1 PRI, and BRI PSTN trunks; they are not supported for other trunks including E1R2, QSIG and IP trunks.

Line appearance buttons are not supported for lines on remote systems in a multi-site network.

Using Line Appearances for Outgoing Calls In order to use a line appearance to make outgoing calls, changes to the normal external dialing short codes are required. For full details see Outgoing Line Programming.

Private Lines Special behaviour is applied to calls where the user has both a line appearance for the line involved and is also the Incoming Call Route destination of that call. Such calls will alert only on the Line Appearance button and not on any other buttons. These calls will also not follow any forwarding.

T3 Phone Line Appearances Line appearances are supported on T3 and T3 IP phones, see T3 Phone Line Appearances.

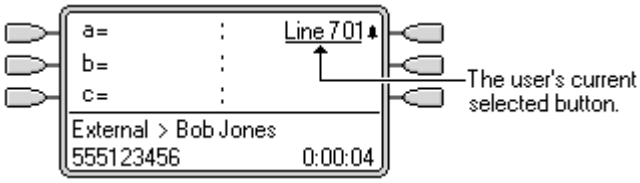
Related links

Appearance Button Operation on page 943

Selected Button Indication

During appearance button usage, one of the user's appearance buttons may be indicated as the user's current selected button. This is the appearance button already in use, or if idle, the appearance button that will be used if the user goes off hook by lifting the handset.

On phones with a display area next to each button, the current selected button is indicated by either an _ underscore of the button label, a * star or a shaded background.



On phones with twin LED lamps, the current selected button is indicated by the red lamp being on

.

On Transtalk 9040 phones, the current selected button is indicated by a ◂ icon.

The system sets which appearance button is the current selected button using the following methods:

- Idle Line Preference This feature can be set on or off for each individual user, the default is on. When on, it sets the current selected button as the first available idle call/line appearance button. See Idle Line Preference.
- Ringing Line Preference This feature can be set on or off for each individual user, the default is on. When on, it sets the current selected button as the button which has been alerting at the users phone for the longest. Ringing Line Preference overrides Idle Line Preference. See Ringing Line Preference.
- Delayed Ring Preference: This setting is used in conjunction with ringing line preference and appearance buttons set to delayed or no ring. It sets whether ringing line preference should observe or ignore the delayed ring applied to the user's appearance buttons when determining which button should have current selected button status.
- **User Selection** The phone user can override both **Idle Line Preference** and **Ringing Line Preference** by pressing the appearance button they want to use or answer. That button will then remain the current selected button whilst active.

If the user currently has a call connected, pressing another appearance button will either hold or disconnect that call. The action is determined by the system's Auto Hold setting.

Answer Pre-Select: Normally when a user has multiple alerting calls, only the details of the call on current selected button are shown. Pressing any of the alerting buttons will answer the call on that button, going off-hook will answer the current selected button. Enabling the user telephony setting **Answer Pre-Select** allows the user to press any alerting button to make it the current selected button and displaying its call details without answering that call. To answer a call when the user has **Answer Pre-Select** enabled, the user must press the alerting button to display the call details and then either press the button again or go off-hook.

Related links

[Appearance Button Operation](#) on page 943

Idle Line Preference

Idle Line Preference determines the user's currently selected button as the first available idle call/line appearance button. Selected button indication is applied to that button and if the user goes off-hook, for example by lifting their handset, an outgoing call is started on that button.

Idle Line Preference is overridden by **Ringing Line Preference** if also on for the user.

By default **Idle Line Preference** is on for all users.

For appearance button users with **Idle Line Preference** off, going off-hook (lifting the handset or pressing **SPEAKER**, **HEADSET**, etc) will have no effect until an appearance button is pressed.

If all the available call/line appearance buttons are in use, no current selected button choice is made by **Idle Line Preference**. In this case, going off hook will have no effect.

?Why Would I Use Just Idle Line Preference In environments that are focused on making outgoing calls, for example telemarketing, incoming calls are infrequent and user's go off-hook expecting to make a call. Using **Idle Line Preference** without **Ringing Line Preference** ensures that the user doesn't inadvertently answer a call when expecting to make a call.

Idle Line Preference Example 1

In this example, only **Idle Line Preference** has been programmed for the user. **Ringing Line Preference** has not been programmed.

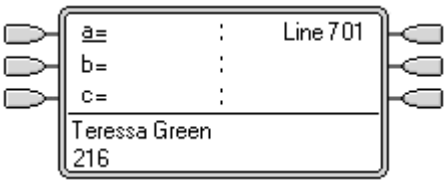
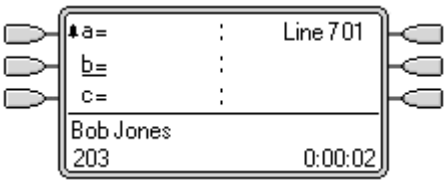
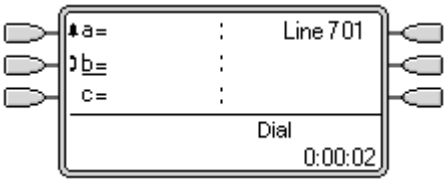
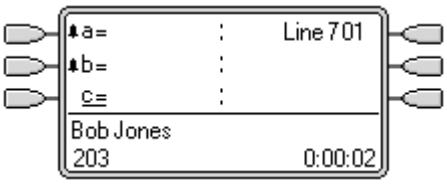
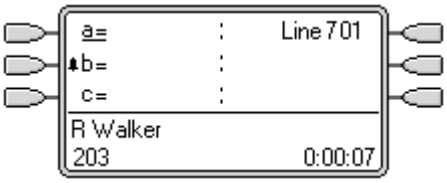
	**Phone Idle** The phone is idle. The current selected button determined by Idle Line Preference is the first available idle call appearance button. This is shown by the _ underscore of the button text.

Table continues…

	**First Call to User** A call for the user arrives. It alerts on the first available call appearance button. Idle Line Preference has changed the current selected button to the next available idle call appearance.
	1. **User Goes Off Hook** With the call still alerting, if the user goes off hook, it will be interpreted as making a call using the currently selected button, not as answering the alerting button. 2. To answer the alerting call, the user should press the alerting button.

Idle Line Preference Example 2

In this example, only **Idle Line Preference** has been programmed for the user. **Ringing Line Preference** has not been not programmed.

	**Two Calls Alerting** The users has two incoming calls alerting. Idle Line Preference has set the currently selected button to their third call appearance.
	**First Caller Abandons** If the first incoming caller disconnects, the currently selected button changes to the first call appearance as this is now the first available idle call appearance button.

Idle Line Preference Example 3

In this example, both **Idle Line Preference** and **Ringing Line Preference** are set for the user.

