Administering Avaya IP Office™ Platform with Web Manager

Release 9.1
Issue 02.18
February 2016

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.

For full support, please see the complete document, *Avaya Support Notices for Hardware Documentation*, document number 03–600759.

For full support, please see the complete document, *Avaya Support Notices for Software Documentation*, document number 03–600758.

To locate this document on our website, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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: http://support.avaya.com 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 a 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 IF YOU PURCHASE A 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, HTTP://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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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. 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 Designated Processor that hosts 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 on a number of Designated Processors up to the number indicated in the order. 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.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use 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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You 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

Each product has its own ordering code and license types. Note that 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: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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.

Note to Service Provider

The product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

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: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://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: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Document changes since last issue

Table 1: Change summary

Section	Summary of changes
Call Management > **Extensions** > **Edit Extension** > **IP DECT** settings	The **IP DECT** extension settings page now states “These settings are mergeable with the exception of the **Reserve License** setting. Changing the **Reserve License** settings requires a reboot of the system.”
System Settings > **Alternate Route Selection** > **Add/Edit Alternate Route**	The **ARS Rout ID** field can now be edited. The field description has been updated as follows. 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 GroupIDs.
Call Management > **Users** > **Add/Edit Users** > **Self Administration**	The login URL has been added to the **User | Web Self Administration** page.
Solution > **Solution Settings** > **User Synchronization Using LDAP**	Additional details have been added to the field descriptions for **User Synchronization Using LDAP**. Two procedures have been created: • Performing LDAP Synchronization on page 212 • Creating a User Provisioning Rule on page 213

Chapter 1: What's New in Release 9.1

The Web Manager capabilities have expanded in this release as it continues to evolve into a single, comprehensive management tool for IP Office.

Configuration Settings

Web Manager provides access to the most frequently used configuration settings, enabling management of:

- Users
- Groups
- Directory
- Extensions
- Auto Attendant
- Incoming Call Route
- Alternate Route Selection (ARS)
- Time Profiles
- Location
- Short Codes
- SSL VPN

Server Edition systems with a Select license can now provision users by synchronizing with an LDAP database.

End users can manage personal configuration settings using the Web Self Administration portal.

System and Solution Management

Web Manager provides the following system and solution management capabilities.

- IP 500 V2 dashboard system display.
- Server Edition solution level global object management.
- Consolidated management of all servers in the Server Edition network, including Application Servers and Unified Communication Modules (UCM).
- Voicemail Pro system preference management.
- Centralized backup, restore, and upgrade.
- Improved file management.

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.

Supported Web Browsers

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

- Internet Explorer 10 and 11.
- Firefox
- Chrome
- Safari 7

Related links

IP Office operational modes on page 10

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.

Basic Edition

Basic Edition is the default operating mode for IP500 control units. Basic Edition supports up to 32 analogue trunks and 100 users (100 if using a 3 digit dial plan, 48 if using a 2 digit dial plan).

Basic Edition has three modes:

- Quick Mode
- Norstar Mode
- PARTNER Mode

Functionally, each mode type is similar. The Basic Edition mode type used depends on the country where the IP Office system is deployed.

Standard Mode

You can increase the capacity and functionality of a Basic Edition system by applying a Standard Mode license. An Basic Edition system can be converted to Standard Mode by installing 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 10

Chapter 3: Getting started with Web Manager

Related links

Importing a certificate into the Firefox browser on page 12
Importing a certificate into the Internet Explorer browser on page 13
Logging in to Web Manager on page 14
Logging out of Web Manager on page 14
Web Manager User Interface on page 15
User Preferences on page 16

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 12

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 12

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**.

Related links

Getting started with Web Manager on page 12

Logging out of Web Manager

Use this procedure to log out of Web Manager.

Procedure

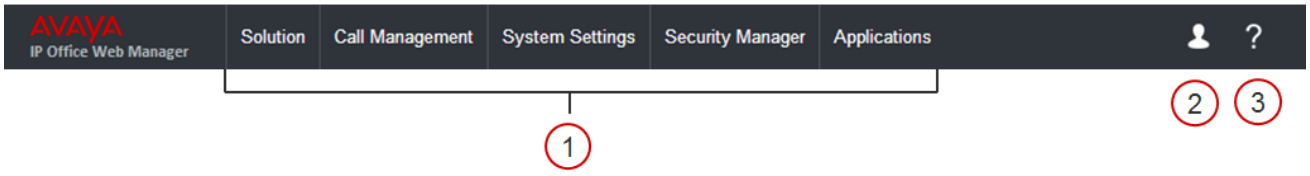
1. In the upper right corner of the Web Manager interface, click **Logout**.
2. You receive a prompt to confirm the log out. Click **OK**.

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 12

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.

Web Manager pages

The table lists the Web Manager pages that can be accessed from the menu bar.

Menu Bar Option	Page
Solution	Solution
Call Management	• Users • Extensions • Groups
System Settings	• Short Codes • Incoming Call Route • Time Profiles • System Directory • Locations • System-SNMP

Table continues…

Menu Bar Option	Page
	• IP Route • Services • Alternate Route Selection
Security Manager	• Service Users • Certificates
Applications	• IP Office Manager • Voicemail Pro — System Preferences • Voicemail Pro — Call Flow Management • one-X Portal • WebRTC Configuration • Web License Manager • File Manager

Related links

Getting started with Web Manager on page 12

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.
Application Preferences	
Inactivity Timeout	Default = 30 seconds. If no activity is detected, the time in seconds after which the Web Manager interface will close and return to the login screen.
Web Manager Logging Level	Default = DEBUG. The level of logging information written to the Web Manager log file. The options are: • INFO • DEBUG • ERROR

Table continues…

Field	Description
Set current user for configuration synchronization	Sets the current logged in user for all the background configuration synchronization tasks.
Use Proxy	Enables communication with expansion systems using the Primary Server's proxy.
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.

Related links

Getting started with Web Manager on page 12

Chapter 4: Solution page

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 19
Solution Settings on page 20
Actions on page 28
Server Menu on page 34

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**

Note:

For release 9.1 and higher, record consolidation is no longer supported for Incoming Call Routes.

By default, to maintain the configurations of the systems in a Server Edition solution, certain types of configuration records are treated differently. **Short Code**, **Time Profile**, **Account Code** and **User Rights** records are only shown at the solution level and cannot be edited in individual system configurations. However, Manager invisibly replicates these records, adding a copy to the configuration of each system in the solution and updating those copies when necessary.

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 **Short Code**, **Time Profile**, **Account Code** and **User Rights** records is performed only at the solution level.
- Those records are then automatically replicated in the configurations of all the systems in the solution but are still only visible and editable at the solution level.

- When the configurations are loaded into Manager 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 **Short Code**, **Time Profile**, **Account Code** and **User Rights** 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. Manager 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 by Manager when the configurations are loaded.

Related links

Solution page on page 18

Solution Settings

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

Related links

Solution page on page 18
View Scheduled Jobs on page 20
Remote Server on page 21
Proxy field descriptions on page 22
Application Server field descriptions on page 23
User Synchronization Using LDAP on page 23

View Scheduled Jobs

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

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

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 20

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 20
Add Remote Server on page 21

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 203.

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. • **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 21

Proxy field descriptions

Solution > **Solution Settings** > **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

Selecting **Proxy** from the **Solution Settings** list displays current proxy detail entries.

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

Click the edit icon to change the settings for an existing proxy.

Click the delete icon to remove an existing proxy.

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 20

Application Server field descriptions

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

If an application server is deployed in the network, select **Application Server** and enter the **Application Server IP Address**.

Related links

Solution Settings on page 20

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.

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.

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.

Related links

Solution Settings on page 20
Connect to Directory Service on page 24
Synchronize User Fields on page 25
View Jobs on page 27
Manage User Provisioning Rules on page 27

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.

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.
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***

Table continues…

Field	Description
	• 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.
Save	If the **Test Connection** action is successful, **Save** is enabled. Click to save the configuration.

Related links

User Synchronization Using LDAP on page 23

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.

- **User Identification**

  Mandatory. This field must be unique for each user to be imported into IP Office.
- **Name**

  Mandatory. The name of the user. User names must be unique across the system. If more than one user has the same name, only the first name must be unique.
- **Full Name**

  Optional. The full name of the user.
- **Email**

  Optional. The email address for the user.
- **Extension**

  Optional. The extension number of the user, if it is provided in LDAP.
- **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.

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

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.
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.

Table continues…

Field	Description
	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 23

View Jobs

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

Field	Description
Job Name	A system generated name.
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 23

Manage User Provisioning Rules

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

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

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, for example 1020, 1021, 1022, etc.
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** • **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 23

Actions

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

Related links

Solution page on page 18

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 203.

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	
Select IP Office Sets	Default = Blank. You can select **IP Office Configuration**. When selected for IP500 V2 Expansion systems, backs up • Configuration • Security Settings

Table continues…

Field	Description
	• 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**
Select Contact Recorder Sets	Default = Blank. You can select **IP Office Configuration**.
Backup Label	
Remote Server	

Table continues…

Field	Description
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 28

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 203.

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	
Restore Points	
Get Restore Points	
Name	
Node Type	
IP Address	
Version	
Set	
Time Stamp	

Related links

Actions on page 28

Transfer ISO

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

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

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.
Select Remote Server	Enabled when **Remote Location** is selected in the **Transfer From** field.
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 28

Upgrade field descriptions

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.

Table continues…

Field	Description
Schedule job	You can schedule the upgrade. Select the **Schedule** check box to enable the **Select Schedule** field.
Select Schedule	The **Select Schedule** list contains upgrade schedules defined in the **Schedule Options** window.

Related links

Actions on page 28

Synchronize Service User and System Password

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

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 28

Server Menu

Navigation: **Server Menu**

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 page on page 18
Dashboard on page 35

Platform on page 35
On-boarding on page 45
Launch SSA on page 45
Service Commands on page 46

Dashboard

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

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

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

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

Related links

Server Menu on page 34

Platform

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

Related links

Server Menu on page 34
System on page 35
Logs on page 37
Updates on page 37
Settings on page 38
AppCenter on page 44
VNC on page 44

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).