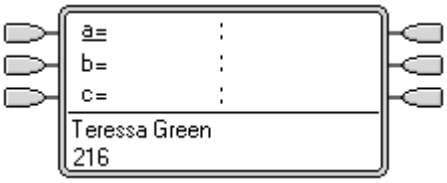
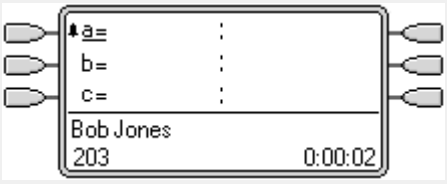
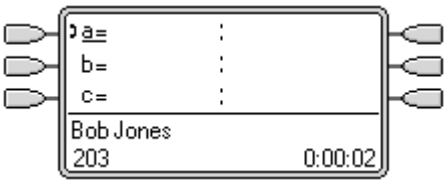
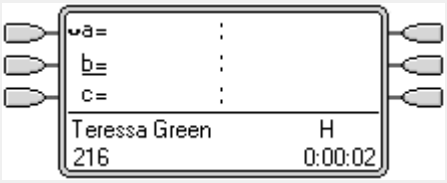
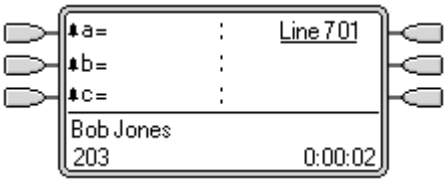
	**Phone Idle** The phone is idle and **Idle Line Preference** has assigned current selected button to the first call appearance.
	**Call Alerting** A call has arrived and **Ringing Line Preference** keeps the current selected button at the first call appearance.

Table continues…

	**Call Answered** With the call answered it retains current selected button status.
	**Call Held** When the call is put on hold, **Idle Line Preference** assigns current selected button status to the next available call appearance button.

Idle Line Preference Example 4

In this example, only **Idle Line Preference** has been programmed for the user. **Ringing Line Preference** has not been programmed.



All Call Appearances Alerting In this case, all the users call appearance buttons are alerting incoming calls. Idle Line Preference has changed the currently selected button to the first available line appearance.

Related links

Appearance Button Operation on page 943

Ringing Line Preference

Ringing Line Preference determines the user's currently selected button as the button which has been alerting the longest. Selected button indication is applied to that button and if the user goes off-hook, for example by lifting their handset, the alerting call on that button is answered.

Ringing Line Preference includes calls alerting on call appearance, line appearance, bridged appearance and call coverage buttons.

Ringing Line Preference overrides **Idle Line Preference**.

By default **Ringing Line Preference** is on for all users.

Ringing Line Preference Order When a user's longest waiting call alerts on several of the user's appearance buttons and Ringing Line Preference is set for the user, the order used for current selected button assignment is;

Call appearance.

Bridged appearance.

Call coverage.

Line appearance.

Example: A user has a call to a covered user alerting initially on a line appearance button. Ringing Line Preference assigns current selected button status to the line appearance. When the same call also begins to alert on the call coverage appearance button, current selected button status switches to the call coverage appearance button.

Ring Delay and Ringing Line Preference Appearance buttons can be set to **Delayed Ring** or **No Ring**. These buttons still alert visually but do not give an audible ring or tone. Ringing line preference is still applied to alerting buttons even if set to **Delayed Ring** or **No Ring**.

Delayed Ring Preference For users with **Ringing Line Preference** selected, their **Delayed Ring Preference** setting sets whether ringing line preference is used or ignores buttons that are visually alerting but have **Delayed Ring** or **No Ring** set. The default is off, ie. ignore ring delay.

Ringing Line Preference Example 1

In this example, both **Ring Line Preference** and **Idle Line Preference** have been set for the user. They also have **Ringing Line Preference** on and **Auto Hold** is on. **Answer Pre-Select** is off.

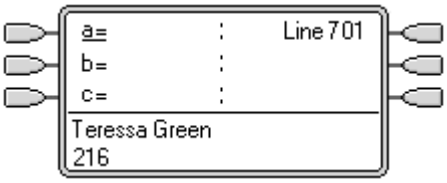
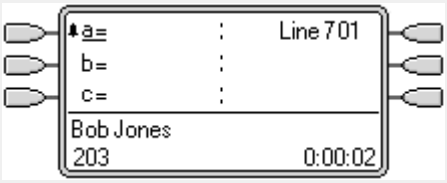
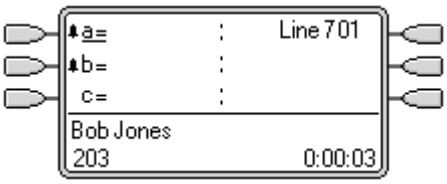
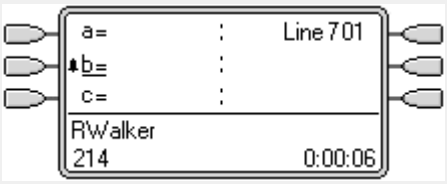
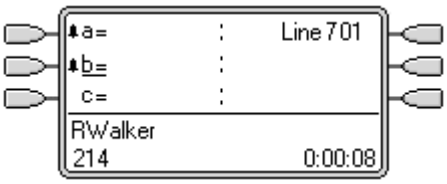
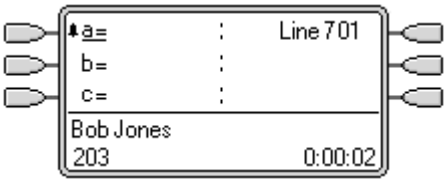
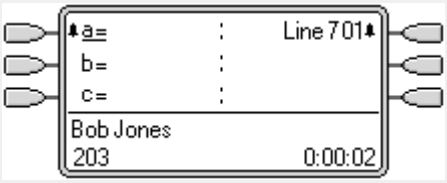
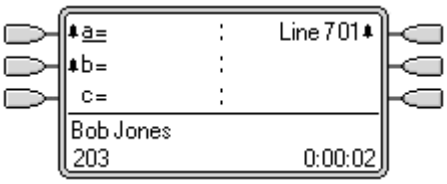
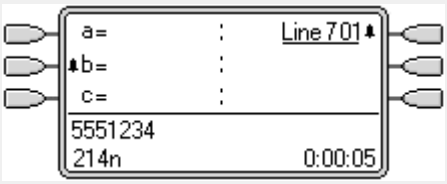
	**Phone Idle** The phone is idle. The current selected button has been determined by Idle Line Preference as the first available idle call appearance button. This is shown by the _ underscore next to that button.
	**First Call Alerting** A call for the user arrives. It alerts on the first available call appearance button. Ringing Line Preference uses this as the currently selected button as it is the only alerting call.
	**Second Call Alerting** Another call for the user arrives. It alerts on the next available call appearance button. As the first call has been alerting longer, under Ringing Line Preference it retains the currently select button status.
	**The First Call Abandons** The first caller disconnects. Ringing Line Preference changes the currently selected button status to the second call appearance button.