Table continues…

Field	Description
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.
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 35

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 35

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.
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 35

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 35
Settings — General on page 39
Settings — System on page 41

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).
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.

Table continues…

Field / Control	Description
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	
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.
Contact Recorder Settings **Debug Level**	This setting can be used to set the debug logging level used by the Contact Recorder application if running. Log files are retrievable through the Logs | Download menu. The options are None, Critical, Error, Warning, Information and Verbose. The default level is Critical.

Table continues…

Field / Control	Description
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 38

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.
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.

Table continues…

Field / Control	Description
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.
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.

Table continues…

Field / Control	Description
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	
Additional Hard Drive Settings	

Related links

Settings on page 38

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 35

VNC

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

The **VNC** page allows you to configure VNC access to the servers graphical desktop. You then have VNC access either through these menus or by using third-party software.

Menu	Description
Settings	Used to start and stop the VNC service supported on the server. The password used is the root password for the server. The Port settings must be matched by the VNC client used to access the desktop.
View	Used to connect to and display the desktop using VNC. Once the password is accepted, the operating system desktop is displayed.

Related links

Platform on page 35

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 214.
- 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 34

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*.

Related links

Server Menu on page 34

Service Commands

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

Related links

Server Menu on page 34
Restart IP Office Service on page 46
Erase Configuration on page 46
Erase Security Settings on page 46
In Service Release/Date on page 47

Restart IP Office Service

Navigation: **Server Menu** > **Platform View** > **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.
- **When 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 46

Erase Configuration

Navigation: **Server Menu** > **Platform View** > **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 46

Erase Security Settings

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

The name and password required to use this command are those used for security configuration access.

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.

Related links

Service Commands on page 46

In Service Release/Date

Navigation: **Server Menu** > **Platform View** > **Service Commands** > **In Service/Release Date**

Describe this action.

Related links

Service Commands on page 46

Chapter 5: Call Management

Related links

Users on page 48
Extension on page 97
Groups on page 111
Auto Attendant on page 134

Users

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

Main content pane

The **Users** main content pane lists provisioned users. The contents of the list depends on the filter option selected.

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 48
User Actions on page 48
Add Users on page 50

User Actions

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

Related links

Users on page 48
Import Users on page 49
Export users on page 49
User Template Management on page 49
Create From Template on page 49

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 48

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 48

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 48

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**, the Select Template window 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: User	Select a template from the list.

Related links

User Actions on page 48
Provision Users on page 50

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 49

Add Users

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

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

Related links

Users on page 48
Users on page 51
Voicemail on page 57
Button Programming on page 61
Telephony on page 62
Short Codes on page 71
Forwarding on page 72

Users

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

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.

For Server Edition, this type of configuration record can be saved as a template and new records created from a template. See Templates.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

In Manager, symbol indicates that the setting can also be set and locked within a set of user rights with which the user is associated using the Working Hour User Rights and Out of Hours User Rights settings. The user rights applied can be controlled by a time profile selected as the user's Working Hours Time Profile setting. The effect of the user rights can be displayed using the User Rights View control.

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.

Table continues…

Field	Description
	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 **User | Voicemail | Voicemail Code**) or their phone log in code (see **User | 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.
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.
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.

Table continues…

Field	Description
	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.
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 Supported Country and 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 options 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.
Profile	Default = Basic User. A user's profile controls whether they can be configured for a number of features. **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 on enterprise branch deployments, see Deploying IP Office in an Avaya Aura Branch Environment. The following requirements must be met when provisioning a centralized user: • An SM line must be configured on the system.

Table continues…

Field	Description
	• 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. 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, other than **Basic User**, is controlled by the user licenses present in the configuration.

System Type	Standard Mode					Server Edition		
User Profile	 Basic User	 Office Worker	 Teleworker	 Mobile Worker	 Power User	 Basic User	 Office Worker	 Power User
one-X Portal Services	Yes [1]	Yes	Yes	–	Yes	–	Yes	Yes
" Telecommuter options	Yes [1]	–	Yes	–	Yes	–	–	Yes
UMS Web Services	Yes [1]	Yes	Yes	–	Yes	–	Yes	Yes
Mobility Features [2]	Yes [1]	–	–	Yes	Yes	Yes	Yes	Yes
TTS for Email Reading	–	–	–	Yes	Yes	–	–	Yes
Remote Worker [3]	–	–	Yes	–	Yes	Yes	Yes	Yes
Avaya Communicator [4]	–	Yes	–	–	Yes	–	Yes	Yes

1. 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

Table continues…

System Type	Standard Mode	Server Edition

supporting a Voicemail Pro server still requires its own **Preferred Edition** license for Voicemail Pro operation.

2. The mobility features are enabled for all users by the **Essential Edition** system license.
3. The system supports users using remote H.323 extensions. On non-Server Edition systems, up to 4 Basic users are supported as remote extensions without needing to be licensed, ie. not 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.
4. 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. For Server Edition, the licenses for SoftConsole are only supported in the configuration of the Primary Server and with users hosted by that server. 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 **Allow Remote Extn** setting of that extension is automatically changed to match the user's **Enable Remote Worker** setting and vice versa.

Table continues…

Field	Description
	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.
Enable Avaya Communicator	Default = Off. This option allows the user to use Avaya Communicator for IP Office as their current telephone device. It can be enabled for users whose **Profile** is set to **Officeworker** or **Power User**. To enable Avaya Communicator for **Basic User**, **Mobile Worker** or **Teleworker**, you need the Avaya Softphone license.
Enable Mobile VoIP Client	Default = Off. Allows the user to use the Mobile VoIP Client for IP Office as their current telephone device. It can be enabled for users whose Profile is set to **Power User**. To enable this setting, you must first enable **Enable one-X Portal Services**.
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 Avaya one-X Mobile for IP Office Administration Guide.
Ex 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, **Ex 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 50

Voicemail

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

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 are mergeable. Changes to these settings do not require a reboot of the system.

In Manager,  symbol indicates that the setting can also be set and locked within a set of user rights with which the user is associated using the Working Hour User Rights and Out of Hours User Rights settings. The user rights applied can be controlled by a time profile selected as the user's Working Hours Time Profile setting. The effect of the user rights can be displayed using the User Rights View control.

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,

Table continues…

Field	Description
	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. • **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.
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).

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.
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.
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.
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.

Table continues…

Field	Description
	• **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.
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**.

Table continues…

Field	Description
	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).

Related links

Add Users on page 50

Button Programming

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

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 are mergeable. 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.

Table continues…

Field	Description
Display All	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.

Related links

Add Users on page 50

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 50
Telephony Call Settings on page 62
Telephony Supervisor Settings on page 65
Telephony Multiline Options on page 68
Telephony Call Log on page 70
Telephony TUI on page 71

Telephony Call Settings

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

For details of the ringing tones, see Ring Tones. DefaultRing uses the system default setting set through the **System | Telephony** tab.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

In Manager, symbol indicates that the setting can also be set and locked within a set of user rights with which the user is associated using the Working Hour User Rights and Out of Hours User Rights settings. The user rights applied can be controlled by a time profile selected as the user's Working Hours Time Profile setting. The effect of the user rights can be displayed using the User Rights View control.

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.

Table continues…

Field	Description
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. • For users set as an CCR Agent, the After Call Work Time (User | Telephony | Supervisor Settings) setting should be 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.
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.
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. Call waiting can also be applied to hunt group calls, see **Hunt Group | Hunt Group | Call Waiting**. Call waiting should not be used for fax and modem devices.

Table continues…

Field	Description
Answer Call Waiting on Hold	Default = On Applies to analog and IP DECT extension users only. If the user has a call waiting and places their current call on hold, the waiting call is automatically connected.
Busy on Held	Default = On  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 Extension Classification (Extn | Analog) to **Quiet Handset** is recommended.
System Phone	Default = Off Users set as a system phone user are able to access additional functions. For Release 6.0 and higher systems, the setting has been replaced by the System Phone Rights setting on the **User | User** tab.

Related links

Telephony on page 62

Telephony Supervisor Settings

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

In Manager, symbol indicates that the setting can also be set and locked within a set of user rights with which the user is associated using the Working Hour User Rights and Out of Hours User Rights settings. The user rights applied can be controlled by a time profile selected as the user's Working Hours Time Profile setting. The effect of the user rights can be displayed using the User Rights View control.

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. • Supports the short code feature Change Login Code. • Users can log out without having a **Login Code** set if they are currently logged in at an extension whose Base Extension Number (Extension | Extn) no longer matches their own Extension (User | User). • 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 Call Listen.

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. For users set as **CCR Agents**, **Forced Login** is automatically enabled and cannot be switched off. Note that users with a **Login Code** and set to **Forced Login** are treated as call center agents. These users consume CCC agents licenses and their status is reported within CBC and CCC applications.
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.

Table continues…

Field	Description
	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. See Authorization Codes.
Incoming Call Bar	Default = Off When enabled, this setting stops a user from receiving any external calls. On the calling phone, the call is rejected.
Outgoing Call Bar	Default = Off When enabled, this setting stops a user from making any external calls except those that use dial emergency features. On many Avaya display phones, this causes a **B** to be displayed. The following features can be used with outgoing call bar: Outgoing Call Bar On, Outgoing Call Bar Off and Change Login Code.
Inhibit Off-Switch Forward/ Transfers	Default = Off. When enabled, this setting stops the user from transferring or forwarding calls externally. This does not stop another user transferring the restricted users calls off-switch on their behalf. Note that a number of other controls may inhibit the transfer operation, see Off-Switch Transfer Restriction.
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 Accept Collect Calls	Default = Off [Brazil Only] Determines whether the user is able to receive and accept collect calls.
CCR Agent	Default = Off. This field is used by the CCR application to indicate which users are Agents monitored by that application. It also indicate to the system those users who can use other CCR features within the system configuration. If a user is set as an CCR Agent, **Forced Login** is enabled and greyed out from being changed and a warning is given if the user does not have a log in code set. The number of simultaneous logged in CCR Agents supported by the system is controlled by licenses entered into the configuration. If all agent licenses on a system have been used, additional agents are prevented from logging in.
Automatic After Call Work	Default = Off. CCR Agents (see above) can be automatically put into **After Call Work** (ACW) state after ending a hunt group call. During ACW state, further hunt group calls are not presented to the agent. Unless ended manually, the After Call Work state is automatically cleared after the agent's After Call Work Time setting. Automatic after call

Table continues…

Field	Description
	work is only supported when the agent is using a phone that supports an After Call Work button.
After Call Work Time (secs)	Default = System Default. Range = 0 (No ACW) to 999 seconds. For CCR Agents with **Automatic After Call Work** enabled, this value sets the duration of the ACW period. If set to **System Default**, the value set in **System | CCR | Default After Call Work Time** is used. A value of **0** disables the user from using ACW.
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 62

Telephony Multiline Options

Navigation: **Call Management** > **Users** > **Edit** > **Telephony** > **Multiline Options**

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). See Appearance Button Operation.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

In Manager, symbol indicates that the setting can also be set and locked within a set of user rights with which the user is associated using the Working Hour User Rights and Out of Hours User Rights settings. The user rights applied can be controlled by a time profile selected as the user's Working Hours Time Profile setting. The effect of the user rights can be displayed using the User Rights View control.

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

Table continues…

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>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>
<tr><td>Ringing Line Preference</td><td>Default = On.
For users with multiple appearance buttons. When the user is free and has several calls alerting, ringing line preference assigns currently selected button status to the appearance button of the longest waiting call. Ringing line preference overrides idle line preference.</td></tr>
<tr><td>Idle Line Preference</td><td>Default = On. For users with multiple appearance buttons. When the user is free and has no alerting calls, idle line preference assigns the currently selected button status to the first available appearance button.</td></tr>
<tr><td>Delayed Ring Preference</td><td>Default = Off.
This setting is used in conjunction with appearance buttons set to delayed or no ring. It sets whether ringing line preference should use or ignore the delayed ring settings applied to the user's appearance buttons.
When on, ringing line preference is only applied to alerting buttons on which the ring delay has expired.
When off, ringing line preference can be applied to an alerting button even if it has delayed ring applied.</td></tr>
<tr><td>Answer Pre-Select</td><td>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.</td></tr>
<tr><td>Reserve Last CA</td><td>Default = Off.</td></tr>
</table>

Table continues…

Field	Description
	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.

Related links

Telephony on page 62

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 are mergeable. Changes to these settings do not require a reboot of the system.

In Manager, symbol indicates that the setting can also be set and locked within a set of user rights with which the user is associated using the Working Hour User Rights and Out of Hours User Rights settings. The user rights applied can be controlled by a time profile selected as the user's Working Hours Time Profile setting. The effect of the user rights can be displayed using the User Rights View control.

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 Default Centralized Call Log On (**System | Telephony | Call Log**). 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).

Table continues…

Field	Description
	This section contains a list of hunt groups on the system. If the system setting Log Missed Huntgroup Calls (System | Telephony | Call Log) 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 62

Telephony TUI

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

Field	Description
Features Menu Controls	
User Setting	Default = Same as System When set to **Custom**, the **Features Menu** list is enabled.
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 For information on telephony features, see the IP Office Product Description.

Related links

Telephony on page 62

Short Codes

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

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

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 are mergeable. Changes to these settings do not require a reboot of the system.

In Manager, symbol indicates that the setting can also be set and locked within a set of user rights with which the user is associated using the Working Hour User Rights and Out of Hours User Rights settings. The user rights applied can be controlled by a time profile selected as the user's Working Hours Time Profile setting. The effect of the user rights can be displayed using the User Rights View control.

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 50

Forwarding

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

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

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, the **Inhibit Off-Switch Forward/ Transfers** (**User | Telephony | Supervisor Settings**) option should be selected. To bar all users

from forwarding calls to external numbers the **Inhibit Off-Switch Forward/Transfers (System | Telephony | Telephony**) option should be selected.

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 destination, it will ignore any further **Forward No Answer** or **Forward on Busy** settings but may follow additional **Forward Unconditional** settings.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

In Manager, symbol indicates that the setting can also be set and locked within a set of user rights with which the user is associated using the Working Hour User Rights and Out of Hours User Rights settings. The user rights applied can be controlled by a time profile selected as the user's Working Hours Time Profile setting. The effect of the user rights can be displayed using the User Rights View control.

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 • Hot Desking The following actions are not blocked: • Do not disturb • Voicemail • 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. For further details see Follow Me. 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.

Table continues…

Field	Description
Forward Unconditional	Default = Off This option, when checked and a **Forward Number** is 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. Using **Follow Me** overrides **Forward Unconditional**. 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.
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 32 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.

Table continues…

Field	Description
	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). Having **Forward Unconditional** active overrides **Forward on No Answer**.
Forward Number	Default = Blank. Range = Internal or External number. Up to 32 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 50

Mobility

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

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	No	No

These settings are mergeable. Changes to these settings do not require a reboot of the system.

In Manager,  symbol indicates that the setting can also be set and locked within a set of user rights with which the user is associated using the Working Hour User Rights and Out of Hours User Rights settings. The user rights applied can be controlled by a time profile selected as the user's Working Hours Time Profile setting. The effect of the user rights can be displayed using the User Rights View control.

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.	
Twinned Handset	Default = Blank.

Table continues…

Field	Description
	For internal twinning, the drop-down list can be used to select an available user as the twinned calls destination. Users not displayed in the list are already twinned with another user. If the list is grayed out, the user is a twinning destination and the primary to which they are twinned is displayed. The secondary phone must be on the same system.
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. This is subject to license requirements of the system software release.	
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.
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.

Table continues…

Field	Description
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.
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.

Table continues…

Field	Description
	- 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. (IP500 V2 digital trunks only) 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. (IP500 V2 digital trunks only). Mobile call control is only supported on digital 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. For details see Mobile Call Control.
Mobile Callback	Default = Off. (IP500 V2 digital trunks only). 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.

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.	
Twinned Handset	Default = Blank. For internal twinning, the drop-down list can be used to select an available user as the twinned calls destination. Users not displayed in the list are already twinned with another user. If the list is grayed out, the user is a twinning destination and the primary to which they are twinned is displayed. The secondary phone must be on the same system.
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.

Table continues…

Field	Description
Mobility Features If enabled this option allows any of the mobility features to be enabled for the user. This is subject to license requirements of the system software release.	
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.
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.
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.

Table continues…

Field	Description
	• 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. (IP500 V2 digital trunks only) 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. (IP500 V2 digital trunks only). Mobile call control is only supported on digital 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. For details see Mobile Call Control.
Mobile Callback	Default = Off. (IP500 V2 digital trunks only). 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.

Related links

Add Users on page 50
Mobility on page 80

Mobility

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

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	No	No

These settings are mergeable. Changes to these settings do not require a reboot of the system.

In Manager, symbol indicates that the setting can also be set and locked within a set of user rights with which the user is associated using the Working Hour User Rights and Out of Hours User Rights settings. The user rights applied can be controlled by a time profile selected as the user's Working Hours Time Profile setting. The effect of the user rights can be displayed using the User Rights View control.

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.	
Twinned Handset	Default = Blank. For internal twinning, the drop-down list can be used to select an available user as the twinned calls destination. Users not displayed in the list are already twinned with another user. If the list is grayed out, the user is a twinning destination and the primary to which they are twinned is displayed. The secondary phone must be on the same system.
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	

Table continues…

Field	Description
If enabled this option allows any of the mobility features to be enabled for the user. This is subject to license requirements of the system software release.	
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.
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.
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

Table continues…

Field	Description
	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. (IP500 V2 digital trunks only) 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. (IP500 V2 digital trunks only). Mobile call control is only supported on digital 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. For details see Mobile Call Control.
Mobile Callback	Default = Off. (IP500 V2 digital trunks only). 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.

Related links

Mobility on page 75

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 50

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 are mergeable. 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.
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.

Table continues…

Field	Description
	• **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.
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 50

Do Not Disturb

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

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

These settings are mergeable. Changes to these settings do not require a reboot of the system.

In Manager, symbol indicates that the setting can also be set and locked within a set of user rights with which the user is associated using the Working Hour User Rights and Out of Hours User Rights settings. The user rights applied can be controlled by a time profile selected as the user's Working Hours Time Profile setting. The effect of the user rights can be displayed using the User Rights View control.

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 50

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 | 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 are mergeable. 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. This setting is not used by the Customer Call Reporter application.
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.

Table continues…

Field	Description
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 50

Personal Directory

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

Each user is able to have up to 100 personal directory records, up to the overall system limit of 10800 records.

These records are used as follows:

- When using ETR, M-Series, T-Series, T3, 1400, 1600, 9500 or 9600 Series phones, the user is able to view and call their personal directory numbers.
- When using a 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 T3, 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 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*.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

Field	Description
Index	Range = 01 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.
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 50

SIP

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

This tab is available when a SIP trunk with a SIP URI record has been added to the configuration. It is also available when an H.323 trunk set to **IP Office SCN** or **IP Office SCN - Fallback** has been added to the configuration.

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 are mergeable. 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 Users on page 50

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.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

Related links

Add Users on page 50
Menu Programming — T3 Telephony on page 91
Menu Programming — Hunt Group on page 91
Menu Programming — 4400/6400 on page 92

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 are mergeable. 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 90

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 are mergeable. 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 90

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 are mergeable. 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 90

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 are mergeable. 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.

Table continues…

Field	Description
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 50

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 are mergeable. 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
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.
BST_NO_MESSAGE_FOR_YOU	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.
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.
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**.
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**. 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 Voicemail Code on the **Hunt Group | Voicemail** tab.

Table continues…

Value	Description
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.
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.
Enable_OTT	Enable one touch transfer operation for the user.

NoUser User 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 that changes to these source numbers require a reboot of the system to become effective.

Value	Description
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.
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_RING BACK	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.
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 DS phones. See Caller Display. Not supported for 1600 and 9600 Series phones.
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.
ProgressEndsOverlapSend	See **Line | VoIP**.