Table continues…

	**Another Call Arrives** Another call arrives. It alerts as the first free call appearance button. However the call at the second call appearance has been alerting longer and so under Ringing Line Preference retain the currently selected button status.

Ringing Line Preference Example 2

In this example, the user has both Ring Line Preference and Idle Line Preference programmed. They also have **Ringing Line Preference** on and **Auto Hold** is on. **Answer Pre-Select** is off.

	**First Call to User** A call for the user arrives. It alerts on the first available call appearance button. Ringing Line Preference uses this as the currently selected button as it is the only alerting call.
	**Call on Line 601** The user's Line Appearance is alerting due to an incoming call on the associated line. Details of the call and its destination are shown. Ringing Line Preference keeps the currently selected button status on the call appearance button as this has been alerting longest.
	**Second Call to User** A second call to the user arrives and alerts on the second call appearance button. Ringing Line Preference keeps the currently selected button status on the call appearance button as this has been alerting longest.
	**The First Caller Abandons** The first call to the user disconnects. Ringing Line Preference passes the currently selected button status to the Line Appearance button as this has been alerting longest.

Related links

Appearance Button Operation on page 943

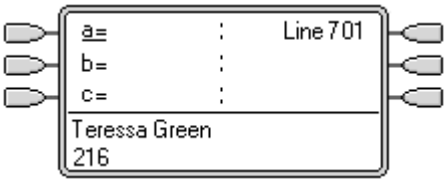
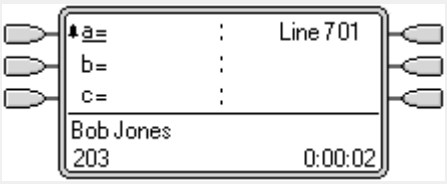
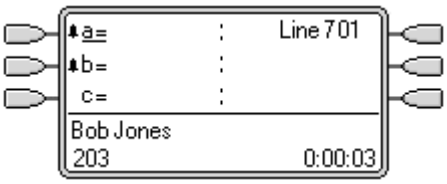
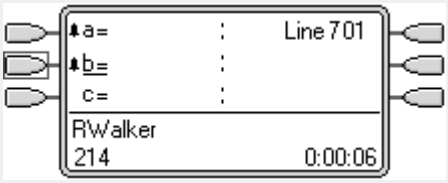
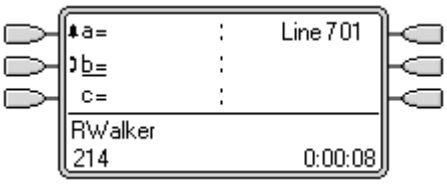
Answer Pre-Select

On some phones, only the details of the call alerting or connected on the current selected button are shown. The details of calls alerting on other buttons are not shown or only shown briefly when they are first presented and are then replaced again by the details of the call on the current selected button.

By default, pressing any of the other alerting buttons will answer the call on that button. Answer pre-select allows a user to press alerting buttons other than the current selected button without actually answering them. Instead the button pressed becomes the current selected button and its call details are displayed.

Note that using answer pre-select with a currently connected call will still either hold or end that call in accordance with the system's Auto Hold setting.

Answer Pre-Select Example 1

	**Phone Idle** The phone is idle. The current selected button has been determined by Idle Line Preference as the first available idle call appearance button. This is shown by the _ underscore next to that button.
	**First Call Alerting** A call for the user arrives. It alerts on the first available call appearance button. Ringing Line Preference uses this as the currently selected button as it is the only alerting call.
	**Second Call Alerting** Another call for the user arrives. It alerts on the next available call appearance button. As the first call has been alerting longer, under Ringing Line Preference it retains the currently select button status.
	**The User Presses the Second Call Appearance** Pressing the second call appearance overrides ringing line preference and assigns current selected button status to the button without actually answering the call. The details of the caller are displayed.
	**The User Answers the Call** The user can press the button again to answer the call or just go off-hook to answer as it is now the currently selected button.

Related links

Appearance Button Operation on page 943

Auto Hold

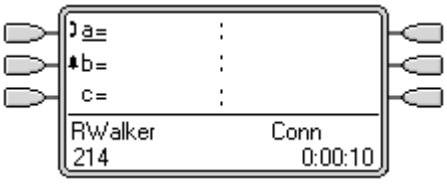
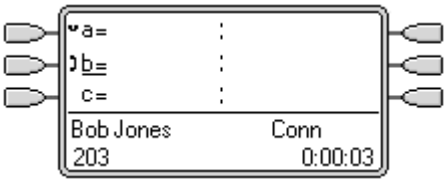
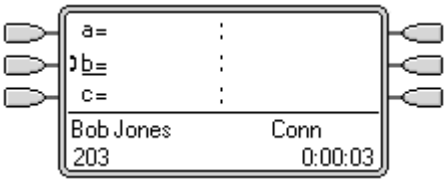
Auto Hold is a system wide feature that affects all appearance button users. This feature determines what happens when a user, who is already on a call, presses another appearance button. The options are:

- If **Auto Hold** is **off**, the current call is disconnected.
- If **Auto Hold** is **on**, the current call is placed on hold.

On Release 4.0 and higher systems **Auto Hold** is **on** by default. On previous levels of system software the default for US was **off**.

Auto Hold Example 1

In this example, the user has two calls currently shown on call appearance buttons. **Answer Pre-Select** is off.

	1. This user has three call appearance buttons. They have answer one call and are still connected to it, shown by the icon. A second call is now alerting on their second call appearance button, shown by the icon. 2. What happens when the user presses the second call appearance key is determined by the system's **Auto Hold** setting:
	**Auto Hold On** When the second call appearance key is pressed, that call is answered and the first call is put on hold, shown by the icon. The user can switch between calls using the call appearance buttons and make/receive other calls if they have additional call appearance buttons
	**Auto Hold Off** When the second call appearance key is pressed, that call is answered and the first call is disconnected.

Related links

Appearance Button Operation on page 943

Ring Delay

Ring delay can be applied to appearance buttons. This option can be used with all types of appearance buttons and can be selected separately for each appearance button a user has. Using

ring delay does not affect the buttons visual alerting through the display and display icons or button lamps.

Ring delay is typically used with line appearance buttons for lines which a user wants to monitor but does not normally answer. However ring delay can be applied to any type of appearance button.

The selectable ring delay options for an appearance button are listed below. The option is selected as part of the normal button programming process.

Immediate Provide audible alerting as per normal system operation.