Table continues…

Value	Description
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.
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.
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.
SIP_OPTIONS_PERIOD=X	(X = time in minutes) The system sends SIP options messages periodically to determine if the SIP connection is active. See Options Operations for information on when SIP options messages are sent. 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**.
SUPPRESS_ALARM=1	Used to suppress the NoCallerID alarm. When set, the NoCallerID alarm is not raised in SysMonitor, SNMP traps, email notifications, SysLog or System Status.
VM_TRUNCATE_TIME=X	(Range X = 0 to 7 seconds) 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

Table continues…

Value	Description
	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.

Related links

Add Users on page 50

Web Self Administration

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

Use this page to enable self administration for users.

Field	Description
Self Adminstration	Default = Off. When enabled, users can log in to the Web Self Administration interface. To log in, enter the following address in a browser. `https://<ip_office_ip_address>:7070/WebManagement/selfadmin.html` Configuration settings are grouped under the following categories. • **User** • **Voicemail** • **DND** • **Forwarding** • **Mobility** • **Personal Directory** • **Button Programming**
Visible	When the **Visible** check box is enabled for a configuration setting category, users can view the configuration.
Write	When the **Write** check box is enabled for a configuration setting category, users can change the configuration.

Related links

Add Users on page 50

Extension

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

Main content pane

The Extension main content pane lists provisioned extensions in the Server Edition solution. The contents of the list depends on the filter option selected.

Extension Filters

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

Related links

Call Management on page 48
Extension Actions on page 97
Add Extension on page 98
Edit Extensions on page 99

Extension Actions

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

Related links

Extension on page 97
Extension Template Management on page 97
Create From Template on page 97

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 97

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 97
Provision Extensions on page 98

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 97

Add Extension

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

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 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 97

Edit Extensions

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

Once you have created an extension, you can edit the extension by clicking on the edit icon next to the extension.

Related links

Extension on page 97
Extension Common Fields on page 99
H323 Extension VoIP on page 102
SIP Extension VOIP on page 105
T38 Fax on page 108
IP DECT Extension on page 110

Extension Common Fields

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

Contains settings applicable to most types of extension.

For Server Edition, this type of configuration record can be saved as a template and new records created from a template.

These settings are not mergeable. Changes to these settings will require a reboot of the system.

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 9 digits. This is the directory number of the extension's default associated user. 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 it that user is set to **Force Login**.

Table continues…

Field	Description	
	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**. Extensions associated with IP phones should not be given extension numbers greater than 7 digits. Users for CBC and CCC should only use up to 4 digit extension numbers.	
Phone Password	Default = Blank. Range = Up to 31 digits. H.323 Extensions only. Does not apply to T3 series phones and DECT phones. The code that must 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.	
Caller Display Type	Default = On. Controls the presentation of caller display information for analog extensions, see Caller Display. 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 Supported Country and 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.
	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.

Table continues…

Field	Description	
	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. 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.
Location	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. The drop down list contains all locations that have been defined in the Location page.	
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**.	

Table continues…

Field	Description
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.
Force Authorization	Default = On. This setting is used with SIP extension devices.

Related links

Edit Extensions on page 99

H323 Extension VoIP

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

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

These settings are not mergeable. Changes to these settings will 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. For T3 IP phones installed using DHCP, the address obtained and being used by the phone is displayed. If that address is from the same range as the DHCP pool being supported by the IP Office system, Manager will indicate an error. 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 available codecs in default preference order are: **G.711 A-Law**, **G.711 U-Law**, **G.729** and **G.723.1**. Note that the default order for G.711 codecs will vary to match the

Table continues…

Field	Description
	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/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.
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.
Media Security	Default = Disable. These settings control whether SRTP is used for this extension and the settings used for the SRTP. The options are: • **Disable**: Media security is not required. All media sessions (audio, video, and data) will be enforced to use RTP only. • **Enforce**: Media security is required. All media sessions (audio, video, and data) will be enforced to use SRTP only. • **Best Effort**: Media security is preferred. Attempt to use secure media first and if unsuccessful, fall back to non-secure media.
Advanced Media Security Options	Not displayed if **Media Security** is set to **Disabled**. The options are: • **Same as System**: Use the same setting as the system setting configured on the **System | VoIP Security** tab. • **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).

Table continues…

Field	Description
	• **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.
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. Switch off for T3 IP extensions. For Avaya 1600, 4600, 5600 and 9600 Series phones, the system will enforce the appropriate setting for the phone type. For Avaya T3 IP phones, when **Out-Of-Band** is unchecked, the Allow Direct Media Path option is ignored and calls are via the system in order to provide tones.
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 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. T3 IP phones must be configured to 20ms packet size to use RTP relay. The phone must have firmware T246 or higher.
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

Table continues…

Field	Description
	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 **Both** and **None** options are not available.

Related links

Edit Extensions on page 99

SIP Extension VOIP

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

These settings are shown for SIP IP extensions.

These settings are not mergeable. Changes to these settings will 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.
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/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

Table continues…

Field	Description
	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. 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.
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. 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**: Use the same settings as the system setting configured on the **System | VoIP Security** tab.

Table continues…

Field	Description
	• **Disable**: Media security is not required. All media sessions (audio, video, and data) will be enforced to use RTP only. • **Enforce**: Media security is required. All media sessions (audio, video, and data) will be enforced to use SRTP only. **Warning:** Selecting **Enforce** on a line or extension that does not support media security will result in media setup failures. • **Best Effort**: Media security is preferred. Attempt to use secure media first and if unsuccessful, fall back to non-secure media.
Advanced Media Security Options	Not displayed if **Media Security** is set to **Disabled**. The options are: • **Same as System**: Use the same setting as the system setting configured on the **System | VoIP Security** tab. • **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
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 = 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

Table continues…

Field	Description
	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.
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

Edit Extensions on page 99

T38 Fax

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

The settings on this tab are only accessible if **Re-invite Supported** and **Fax Transport Support** are selected on the VoIP tab.

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.

These settings are not mergeable. Changes to these settings will require a reboot of the system.

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. The system can support Versions **0**, **1**, **2** and **3**. During fax relay, the two gateways will negotiate to use the highest version which they both support.
Transport	Default = UDPTL (fixed). Currently only **UDPTL** is supported. **TCP** and **RTP** transport are not supported For **UDPTL**, redundancy error correction is supported. Forward Error Correction (FEC) is not supported.
Redundancy Redundancy sends additional fax packets in order to increase the reliability. However increased redundancy increases the bandwidth required for the fax transport.	
Low Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for low speed V.21 T.30 fax transmissions.
High Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for V.17, V.27 and V.28 fax transmissions.
TCF Method	Default = Trans TCF. TCF = Training Check Frame.
Max Bit Rate (bps)	Default = 14400. Lower rates can be selected if the current rate is not supported by the fax equipment or is found to not be reliable.
EFlag Start Timer (msecs)	Default = 2600.
EFlag Stop Timer (msecs)	Default = 2300.
Tx Network Timeout (secs)	Default = 150.
Scan Line Fix-up	Default = On.
TFOP Enhancement	Default = On.
Disable T30 ECM	Default = Off. When selected, disabled the T.30 Error Correction Mode used for fax transmission.
Disable EFlags For First DIS	Default = Off.
Disable T30 MR Compression	Default = Off.
NSF Override Default = Off. If selected, the NSF (Non-Standard Facility) information sent by the T38 device can be overridden using the values in the fields below	
Country Code	Default = 0.

Table continues…

Field	Description
Vendor Code	Default = 0.

Related links

Edit Extensions on page 99

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 are mergeable with the exception of the **Reserve License** setting. Changing the **Reserve License** settings requires a reboot of the system.

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	

Table continues…

Field	Description
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

Edit Extensions on page 99

Groups

Navigation: **Call Management** > **Groups**

Main content pane

The **Groups** main content pane lists provisioned groups. The contents of the list depends on the filter option selected.

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 48
Add Groups on page 111

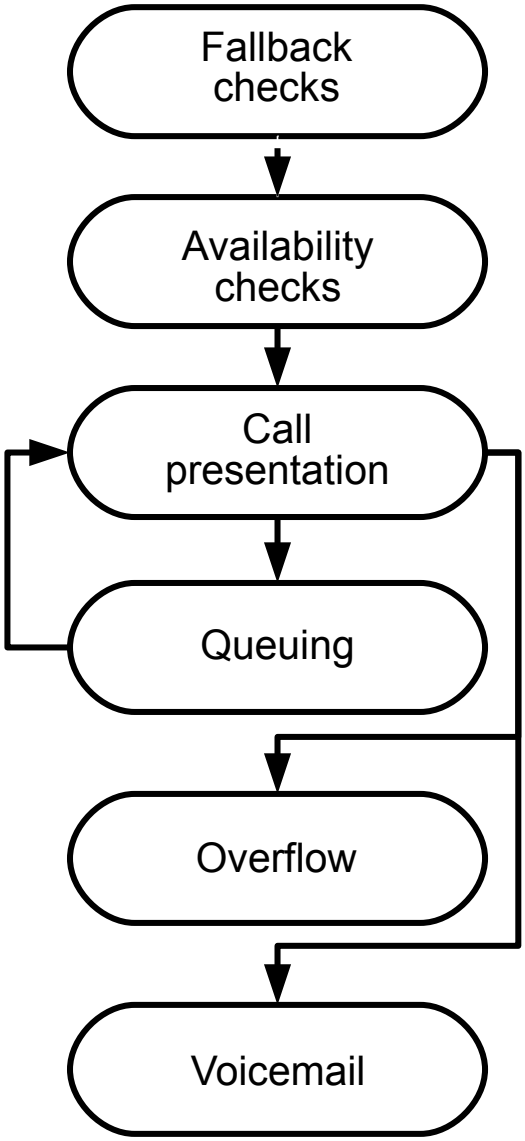
Add Groups

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

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

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

Groups on page 111
Group settings on page 115
Queuing on page 119
Overflow on page 122
Fallback on page 124
Voicemail on page 127
Voice Recording on page 130
Announcements on page 132

Group settings

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

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.

For Server Edition, this type of configuration record can be saved as a template and new records created from a template.