Delayed Ring Only provide audible alerting after the system ring delay or, if set, the individual user's ring delay.

No Ring Do not provide any audible alerting.

There are two possible sources for the delay used when delayed ringing is selected for a button.

System | Telephony | Telephony | Ring Delay: Default = 5 seconds, Range 1 to 98 seconds. This is the setting used for all users unless a specific value is set for an individual user.

User | Telephony | Multi-line Options | Ring Delay: Default = Blank (Use system setting), Range 1 to 98 seconds. This setting can be used to override the system setting. It allows a different ring delay to be set for each user.

Notes

Calls That Ignore Ring Delay Ring delay is not applied to hold recall calls, park recall calls, transfer return calls, voicemail ringback calls and automatic callback calls. For phones using Internal Twinning, ring delay settings are not applied to calls alerting at a secondary twinned extension (except appearance buttons set to **No Ring** which are not twinned).

Auto Connect Calls Ring delay is applied to these calls before auto-connection. This does not apply to page calls.

Multiple Alerting Buttons Where a call is presented on more than one button on a user's phone, see Multiple Alerting Buttons, the shortest delay will be applied for all the alerting buttons. For example, if one of the alerting buttons is set to **Immediate**, that will override any alerting button set to **Delayed Ring**. Similarly if one of the alerting buttons is set to **No Ring**, it will be overridden if the other alerting button is set to **Immediate** or **Delayed Ring**.

Line Appearance Buttons Calls routed to a user that could potentially be presented on both a call appearance button and a line appearance button are only presented on the line appearance button. In this scenario, the ring delay settings used is that of the first free call appearance button.

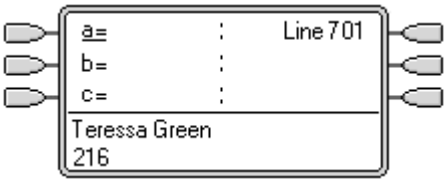
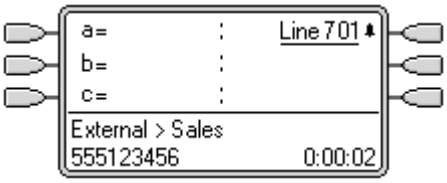
Delay on Analog Lines Analog lines set to Loop Start ICLID already delay ringing whilst the system waits for the full ICLID in order to resolve incoming call routing. In this scenario the ring delay operates in parallel to the routing delay.

Ring Delay and Ringing Line Preference Appearance buttons can be set to **Delayed Ring** or **No Ring**. However ringing line preference is still applied to alerting buttons even if set to **Delayed Ring** or **No Ring**.

The user's **Delayed Ring Preference** setting is used to determine whether ringing line preference is used with or ignores buttons that are alerting but have **Delayed Ring** or **No Ring** set.

Ring Delay Example 1

In this example, the user has a line appearance button set but configured to no ring.

	**Phone Idle** The phone is idle. The current selected button has been determined by Idle Line Preference as the first available call appearance button. This is shown by the _ underscore next to that button.
	**Incoming Call Alerting on the Line** An incoming call arrives on the line and begin to alert somewhere on the system. The user's line appearance button shows this visually but doesn't ring audibly. Ringing line preference would makes the line appearance the user's currently selected button and therefore they would answer the line if they went off-hook.

Related links

[Appearance Button Operation](#) on page 943

Delayed Ring Preference

When a call is alerting at an idle phone, by default Ringing Line Preference sets the call as the currently selected button and if the user then goes off-hook they will answer that call.

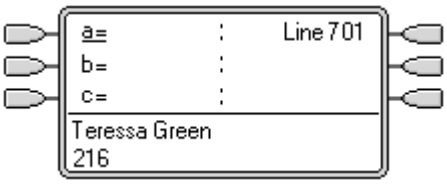
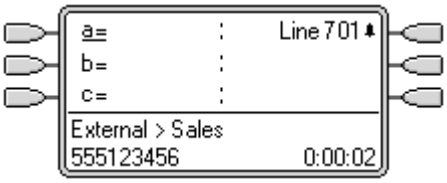
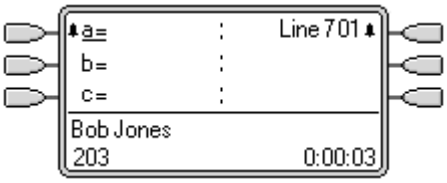
In most situations this is acceptable as the user hears ringing which informs them that there is a call waiting to be answered. If the user wants to make a call instead, they can press another call appearance button to go off-hook on that other button.

When ring delay is being used there can potentially be a problem if the user lifts the handset to make a call without looking at the display. If they do this while the a call is alerting silently on a button with ring delay, the user will actually answer the waiting call rather than get dial tone to make a call.

Once the call alerting on a button has currently selected call status, it retains that status even if a prior call on a button with ring delay applied comes out of its ring delay period.

Delayed Ring Preference Example 1

In this example the user has a line appearance button for a line they monitor. This line appearance button has been set to no ring as the user occasionally need to use that line but does not normally answer calls on that line.

	**Phone Idle** The phone is idle. The current selected button has been determined by Idle Line Preference as the first available call appearance button. This is shown by the _ underscore next to that button.
	**Incoming Call Alerting on the Line** An incoming call arrives on the line and begin to alert somewhere on the system. The user's line appearance button shows this visually but doesn't ring audibly. Normally ringing line preference would make the line appearance the user's currently selected button and therefore they would answer the line if they went off-hook expecting to make a call. However, because **Delayed Ring Preference** is on for the user, ringing line preference is not applied and idle line preference makes their current selected button the first call appearance. If the user were to go off-hook they would be making a call on that call appearance.
	**Call Alerting for the User** A call for the user arrives. It alerts on the first available call appearance button. Ringing line preference is applied and makes that the users currently selected button. If the user goes off-hook now that will answer the call on the call appearance and not the line appearance.

Delayed Ring Preference Example 2

This is similar to the previous example except that the user and the line has been configured for a 15 second ring delay. This informs the users that the line has not been answered for some reason and allows them to answer it by just going off-hook.

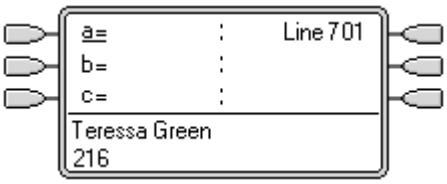
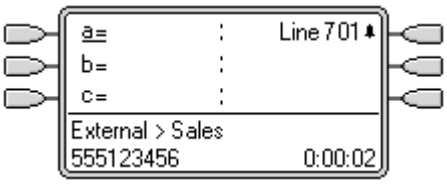
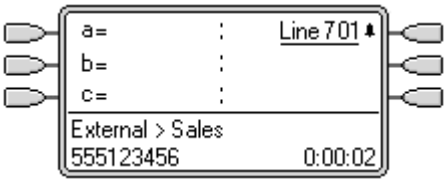
	**Phone Idle** The phone is idle. The current selected button has been determined by Idle Line Preference as the first available call appearance button. This is shown by the _ underscore next to that button.

Table continues…

	**Incoming Call Alerting on the Line** An incoming call arrives on the line and begin to alert somewhere on the system. The user's line appearance button shows this visually but doesn't ring audibly. Because **Delayed Ring Preference** is on for the user, ringing line preference is not applied and idle line preference makes their current selected button the first call appearance. If the user were to go off-hook they would be making a call on that call appearance.
	**Call Continues Alerting** When the ring delay for the line appearance expires, if no other call has taken ringing line preference it becomes the current selected call and will be answered if the user goes off-hook.

Related links

Appearance Button Operation on page 943

Collapsing Appearances

This topic covers what happens when a user with several calls on different appearance buttons, creates a conference between those calls. In this scenario, the call indication will collapse to a single appearance button and other appearance buttons will return to idle. The exception is any line appearance buttons involved which will show 'in use elsewhere'.

Collapsing Appearances Example 1

In this example, the user will setup a simple conference. **Ringing Line Preference** and **Idle Line Preference** are set for the user. **Auto Hold** for the system is on. **Answer Pre-Select** is off.

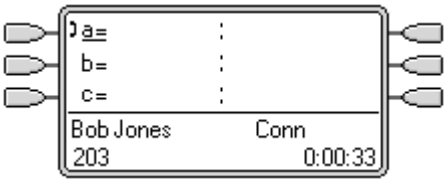
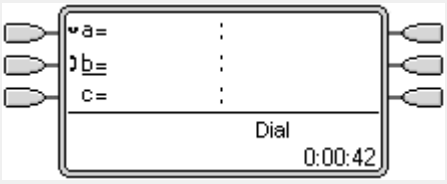
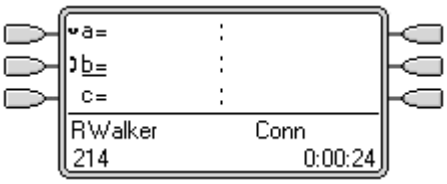
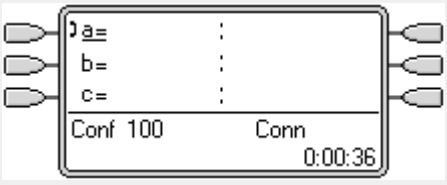
	**Initial Call** The user has a call in progress, shown on their first call appearance button. It is decided to conference another user into the call.
	**Make Conference Enquiry** Pressing the **CONFERENCE** button on the users phone automatically places the current call on hold and takes the phone off hook on the next available call appearance.

Table continues…

	**Enquiry in Progress** The other extension has answered and is invited to join a conference call. The user presses the **CONFERENCE** button on their phone again.
	**Conference Starts/Call Appearances Collapse** The conference call has started. The call appearances have collapsed to a single appearance.

Related links

Appearance Button Operation on page 943

Joining Calls

Appearance buttons can be used to "join" existing calls and create a conference call. A user can join calls that are shown on their phone as 'in use elsewhere'.

This feature is often referred to as 'bridging into a call'. However this causes confusion with Bridged appearance buttons and so the term should be avoided.

The ability to join calls is controlled by the following feature which can be set for each user:

- **Cannot be Intruded**: Default = On If this option is set on for the user who has been in the call the longest, no other user can join the call. If that user leaves the call, the status is taken from the next internal user who has been in the call the longest. The exceptions are:
  - Voicemail calls are treated as **Cannot be Intruded** at all times.
  - When an external call is routed off switch by a user who then leaves the call, the **Cannot be Intruded** status used is that of the user who forwarded the call off switch.
  - Any call that does not involve an internal user at any stage is treated as **Cannot be Intruded** on. For example:
    - When an external call is routed off switch automatically using a short code in the incoming call route.
    - multi-site network calls from other systems that are routed off-switch.
    - VoIP calls from a device not registered on the system.
- The **Can Intrude** setting is not used for joining calls using appearance buttons.

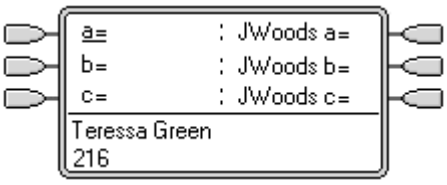
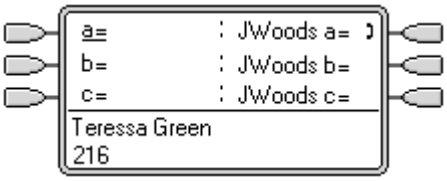
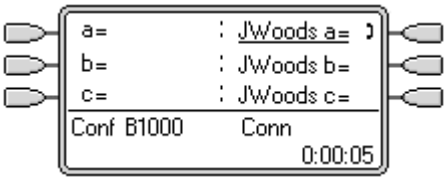
The following also apply:

Inaccessible In addition to the use of the **Cannot be Intruded** setting above, a call is inaccessible if:

- The call is still being dialed, ringing or routed.
- It is a ringback call, for example a call timing out from hold or park.
- If all the internal parties, if two or more, involved in the call have placed it on hold.
- **Conferencing Resources** The ability to bridge depends on the available conferencing resource of the system. Those resources are limited and will vary with the number of existing parties in bridged calls and conferences. The possible amount of conferencing resource depends on the system type and whether Conferencing Center is also installed.
- **Conference Tone** When a call is joined, all parties in the call hear the system conferencing tones. By default this is a single tone when a party joins the call and a double-tone when a party leaves the call. This is a system setting.
- **Holding a Bridged Call** If a user puts a call they joined on hold, it is their connection to the joined call (conference) that is put on hold. The other parties within the call remain connected and can continue talking. This will be reflected by the button status indicators. The user who pressed hold will show 'on hold here' on the button they used to join the call. All other appearance users will still show 'in use here'.
- **Maximum Two Analog Trunks** Only a maximum of two analog trunks can be included in a conference call.
- **Parked Calls** A Line Appearance button may indicate that a call is in progress on that line. Such calls to be unparked using a line appearance.