These settings are mergeable. 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

Table continues…

Field	Description
	Defines the group type. The options are: • **Standard Hunt Group**: The default group type and the standard method for creating IP Office user groups. • **CCR Agent Group**: This option is used in conjunction with IP Office CCR application to indicate the groups for which it collects information. CCR Agent Hunt Groups should only contain users who have been configured as CCR Agents (User | Telephony | Supervisor Settings) option. When selected, the menus to select hunt group members will only show users configured as CCR Agents and a warning will be given if the group already contains any users who are not CCR Agents. The queuing option for the hunt group is also forced on for a CCR Agent group. • **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. A user that is not a member of any group is automatically added to the default system XMPP group. As a result, if no XMPP groups are defined, then all users are in the system XMPP group. If a user is a member of a very large XMPP group a large amount of network traffic can be generated. This can be problematic for mobile users. • **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).
Extension	Range = 2 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.

Table continues…

Field	Description
Ex 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** ring simultaneously. • **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.
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 up to 4 music on hold sources; the **System Source** (either an internal file or the external source port or tones) plus up to 3 additional internal wav files, 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

Table continues…

Field	Description
	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 (**System Source** or **Alternate Sources** 2 to 4) 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.
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.
Central System	The field is for information only. It displays the IP Office system where the hunt group was created and can be configured. For pre-Release 5.0 systems, this field is only visible if the IP Office has an **Advanced Small Community Networking** license.
Advertise Group	Default = Off (On for Server Edition). If selected, details of the hunt group are advertised to the other systems within a multi-site network and the hunt group can be dialled from those other systems without the need for routing short codes. For pre-Release 5.0 systems, this field is only visible if the IP Office has an **Advanced Small Community Networking** license. In a Server Edition system this field is fixed as on and details of all hunt groups are advertised to all systems within the network. • Advertised groups must have an extension number that is unique within the network. If an advertised hunt group's extension number conflicts with a local groups extension number, the advertised group is ignored. • Groups set as advertised will appear in the configuration of other IP Office systems. However an advertised group can only be edited on the IP Office system on which it was

Table continues…

Field	Description
	created. Note that advertised groups are not saved as part of the configuration file when **File | Save Configuration As** is used. • Hunt groups that contain members from other IP Office systems are automatically advertised.
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.

Related links

Add Groups on page 111

Queuing

Navigation: **Call Management** > **Groups** > **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 are mergeable. Changes to these settings do not require a reboot of the system.

Field	Description
Queuing On	Default = On This settings allows calls to this hunt group to be queued. The normal  icon is replaced  . This option is automatically enabled and cannot be disabled for a CCR agent group.
Queue Length	Default = No Limit. Range = No Limit, 1 to 999 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.
Normalize Queue Length	Default = Off. 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.

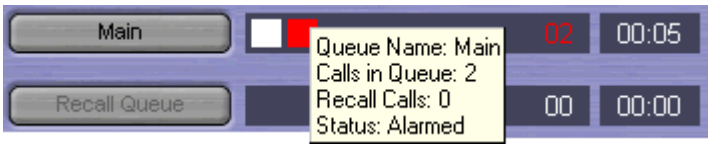
Table continues…

Field	Description
	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. When enabled, the  icon is used for the hunt group.
Controls	The following short code features/button programming actions can be used:

Table continues…

Group Queue Settings	
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 111

Overflow

Navigation: **Call Management** > **Groups** > **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.

For calls being tracked by the Customer Call Reporter application, overflow calls are recorded against the original targeted group but using separate statistics; **Overflowed Calls**, **Overflowed Calls Waiting**, **Overflowed Answered** and **Overflowed Lost**. For full details refer to the *Customer Call Reporter User Guide*.

These settings are mergeable. 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.
Immediate Overflow:	Default = Off.

Table continues…

Field	Description
	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 111

Fallback

Navigation: **Call Management** > **Groups** > **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.

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.

Time Profile:

A **Day Service Time Profile** can be associated with the hunt group. A time profile if required, is set through the **Time Profile | Time Profile** tab.

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 are mergeable. 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

Table continues…

Field	Description
	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. 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
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 111

Voicemail

Navigation: **Call Management** > **Groups** > **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 are mergeable. 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.
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

Table continues…

Field	Description
	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).
Broadcast	Default = Off. (Voicemail Pro only). If a voicemail message is left for the hunt group and Broadcast is enabled, 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.
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.
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

Table continues…

Field	Description
	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 111

Voice Recording

Navigation: **Call Management** > **Groups** > **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 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
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.

Table continues…

Field	Description
	• **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 Groups on page 111

Announcements

Navigation: **Call Management** > **Groups** > **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 | 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 are mergeable. 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. This setting is not used by the Customer Call Reporter application.
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.

Table continues…

Field	Description
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 111

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 48
Add Auto Attendant field descriptions on page 136

Add Auto Attendant field descriptions

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

Related links

Auto Attendant on page 134
Auto Attendant on page 136
Actions on page 137

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 are mergeable. 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.
Direct Dial-By-Number	Default = Off.

Table continues…

Field	Description
	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 136

Actions

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

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 are mergeable. 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 **Ex 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.
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

Table continues…

Field	Description
	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 136

Chapter 6: System Settings

Navigation: **System Settings**

Related links

System Short Codes on page 140
Incoming Call Route on page 142
Time Profiles on page 151
Directory on page 153
Locations on page 156
System-SNMP on page 159
IP Route on page 166
Services on page 169
Alternate Route Selection on page 172

System Short Codes

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

Main content pane

The **Short Codes** main content pane lists provisioned short codes. Click the icons beside a short code to edit or delete.

Related links

System Settings on page 140
Add Short Code on page 140

Add Short Code

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

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.

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 are mergeable. 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.
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 140

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.

Related links

System Settings on page 140
Add Incoming Call Route on page 142
Incoming Call Route MSN Configuration on page 151

Add Incoming Call Route

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

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

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

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

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

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

Multiple Matches

If there is a match between more than one incoming call route record, the one added to the configuration first is used.

Incoming Call Route Destinations

Each incoming route can include a fallback destination for when the primary destination is busy. It can also include a time profile which control when the primary destination is used. Outside the time profile calls are redirected to a night service destination. Multiple time profiles can be associated

with an incoming call route. Each time profile used has its own destination and fallback destination specified.

Incoming Call Routing Examples

Example 1

For this example, the customer has subscribes to receive two 2-digit DID numbers. They want calls on one routed to a Sales hunt group and calls on the other to a Services hunt group. Other calls should use the normal default route to hunt group Main. The following incoming call routes were added to the configuration to achieve this:

Line Group	Incoming Number	Destination
0	77	Sales
0	88	Services
0	blank	Main

Note that the incoming numbers could have been entered as the full dialed number, for example 7325551177 and 7325551188 respectively. The result would still remain the same as incoming number matching is done from right-to-left.

Line Group	Incoming Number	Destination
0	7325551177	Sales
0	7325551188	Services
0	blank	Main

Example 2

In the example below the incoming number digits 77 are received. The incoming call route records 677 and 77 have the same number of matching digit place and no non-matching places so both a potential matches. In this scenario the system will use the incoming call route with the Incoming Number specified for matching.

Line Group	Incoming Number	Destination
0	677	Support
0	77	Sales
0	7	Services
0	blank	Main

Example 3

In the following example, the 677 record is used as the match for 77 as it has more matching digits than the 7 record and no non-matching digits.

Line Group	Incoming Number	Destination
0	677	Support
0	7	Services
0	blank	Main

Example 4

In this example the digits 777 are received. The 677 record had a non-matching digit, so it is not a match. The 7 record is used as it has one matching digit and no non-matching digits.

Line Group	Incoming Number	Destination
0	677	Support
0	7	Services
0	blank	Main

Example 5

In this example the digits 77 are received. Both the additional incoming call routes are potential matches. In this case the route with the shorter Incoming Number specified for matching is used and the call is routed to **Services**.

Line Group	Incoming Number	Destination
0	98XXX	Support
0	8XXX	Services
0	blank	Main

Example 6

In this example two incoming call routes have been added, one for incoming number 6XXX and one for incoming number 8XXX. In this case, any three digit incoming numbers will potential match both routes. When this occurs, potential match that was added to the system configuration first is used. If 4 or more digits were received then an exact matching or non-matching would occur.

Line Group	Incoming Number	Destination
0	6XXX	Support
0	8XXX	Services
0	blank	Main

Related links

Incoming Call Route on page 142
Incoming Call Route General Settings on page 144
Incoming Call Route Voice Recording on page 148
Incoming Call Route Destinations on page 149

Incoming Call Route General Settings

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

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 (see 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.

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.

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

Table continues…

Field	Description
	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.
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.

Table continues…

Field	Description
	• 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 **System | Telephony | 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. See Call Tagging.
Hold Music Source	Default = System source. The system can support up to 4 music on hold source; the **System Source** (either an internal file or the external source port or tones) plus up to 3 additional internal wav files, see **System | Telephony | Tones & 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

Table continues…

Field	Description
	system in a multi-site network, the matching source on that system (**System Source** or **Alternate Sources** 2 to 4) 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 the **System | Telephony | Ring Tones** tab, 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 142

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 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
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.

Related links

Add Incoming Call Route on page 142

Incoming Call Route Destinations

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

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 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
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.
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 142

Incoming Call Route MSN Configuration

Navigation: **System Settings** > **Incoming Call Route** > **Add/Edit 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 142

Time Profiles

Navigation: **System Settings** > **Time Profiles**

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.

Related links

System Settings on page 140
Add Time Profile on page 151

Add Time Profile

Navigation: **System Settings** > **Time Profiles** > **Add/Edit Time Profile**

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.

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
Name	Range = Up to 15 characters This name is used to select the time profile from within other tabs.
Override Default = Off. You can manually override a time profile. The override settings allow you to mix timed and manual settings.	
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. • **Days of Week** The days of the week to which the time period applies.

Table continues…

Field	Description
Recurrence Pattern (Calendar Date)	When a new calendar date entry is required, click **Add Date** and then enter the settings required. Alternately right-click and select **Add Calendar Time Entry**. Calendar records can be set for up to the end of the next calendar year. • **Start Time** The time at which the time period starts. • **End Time** The time at which the time period ends. • **Year** Select either the current year or the next calendar year. • **Date** To select or de-select a particular day, double-click on the date. Selected days are shown with a dark gray background. Click and drag the cursor to select or de-select a range of days.