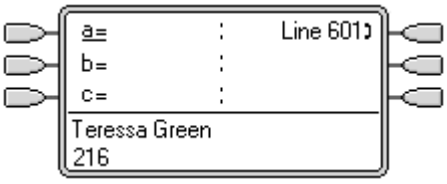
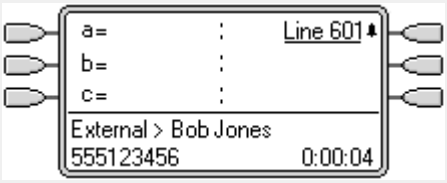
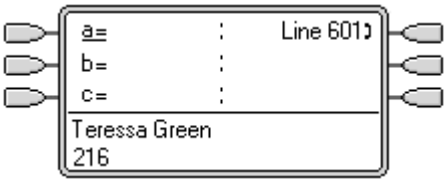
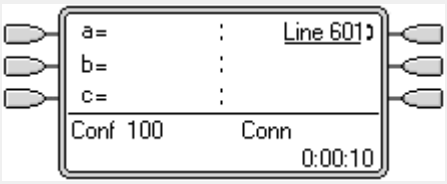
Joining Example 1: Joining with a Bridged Appearance

In this example, the user joins a call using a bridged appearance button. **Answer Pre-Select** is off.

	**User with Bridged Appearance Buttons** The user has bridged appearance buttons that match their colleagues call appearance buttons.
	**Call on Bridged Appearance** The colleague has a call in progress on their first call appearance. This is matched on the first bridged appearance button.
	**User Joins the Call** Pressing the bridged appearance button will take our user off hook and join them into their colleagues call, creating a conference call.

Joining Example 2: Joining with a Line Appearance

In this example, the user joins a call by pressing a line appearance button. **Answer Pre-Select** is off.

	**Line Goes Active** A call is active on the line with line ID number 601. If this is an incoming call, it will show active but will not alert until its call routing has been determined. On ICLID analog lines, alerting is delayed until the ICLID that might be used to do that routing has been received.
	**Line Appearance Alerting** The call routing is completed and the call is now ringing against its target. The line appearance also begins alerting and Ringing Line Preference has made it the current selected button.
	**Call Answered** Alerting on the line appearance has stopped but the line is still active. This indicates that the call has probably been answered. As our user's phone is idle, Idle Line Preference has returned the current select button to the first available call appearance button.
	**User Joins the Call** Our extension user has been asked by their colleague to join the call just answered on line 601. By pressing the line appearance button they have joined the call on that line and created a conference call.

Related links

Appearance Button Operation on page 943

Multiple Alerting Appearance Buttons

In some scenarios, it is may be potentially possible for the same call to alert on several appearance buttons. In this case the following apply:

- **Line appearance buttons override call and bridged appearance buttons** In cases where a call on a line goes directly to the user as the incoming call route's destination, the call will only alert on the line appearance. In this scenario the ring delay settings used is that of the first free call appearance button.
- **A call can alert both call appearance, line appearance and bridged appearance buttons** The most common example of this will be hunt group calls where the hunt group members also have bridged call appearances to each other. In this case the button used to answer the call will remain active whilst the other button will return to idle.

- **Calls on a line/bridged appearance buttons can also alert on call coverage button** In this case alerting on the call coverage button may be delayed until the covered user's **Individual Coverage Time** has expired.
- **Ringing Line Preference Order** When a call alerts on several of the user's appearance buttons and **Ringing Line Preference** is set for the user, the order used for current selected button assignment is:

  1. Call appearance.
  2. Bridged appearance.
  3. Call coverage.
  4. Line appearance.

Example A user has a call to a covered user alerting initially on a line appearance button. **Ringing Line Preference** will assign current selected button status to the line appearance. When the same call also begins to alert on the call coverage appearance button, current selected button status switches to the call coverage appearance button.

Ring Delay Where ring delays are being used, the shortest delay will be applied for all the alerting buttons. For example, if one of the alerting buttons is set to **Immediate**, that will override any alerting button set to **Delayed Ring**. Similarly if one of the alerting buttons is set to **No Ring**, it will be overridden if the other alerting button is set to **Immediate** or **Delayed Ring**.

Related links

Appearance Button Operation on page 943

Twinning

Twinning is a mechanism that allows an user to have their calls alert at two phones. The user's normal phone is referred to as the primary, the twinned phone as the secondary.

By default only calls alerting on the primary phone's call appearance buttons are twinned. For internal twinning, the system supports options to allow calls alerting on other types of appearance buttons to also alert at the secondary phone. These options are set through the **User | Twinning** section of the system configuration and are **Twin Bridge Appearances**, **Twin Coverage Appearances** and **Twin Line Appearances**. In all cases they are subject to the secondary having the ability to indicate additional alerting calls.

Call alerting at the secondary phone ignoring any Ring Delay settings of the appearance button being used at the primary phone. The only exception is buttons set to No Ring, in which case calls are not twinned.

Related links

Appearance Button Operation on page 943

Busy on Held

For a user who has **Busy on Held** selected, when they have a call on hold, the system treats them as busy to any further calls. This feature is intended primarily for analog phone extension users. Within Manager, selecting **Busy on Held** for a user who also has call appearance keys will cause a prompt offering to remove the **Busy on Held** selection.

Related links

Appearance Button Operation on page 943

Reserving a Call Appearance Button

Functions such as transferring calls using a **Transfer** key require the user to have at least one available call appearance button in order to complete the outgoing call part of the process. However, by default all call appearance button are available to receive incoming calls at all times. Through the system configuration it is possible to reserve the user's last call appearance button for making outgoing calls only.

1400, 1600, 9500 and 9600 Series telephone users can put a call on hold pending transfer if they already have held calls even if they have no free call appearance button available. See Context Sensitive Transfer.

Reserving a Call Appearance

The method for doing this depends on the system software level.

Pre-4.0 IP Office: On the **User | Source Numbers** tab, enter the line **RESERVE_LAST_CA=** .

Release 4.0+: On the **User | Telephony | Multi-line Options** tab, select the option **Reserve Last CA**.

Related links

Appearance Button Operation on page 943

Logging Off and Hot Desking

Users can be setup to log in and log out at different phones, this is called 'hot desking'. All the users settings, including their extension number, are transferred to the phone at which the user is logged in. This includes their key and lamp settings and appearance buttons.

This type of activity has the following effect on appearance buttons:

If logged out, or logged in at a phone that doesn't support appearance button functions:

- Bridged appearances set to the user will be inactive.

- Call coverage set to the user will still operate.

If logged in at a phone with fewer buttons than programmed for the user:

- Those buttons which are inaccessible on the logged in phone will be inactive.
- Any bridged appearances to those button from other users will be inactive.

Remote Hot Desking

Release 4.0+ supports, through the addition of license keys, users hot desking between systems within a multi-site network. However, the use of appearance buttons (call coverage, bridged appearance and line appearance) within a multi-site network is not supported. Therefore when a user logs in to a remote system, any such button that they have will no longer operate. Similarly any button that other users have with the remote user as the target will not operate.

Related links

Appearance Button Operation on page 943

Applications

A number of system applications can be used to make, answer and monitor calls. These applications treat calls handled using key and lamp operation follows:

SoftConsole These applications are able to display multiple calls to or from a user and allow those calls to be handled through their graphical interface.

- All calls alerting on call appearance buttons are displayed.
- Calls on line, call coverage and bridged appearance buttons are not displayed until connected using the appropriate appearance button
- Connected and calls held here on all appearance button types are displayed.

Related links

Appearance Button Operation on page 943

Programming Appearance Buttons

About this task

This section covers the programming of appearance buttons for users into existing system configurations.

Appearance Functions The functions **Call Appearance**, **Bridged Appearance**, **Coverage** and **Line Appearance** are collectively known as "appearance functions". For full details of their operation and usage refer to the Appearance Button Operation section. The following restrictions must be observed for the correct operation of phones.

Appearance functions programmed to buttons without suitable status lamps or icons are treated as disabled. These buttons are enabled when the user logs in on a phone with suitable buttons in those positions.

Line appearance buttons require line ID numbers to have been assigned, see Programming Line Appearance Numbers. The use of line appearances to lines where incoming calls are routed using DID (DDI) is not recommended.

How many buttons are allowed? The recommended limits depend on the type of system. The are 10 for IP500 V2 systems, 20 for Server Edition and 40 for Server Edition Select. The limits are applied as follows:

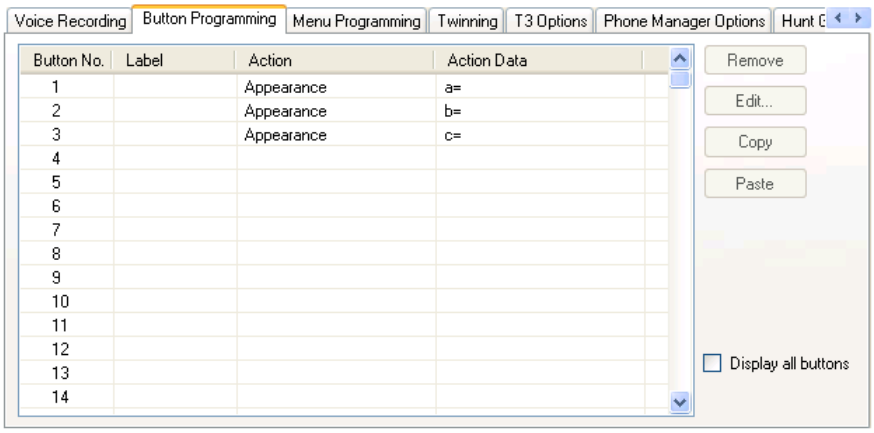
- Number of bridged appearances to the same call appearance.
- Number of line appearances to the same line.
- Number of call coverage appearances of the same covered user.

Programming Appearance Buttons Using Manager

If only button programming changes are required, the configuration changes can be merged back to the system without requiring a reboot.

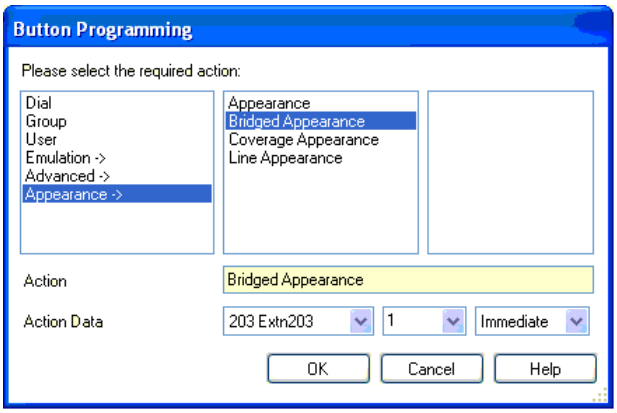
Procedure

1. Start Manager and load the current configuration from the system.
2. Locate and select the user for whom appearance buttons are required.
3. Select **Button Programming**.



The number of buttons displayed is based on the phone associated with the user when the configuration was loaded from the system. This can be overridden by selecting **Display all buttons**.

4. For the required button, click the button number and then click **Edit**.
5. Click the **...** button.



6. From the list of options that appears, click **Appearance**.
7. Select the type of appearance button required.
8. Use the **Action Data** drop-down fields to select the required settings.

   Click **OK**.
9. Repeat for any additional call appearance buttons required.

   Click **OK**.
10. Repeat for any other users requiring appearance buttons.

Related links

Appearance Button Operation on page 943
Appearance Function System Settings on page 967
Appearance Function User Settings on page 968
Programming Line Appearance ID Numbers on page 969
Outgoing Line Programming on page 971

Appearance Function System Settings

System settings are applied to all users and calls. The system settings that affect appearance operation are found on the System | Telephony tabs and are:

- Auto Hold
- Conferencing Tone
- Ring Delay
- Visually Differentiate External Call

Related links

Programming Appearance Buttons on page 965

Appearance Function User Settings

User settings are applied separately to each individual user. In addition to button programming, the following user settings are applicable to appearance button operation:

Cannot be Intruded: Default = On. This feature controls whether other users can use their appearance buttons to join the users call. It applies when the user is the longest present internal party already within the call.

- **Individual Coverage Time (secs):** Default = 10 seconds, Range 1 to 99999 seconds. This function sets how long the phone will ring at your extension before also alerting at any call coverage users. This time setting should not be equal to or greater than the **No Answer Time** applicable for the user.
- **Ring Delay**: Default = Blank (Use system setting). Range = 0 (use system setting) to 98 seconds. This setting is used when any of the user's programmed appearance buttons is set to Delayed ringing. Calls received on that button will initially only alert visually. Audible alerting will only occur after the ring delay has expired.
- **Coverage Ring**: Default = Ring. This field selects the type of ringing that should be used for calls alerting on any the user's call coverage and bridged appearance buttons. **Ring** selects normal ringing. **Abbreviated Ring** selects a single non-repeated ring. **No Ring** disables audible ringing. Note that each button's own ring settings (**Immediate**, **Delayed Ring** or **No Ring**) are still applied.

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

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

Attention Ring Setting	Coverage Ring Setting		
	Ring	**Abbreviated**	**Off**
Ring	Ring	Abbreviated	Off
Abbreviated	Abbreviated	Abbreviated	Off

- **Attention Ring**: Default = Abbreviated Ring. This field selects the type of ringing that should be used for calls alerting on appearance buttons when the user already has a connected call on one of their appearance buttons. **Ring** selects normal ringing. **Abbreviated Ring** selects a single ring. Note that each button's own ring settings (**Immediate**, **Delayed Ring** or **No Ring**) are still applied.
- **Ringing Line Preference**: Default = On. For users with multiple appearance buttons. When the user is free and has several calls alerting, ringing line preference assigns currently selected button status to the appearance button of the longest waiting call. Ringing line preference overrides idle line preference.
- **Idle Line Preference**: Default = On. For users with multiple appearance buttons. When the user is free and has no alerting calls, idle line preference assigns the currently selected button status to the first available appearance button.