Related links

Time Profiles on page 151

Directory

Navigation: **System Settings** > **System Directory**

Main content pane

The **System Directory** main content pane lists provisioned directory records. Click the icons beside a record to edit or delete.

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 own **System | Directory Services | HTTP configuration**.

Directory Record Usage

Directory records are used for two types of functions.

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 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 Record Capacity

A maximum of 2500 directory records are supported in the system configuration. 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**	2500	7500	7500	7500
Server Edition	**Primary Server**	2500	7500	7500	7500
	Secondary Server	–	–	7500	7500
	Expansion System (L)	–	–	7500	7500
	Expansion System (V2)	–	–	7500	7500

Server Edition Directory Operation

For Server Edition systems, system directory configuration is only supported through the Primary Server. It is used to setup the central system directory. Other systems in the network are configured to import the central directory from the Primary Server. See Centralized System Directory.

Related links

System Settings on page 140
Add Directory Entry on page 155

Add Directory Entry

Navigation: **System Settings** > **System Directory** > **Add/Edit Directory Entry**

Click **Add/Edit Directory Entry** to open the Add Directory window and configure a directory record.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

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 own **System | Directory Services | HTTP** configuration.

Field	Description
Index	Range = 001 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.

Table continues…

Field	Description
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. Note that if the system has been configured to use an external dialing prefix, that prefix should be added to directory numbers.

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.

Related links

Directory on page 153

Locations

Navigation: **System Settings** > **Locations**

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.

Related links

System Settings on page 140
Add Location on page 157

Add Location

Navigation: **System Settings** > **Locations** > **Add/Edit Location**

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.

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 are mergeable. 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.
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**.

Table continues…

Field	Description
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.
NAT Considerations (Not applicable to Web Manager)	
Allow Direct Media within this location	Default = Off. Reserved for future use.
Time Settings	
Time Zone	Default = Same as System Select a time zone from the list.
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.

Table continues…

Field	Description
	• **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 156

System-SNMP

Navigation: **System Settings** > **System-SNMP**

Main content pane

The **System-SNMP** main content pane lists provisioned SNMP traps. The contents of the list depends on the filter options selected. Click the icons beside a record to edit or delete.

Related links

System Settings on page 140
SNMP Traps on page 159
SNMP Settings on page 165

SNMP Traps

Navigation: **System Settings** > **System-SNMP** > **Add/Edit SNMP Trap**

Click **Add SNMP Trap** to open the Create SNMP Trap window. Note that the **SNMP Enabled** field on the **SNMP Settings** page must be set to **Yes** to enable the **Add SNMP Trap** action.

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.

These settings are not mergeable. Changes to these settings will require a reboot of the system.

Field	Description
New Alarm	This area is used to show and edit the alarm.
Destination To use SNMP or Email the appropriate settings must be configured on the Configuration sub-tab. Note that the Destination type is grayed out if the maximum number of configurable alarms destinations of that type has been reached. Up to 5 alarm destinations can be configured for SNMP, 3 for SMTP email, and 2 for Syslog	
Trap	If selected, the details required in addition to the selected Events are: • **Server Address**: Default = Blank. The IP address or fully qualified domain name (FQDN) of the SNMP server to which trap information is sent. • **Port**: Default = 162. Range = 0 to 65535. The SNMP transmit port. • **Community**: Default = Blank The SNMP community for the transmitted traps. Must be matched by the receiving SNMP server. • **Format**: Default = IP Office. The options are: - **IP Office** SNMP event alarms format in accordance with IP Office. - **SMGR** SNMP event alarms format in accordance with SMGR.
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

Table continues…

Field	Description
	subject line of SMTP email alarms takes the form "System name: IP address - System Alarm".

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.

Type	Events	Event State	Message
Entity	**Application**	Voicemail operation	The Voicemail server is now operational.
		Voicemail Failure	The Voicemail server is down.
		Voicemail Event - storage OK	The Voicemail server storage is OK.
		Voicemail Event - storage nearly full	The Voicemail server storage is nearly full.
		Voicemail Event - storage full	The Voicemail server storage is full.
	Service	All licenses in use	The following licenses are all in use. License Type: <name>.
		All resources in use	The following system resources are all in use: <resource type> will be provided.
		Authentication failure	Avaya Contact Center Select data synchonization failed: authentication failure.
		Clock source changed	8kHz clock source changed. Details will be provided.
		CPU warning/critical	• Warning alarm: CPU utilization near capacity. • Critical alarm: CPU exhausted.
		Feature license missing	Attempt to use a feature for which no license is installed. License Type: <name>.
		Hold music file failure	Failed to load Hold Music source file.
		Log stamped	Log Stamp #nnn created in Monitor logs.
		Logon failed	Logon failure reason will be provided.

Table continues…

Type	Events	Event State	Message
		Memory use warning/critical	• Warning alarm: Memory utilization near capacity. • Critical alarm: Memory exhausted.
		Network interconnect failure	Details of the network interconnection failure will be provided.
		No free channels available	No free channels were available. Outgoing group ID: <number>.
		OEM card slot error	System running secondary software or error description with OEM card will be provided.
		SIP message too large	SIP message Rx error - too large - ignored.
		SIP Registration Expiry	• Avaya IP Office Contact Contact Center SIP registration expired • Avaya Contact Center Select SIP registration expired.
		Sync Request Timeout	Avaya Contact Center Select data synchonization failed: no response from CCMA server
	Memory Card	Change	The PC card in name has changed.
	Expansion Module	Operational	Expansion module name link is up.
		Failure	Expansion module name link is down.
		Error	Expansion module name link has a link error.
		Change	Expansion module name link has changed.
	Trunk	Operational	Trunk number (name) [on expansion module number] is now operational.
		Failure	Trunk number (name) [on expansion module number] is down.
	Trunk	Trunk seize failure	Seize failure: Channel [number] or Port [number].
		Incoming call outgoing trunk failure	Incoming call outgoing trunk: Channel [number] or Port [number].
		CLI not delivered	CLI not delivered: Channel [number] or Port [number].
		DDI incomplete	DDI incomplete. Expected Number of digits: <number>.

Table continues…

Type	Events	Event State	Message
		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: <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
	VCM	Operational	VCM module name is now operational.
		Failure	VCM module name has failed.
Memory Card	**Invalid Card**		
	Free Capacity		
Generic	**Generic**	Non-primary location boot alarm	System running backup software.
		Invalid SD Card	Incompatible or Invalid (System or Optional) SD Card fitted.
		Network link failure	Network Interface name (ip address) has been disconnected.
		Network link operational	Network Interface name (ip address) has been connected.
		System warm start	System has been restarted (warm start).
		System cold start	System has restarted from power fail (cold start).
		SNMP Invalid community	Invalid community specified in SNMP request.

Table continues…

Type	Events	Event State	Message
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 will cause an alarm.	
Syslog	**Basic Audit**	Events as written to the system Audit Trail. Available on Syslog output only.	
System	**Configuration**	CCR group agent not targeted	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

Table continues…

Type	Events	Event State	Message
			Called:number sent on the line CallerID:ID Usr:user Extn:extension
		Emergency call failure	Failed Emergency Call | Emergency call! Location:location Dialled:dialled number FailCause:cause Usr:user Extn:extension

Related links

System-SNMP on page 159

SNMP Settings

Navigation: **System Settings** > **SNMP Settings**

Note that the QoS Parameters are only available in Manager.

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 65534. 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 Enable RTCP Monitor on Port 5005 is selected (Systems | LAN1 | VoIP). 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.	

Table continues…

Field	Description		
• An alarm will not be triggered for the QoS parameters recorded during the first 5 seconds of a call.			
Round Trip Delay (msec)	Default = 350. Less than 160ms is high quality. Less than 350ms is good quality. Any higher delay will be noticeable by those involved in the call. Note that, depending on the compression codec being used, some delay stems from the signal processing and cannot be removed: G.711 = 40ms, G.723a = 160ms, G.729 = 80ms.		
Jitter (msec)	Default =20. Jitter is a measure of the variance in the time for different voice packets in the same call to reach the destination. Excessive jitter will become audible as echo.		
Packet Loss (%)	Default = 3.0. Excessive packet loss will be audible as clipped words and may also cause call setup delays.		
		Good Quality	**High Quality**
	Round Trip Delay	< 350ms	< 160ms
	Jitter	< 20ms	< 20ms
	Packet Loss	< 3%	< 1%

Related links

System-SNMP on page 159

IP Route

Navigation: **System Settings** > **IP Route**

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.

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

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.

Related links

System Settings on page 140
Add IP Route on page 168

Add IP Route

Navigation: **System Settings** > **IP Route** > **Add/Edit IP Route**

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.

This tab is 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 are mergeable. 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 166

Services

Navigation: **System Settings** > **Services**

Main content pane

The **Services** main content pane lists provisioned SSL VPNs. The contents of the list depends on the filter options selected. Click the icons beside an SSL VPN to edit or delete.

Related links

System Settings on page 140
Add SSL VPN Service on page 169

Add SSL VPN Service

Navigation: **System Settings** > **Services** > **Add/Edit Service**

Click **Add/Edit Service** to open the Add SSL VPN Service page where you can provision a location. When you click **Add/Edit Service**, you are prompted to specify a server.

This type of service provides a secure tunnel between the IP Office system at a customer site and an Avaya VPN Gateway (AVG) installed at a service provider site. This secure tunnel allows service providers to offer remote management services to customers, such as fault management, monitoring, and administration. SSL VPN Services are supported by IP500 V2 and Linux based IP Office systems only. For full details on how to configure and administer SSL VPN services, refer to the Avaya IP Office SSL VPN Solutions Guide.

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.

For Server Edition, this type of configuration record can be saved as a template and new records created from a template.

These settings are mergeable. Changes to these settings do not require a reboot of the system.

Service

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.
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.

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.

Field	Description
	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 169

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.

Related links

System Settings on page 140
Add Alternate Route on page 172

Add Alternate Route

Navigation: **System Settings** > **Alternate Route Selection** > **Add/Edit Alternate Route**

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.

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 are mergeable. 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.

Table continues…

Field	Description
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's Dial Delay Time (System | Telephony | Telephony) value is used.
Secondary Dial Tone	Defaults = Off. When on, this setting instructs the system to play secondary dial tone to the user. The tone used is set by the field below. The tone used is set as either **System Tone** (normal dial tone) or **Network Tone** (secondary dial tone). Both tone types are generated by the system in accordance with the system specific locale setting. Note that in some locales normal dial tone and secondary dial tone are the same. When **Secondary Dial Tone** is selected, the ARS form will return tone until it receives digits with which it can begin short code matching. Those digits can be the result of user dialing or digits passed by the short code which invoked the ARS form. For example with the following system short codes: In this example, the 9 is stripped from the dialed number and is not part of the telephone number passed to the ARS form. So in this case secondary dial tone is given until the user dials another digit or dialing times out. • **Code**: 9N • **Telephone Number**: N • **Line Group ID**: 50 Main In this example, the dialed 9 is included in the telephone number passed to the ARS form. This will inhibit the use of secondary dial tone even if secondary dial tone is selected on the ARS form. • **Code**: 9N • **Telephone Number**: 9N • **Line Group ID**: 50 Main
Check User Call Barring	Default = Off If enabled, the dialing user's **Outgoing Call Bar** setting and any user short codes set to the function **Barred** are checked to see whether they are appropriate and should be used to bar the call.
Description	Default = Blank. Maximum 31 characters. 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.

Table continues…

Field	Description
	Short codes can be used to take an ARS form in and out of service. This is done using the short code features Disable ARS Form and Enable ARS Form and entering the ARS Route ID as the short code **Telephone Number** value.
Out of Service Route	Default = None. This is the alternate ARS form used to route calls when this ARS form is not in service.
Time Profile	Default = None. Use of a ARS form can be controlled by an associate time profile. Outside the hours defined within the time profile, calls are rerouted to an alternate ARS form specified in the Out of Hours Route drop-down. Note that the Time Profile field cannot be set until an Out of Hours Route is selected.
Out of Hours Route	Default = None. This is the alternate ARS form used to route calls outside the hours defined within the Time Profile selected above.
Short Codes	Short codes within the ARS form are matched against the "Telephone Number" output by the short code that routed the call to ARS. The system then looks for another match using the short codes with the ARS form. Only short codes using the following features are supported within ARS: **Dial**, **Dial Emergency**, **Dial Speech**, **Dial 56K**, **Dial64K**, **Dial3K1**, **DialVideo**, **DialV110**, **DialV120** and **Busy**. Multiple short codes with the same **Code** field can be entered so long as they have differing **Telephone Number** and or **Line Group ID** settings. In this case when a match occurs the system will use the first match that points to a route which is available.
Alternate Route Priority	Default = 3. Range = 1 (low) to 5 (high). If the routes specified by this form are not available and an **Alternate Route** has been specified, that route will be used if the users priority is equal to or higher than the value set here. User priority is set through the **User | 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, 1 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.

Table continues…

Code	Cause Code
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 172

Chapter 7: Security Manager

Navigation: **Security Manager**

Related links

Service Users on page 177
Certificates on page 180

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 177
Synchronize Security Database on page 177
Add Service User on page 178
User Preferences on page 179

Synchronize Security Database

Navigation: **Security Manager** > **Service Users** > **Synchronize Security Database**

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 177

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.
Account Status	Default = Enabled. Displays the current service user account status (correct at the time of reading from the system). The options are: • **Enabled** This status is the normal non-error state of a service user account. This setting can be selected manually to re-enable an account that has been disabled or locked. Note that re-enabling a locked account will reset all timers relating to the account such as **Account Idle Time**. • **Force New Password** This status can be selected manually. The service user is then required to change the account password when they next log in. Until a password change is successful, no service access is allowed. Note that the user must be a member of a Rights Group that has the Security Administration option **Write own service user password** enabled. • **Disabled** This status prevents all service access. This setting can be selected manually. The account can be enabled manually by setting the **Account Status** back to **Enabled**. • **Locked – Password Error** This status indicates the account has been locked by the **Password Reject Action** option **Log and Disable Account** on the security General Settings tab. The account can be enabled manually by setting the **Account Status** back to **Enabled**. • **Locked - Temporary** This status indicates the account is currently locked temporarily by the **Password Reject Action** option **Log and Temporary Disable** on the security General Settings tab. The account can be enabled manually by setting the **Account**

Table continues…

Field	Description
	Status back to **Enabled**, otherwise the service user must wait for the 10 minute period to expire. • **Locked - Idle** This status indicates the account has been locked by passing the number of days set for the Account Idle Time on the security General Settings tab without being used. The account can be enabled manually by setting the **Account Status** back to **Enabled**. • **Locked - Expired** This status indicates the account has been locked after passing the Account Expiry date set below. The account can be enabled manually by setting **Account Status** back to **Enabled**, and resetting the **Account Expiry** date to a future date or to **No Account Expiry**. • **Locked – Password Expired** This status indicates the account has been locked after having not been changed within the number of days set by the Password Change Period option on the security General Settings tab. The account can be enabled manually by setting the **Account Status** back to **Enabled**.
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 177

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 177

Certificates

Navigation: **Security Manager** > **Certificates**

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 *IP Office SSL VPN Solutions Guide*) 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.

Field	Description
Identity Certificate: The **Identity Certificate** is an X.509v3 certificate that identifies the system to a connecting client device (usually a PC running a application). This certificate is offered in the TLS exchange when the system is acting as a TLS server, which occurs when accessing a secured service. An identity certificate can also be used when IPOffice acts as TLS client and the TLS server requires IPOffice to send client certificate. By default, the system's own self-generated certificate is used. A certificate is advertised when the **Service Security Level** is set to a value other than **Unsecure Only**. The certificate can take up to one minute to generate. During this time, normal system operation is suspended. You can regenerate the certificate by clicking **Delete**. Regenerating a certificate may impact system performance. Perform this action during a maintenance window. Use the **Set** command to replace the system generated certificate with an external certificate.	
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.
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

Table continues…

Field	Description
	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.
Private Key	Default = System generated random value. A blank field is displayed. Use this field to enter a private key. If you set a private key, it is only used in the case of self-signed certificates. To set the private key, you must click **Delete** to generate a new certificate.
Issued to	Default = IP Office identity certificate. Common name of issuer in the certificate.
Default Subject Name	Default = None.
Subject Alternative Name(s)	Default = None.
Set	Set the current certificate and associated private key. The certificate and key must be a matching pair. 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. 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-224, 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. **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.

Table continues…

Field	Description
View	View the current 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	Deletes the current certificate and the system generates a new certificate. This can take up to one minute to generate. During this time, normal system operation is suspended. Regenerating a certificate may impact system performance. Perform this action during a maintenance window.
Use Different Identity Certificate for Telephony	Default = Off. When set to Off, all secure communications use the default identity certificate and settings. When set to On, telephony related secure communications use a separate identity certificate that must by set by the Security Administrator.
Received Certificate Checks (Management Interface)	Default = None. This setting is used configuration administration connections to the system by applications such as Manager. When the **Service Security Level** of the service being used is set to **High**, a certificate is requested by the system. The received certificate is tested as follows: • **None:** No extra checks are made (The certificate must be in date). • **Low:** Certificate minimum key size 1024 bits, in date. • **Medium:** Certificate minimum key size 1024 bits, in date, match to store. • **High:** Certificate minimum key size 2048 bits, in date, match to store, no self signed, no reflected, chain validation.
Received Certificate Checks (Telephony Endpoints)	Default = None. This setting is used with IP telephony endpoints connecting to the system. This setting is used by IP Office to validate the identity certificate offered by the other end of TLS connection. IP Office does not support mutual authentication for SIP terminals (an identity certificate is not installed in all SIP terminals). Therefore, IP Office does not require a client certificate from a SIP terminal, only SIP and SM trunks. The received certificate is tested as follows: • **None:** No extra checks are made (The certificate must be in date). • **Low:** Certificate minimum key size 1024 bits, in date. • **Medium:** Certificate minimum key size 1024 bits, in date, match to store. • **High:** Certificate minimum key size 2048 bits, in date, match to store, no self signed, no reflected, chain validation.
Trusted Certificate Store: Installed Certificates	Default = A set of fixed Avaya provided Intermediate CA or Root CA certificates.

Table continues…

Field	Description
	The certificate store contains a set of trusted certificates used to evaluate received client certificates. Up to 25 X.509v3 certificates may be installed. The source may be: • Current User Certificate Store. • Local Machine Certificate Store. • File in one of the following formats: - PKCS#12 (.pfx) - PEM (.cer) - password protected PEM (.cer) - DER (.cer) - password protected DER (.cer) • Pasted from clipboard in PEM format, including header and footer text.
Add	Set the current certificate and associated private key. The certificate and key must be a matching pair. 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-224, 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 current 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 current certificate.
SCEP Settings	

Table continues…

Field	Description
The Simple Certificate Enrollment Protocol is a protocol intended to ease the issuing of certificates in a network where numerous devices are using certificates. Rather than having to individually administer the certificate being used by each device, the devices can be configured to request a certificate using SCEP. These settings are relevant for IP Office Branch deployments. These settings are not used in IP Office Standard mode.	
Active	Default = Off.
Request Interval (seconds)	Default = 120 seconds. Range = 5 to 3600 seconds.
SCEP Server IP/ Name	Default = Blank.
SCEP Server Port	Default = 80 for HTTP and 443 for HTTPS.
SCEP URI	Default = /ejbca/publicweb/apply/scep/pkiclient.exe
SCEP Password	Default = Blank.

Related links

Security Manager on page 177

Chapter 8: Applications

Navigation: **Applications**

Related links

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. 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>/WebMgmtEE/WebManagement.html`.
2. Log on as **Administrator**.
3. In Web Manager, select **Tools** > **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 **Tools** > **Service Users**.
9. Click **Synchronize Security Database**.
10. Select **Solution** and click **IP Office Manager**.

Related links

Applications on page 185

Launch Manager

Navigation: **Applications** > **IP Office Manager**

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.

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.

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 185 Synchronizing Server Edition Passwords in .