- **Delayed Ring Preference**: Default = Off. This setting is used in conjunction with appearance buttons set to delayed or no ring. It sets whether ringing line preference should use or ignore the delayed ring settings applied to the user's appearance buttons.

When on, ringing line preference is only applied to alerting buttons on which the ring delay has expired.

When off, ringing line preference can be applied to an alerting button even if it has delayed ring applied.

- **Answer Pre-Select**: Default = Off. Normally when a user has multiple alerting calls, only the details and functions for the call on currently selected button are shown. Pressing any of the alerting buttons will answer the call on that button, going off-hook will answer the currently selected button. Enabling **Answer Pre-Select** allows the user to press any alerting button to make it the current selected button and displaying its call details without answering that call until the user either presses that button again or goes off-hook. Note that when both **Answer Pre-Select** and **Ringing Line Preference** are enabled, once current selected status is assigned to a button through ringing line preference it is not automatically moved to any other button.
- **Reserve Last CA**: Default = Off. Used for users with multiple call appearance buttons. When selected, this option stops the user's last call appearance button from being used to receive incoming calls. This ensures that the user always has a call appearance button available to make an outgoing call and to initiate actions such as transfers and conferences.

1400, 1600, 9500 and 9600 Series telephone users can put a call on hold pending transfer if they already have held calls even if they have no free call appearance button available. See Context Sensitive Transfer.

Abbreviated Ring: This option has been replaced by the **Attention Ring** setting above.

Related links

Programming Appearance Buttons on page 965

Programming Line Appearance ID Numbers

Line appearances are supported for analog, E1 PRI, T1, T1 PRI, and BRI PSTN trunks. They are not supported for E1R2, QSIG and IP trunks.

Note that setting and changing line settings including line appearance ID numbers requires the system to be rebooted.

Related links

Programming Appearance Buttons on page 965

Manual Renumbering

About this task

Procedure

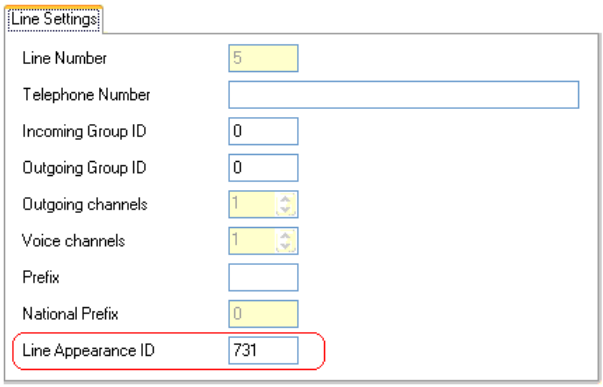
1. Start Manager and load the current configuration from the system.

2. Select **Line**.
3. Select the line required.

   The tab through which line appearance ID numbers are set will vary depending on the type of line. A couple of examples are shown below.

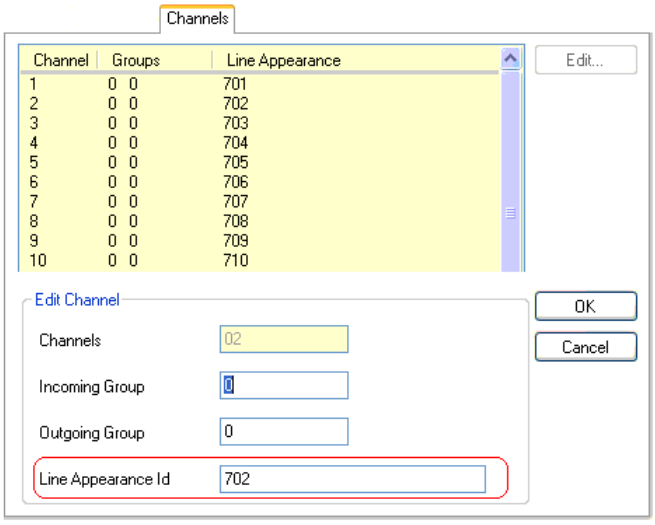
   a. Analog Line

      On the **Line Settings** tab select **Line Appearance ID** and enter the ID required.



   b. Basic/Primary Rate Trunks

      On the Channels tab select the individual channel and click Edit. Select **Line Appearance ID** and enter the required ID, then click **OK**. Repeat for all the channels required.



4. Click **OK**and repeat for any other lines.

Outgoing Line Programming

Assigning line ID numbers to lines and associating line appearance buttons to those lines is sufficient for answering incoming calls on those lines. However, to use line appearance buttons for outgoing calls may require further programming.

Short Codes and Outgoing Line Appearance Calls Once a line has been seized using a line appearance button, short code matching is still applied to the number dialed. That can include user, system and ARS short codes.

The short codes matching must resolve to an off-switch number suitable to be passed direct to the line.

The final short code applied must specify a 'dial' feature. This allows call barring of specific matching numbers to be applied using short codes set to features such as 'Busy'.

Related links

Programming Appearance Buttons on page 965

Chapter 19: Documentation resources

For a listing of documentation resources related to IP Office, see *Avaya IP Office™ Platform Start Here First*. Download documents from the Avaya Support website at http://support.avaya.com.

IP Office documentation is also available on the IP Office Knowledgebase at http://marketingtools.avaya.com/knowledgebase/.

Related links

Finding documents on the Avaya Support website on page 972

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Related links

Documentation resources on page 972

Chapter 19: Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

For questions regarding IP Office documentation, send an email to infodev@avaya.com.

Chapter 19: Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Chapter 19: Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Chapter 19: Additional IP Office resources

You can find information at the following additional resource websites.

Avaya

http://www.avaya.com is the official Avaya website. The front page also provides access to individual Avaya websites for different countries.

Avaya Sales & Partner Portal

http://sales.avaya.com is the official website for all Avaya Business Partners. The site requires registration for a user name and password. Once accessed, the portal can be customized for specific products and information types that you wish to see and be notified about by email.

Avaya IP Office Knowledge Base

http://marketingtools.avaya.com/knowledgebase provides access to an online, regularly updated version of the IP Office Knowledge Base.

Avaya maintenance, lifecycle and warranty information

Avaya support services complement standard Avaya maintenance, lifecycle and warranty policies that are posted on http://support.avaya.com. For more information, send email to support@avaya.com.

International Avaya User Group

http://www.iaug.org is the official discussion forum for Avaya product users.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W