Related links

Applications on page 185

Voicemail Pro — System Preferences

Navigation: **Applications** > **Voicemail Pro — System Preferences**

Related links

Applications on page 185
General on page 187
Email on page 189
Housekeeping on page 191
SNMP Alarm on page 192
Outcalling on page 193
Voicemail Recording on page 194
Syslog on page 194
Alarms on page 195
User Group on page 196

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
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.

Table continues…

Field	Description
Min. Message Length (secs)	Default = 0 seconds (in IP Office mode) and 3 seconds (in Intuity mode). Use this field to set a restriction on the minimum length for a message. The minimum value that you can set is 0 seconds, and the maximum value is 10 seconds. Messages that are of shorter length than the set minimum length are deleted immediately. In IP Office mode, this field is unavailable.
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.
Min. Password Length	Default = 0 (in IP Office mode) and 2 (in Intuity mode). Use this field to set a restriction on the minimum length of a mailbox password. The minimum value that you can set is 0 in IP Office mailbox mode and 2 in Intuity emulation mode. The maximum value is 15. The Min. Password Length field is unavailable on distributed Voicemail Pro servers, as the password length for mailboxes is controlled by the central Voicemail Pro server.
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.
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.
Failback Option	Default = Manual 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.
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.
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.

Related links

Voicemail Pro — System Preferences on page 187

Email

Navigation: **Applications** > **Voicemail Pro — System Preferences** > **Email**

Note:

If you are using Voicemail Pro in a distributed environment, a distributed server delivers a recorded message to the central Voicemail Pro server on completion of the recording. However, the presentation to the Voicemail Pro server for message waiting indication (MWI) and access via telephone might be delayed because of the internal processing of the message and the network latency. The delay might be up to 2 minutes in high traffic situations.

Field	Description
Enable MAPI/EWS	Default = MAPI <Description> The options are: • MAPI • EWS • None
MAPI Service	
Address	Default = Blank.
Port	Default = 50792
SMTP Sender These settings are used to configure the SMTP server and the server account that Voicemail Pro server uses for sending e-mails through SMTP. Multiple servers can be configured. The first entry specifies the default SMTP server used for sending e-mails if there is no other entry matching the domain specified in the e-mail destination address. Additional servers can be added when different settings are required for sending e-mails to specific domains. For example, the default can be configured for the customer's internal network exchange server with additional entries added for e-mails to external e-mail domain addresses such as yahoo.com. VPNM, distributed Voicemail Pro servers, and primary/backup Voicemail Pro servers all use SMTP to exchange information and messages between Voicemail Pro servers. When that is the case, the first entry in the SMTP Sender list must be the one used and needs to be configured for that service with the domain and server setting both matching the IP address or fully-qualified domain of the Voicemail Pro server.	
Logging	Default = No. Set to Yes to enable SMTP logging. For information on SMTP logging see *Avaya IP Office Platform Voicemail Pro Administration*.
Add SMTP Sender	Click to open the SMTP Sender Configuration window.
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:**

Table continues…

Field	Description
	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
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

Table continues…

Field	Description
	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 187

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 **LIFO** (Last In First Out) or **FIFO** (First In First Out)

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.
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 187

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**.

Table continues…

Field	Description
	• For Voicemail Pro Server Edition, IP Office sends SNMP alarms based on the percentage of the available free space of the total disk space. The SNMP alarms are as follows: - **Disk State Critical**: Free disk space is less than 5% - **Disk State OK**: Free disk space is between 5 to 10% - **Disk State Free**: Free disk space is greater than 10% - **Disk State Stop Recording**: Free disk space is 0.
Default Settings	Return to the default alarm settings. Alarm Threshold Level is reset to 60. The Space OK level is reset to 90. The Critical Alarm level is reset to 30.

Related links

Voicemail Pro — System Preferences on page 187

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 187

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 187

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 = Blank. A UDP port number at which the syslog server is listening for syslogs.

Related links

Voicemail Pro — System Preferences on page 187

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).

Table continues…

Field	Description
	If a number of retires is specified, this option can be used to select the number of minutes between repeated alarm attempts until the alarm is cleared.
Enable Cancel Code	Default = No. When off, the alarm is cleared if the alarm call is answered. When on, a dialing code can be specified. If the correct code is not dialed in response to an alarm, the alarm is not cleared and will repeat if retries have been specified.
Cancel Code	Default = * , Range = Up to 4 digits. used to enter the dialing required to clear the alarm call. The value * will match any dialing. To cancel the alarm, the cancel code must be entered followed by the hash key (#). The file used to play the alarm message must mention the cancel code and the fact that cancel code must be followed by the hash key (#).
Alarms The following additional fields are displayed in the Alarms table.	
Created	
Next Activation	
Type	
When	
Number	

Related links

Voicemail Pro — System Preferences on page 187

User Group

Navigation: **Applications** > **Voicemail Pro — System Preferences** > **User Group**

Field	Description
User Group	
Name	

Related links

Voicemail Pro — System Preferences on page 187

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:

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

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 185

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:

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 185

WebRTC Configuration

Navigation: **Applications** > **WebRTC Configuration**

Related links

Applications on page 185
System Settings on page 198
SIP Server Settings on page 198

Media Gateway Settings on page 199

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 • **Alarm** • **Error** • **Warn** • **Info** • **Debug**

Related links

WebRTC Configuration on page 197

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.

Table continues…

Field	Description
	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 197

Media Gateway Settings

Navigation: **Applications** > **WebRTC Configuration** > **Media Gateway Settings**

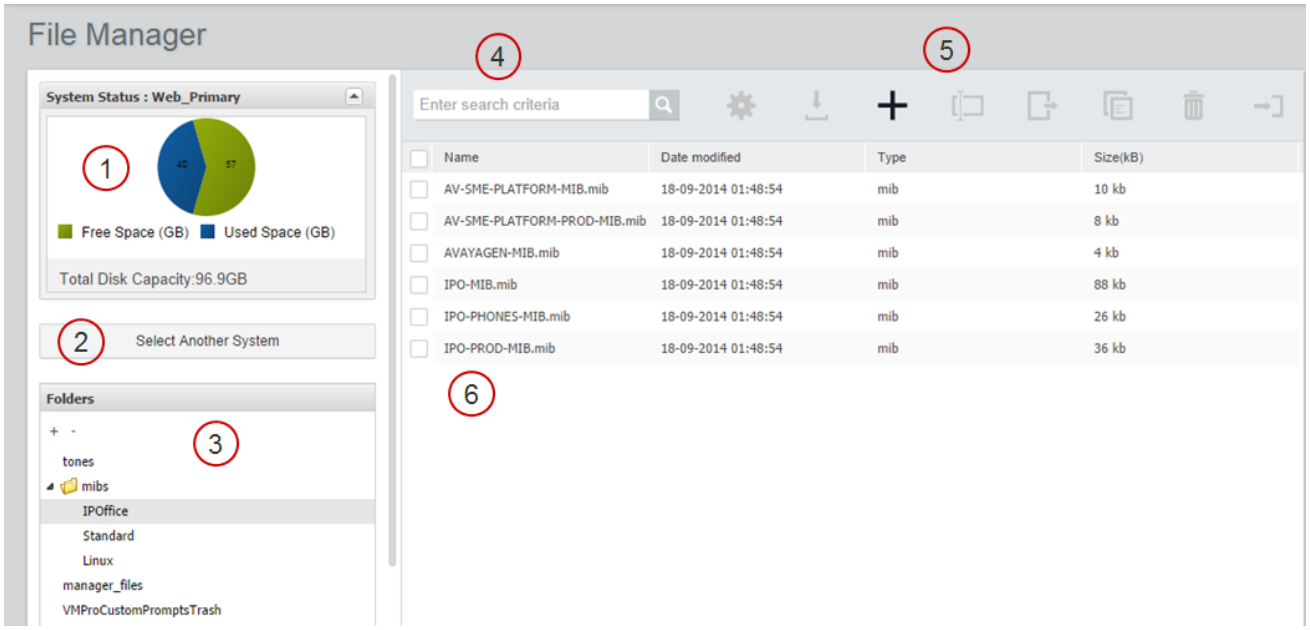
File	Description
RTP Port Range (Private) Minimum	Default = 58002. Minimum RTP port value used for WebRTC media termination from the private interface.
RTP Port Range (Private) Maximum	Default = 60002. Maximum RTP port value used for WebRTC media termination from the private interface.
RTP Port Range (Public) Minimum	Default = 56000. Minimum RTP port value used for WebRTC media termination from the public interface.
RTP Port Range (Public) Maximum	Default = 58000. Maximum RTP port value used for WebRTC media termination from the public interface.
Codecs — Audio	The audio codecs used by the WebRTC Gateway, listed by priority. Use the arrows to change the priority. The options are: 1. PCMU 2. PCMA 3. telephone-event
Codecs — Video	The audio codecs used by the WebRTC Gateway. The options are: 1. VP8
DTMF Payload Type	Default = 101. RFC2833 default payload type used by the WebRTC Gateway.
STUN Server Address	Default = Blank. STUN server address (optional).
STUN Server Port	Default = Blank. STUN server port (optional).
TURN Server Address	Default = Blank. TURN server address (optional).
TURN Server Port	Default = Blank. TURN server port (optional).
TURN User Name	Default = Blank. TURN user name (optional).
TURN Password	Default = Blank. Password for Turn user name, if used.
Enforce TURN	Default = No. When set to Yes, enforces media traffic via the TURN server.

Related links

WebRTC Configuration on page 197

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 185

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.

Related links

Applications on page 185

Chapter 9: Backup and restore

Backup overview

Related links

Backup and restore policy on page 203
Backup and Restore location on page 204
Backup data sets on page 205
Disk Usage on page 206
Managing Disk Space for Backup and Restore on page 207

Backup and restore policy

It is essential to implement a considered, robust and secure backup policy before any failure or other restore requirements. 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 implemented. Consider the following aspects as a part of such a policy:

- Ignition settings. These should 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.
- License key data: All ADI license key files should 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 – Primary and Application Server only
- Periodic configuration backup for Voicemail Pro – Primary only
- Periodic voice mailbox and recording data backup – Primary only
- The timing of backup operation: This should be done when little or no traffic is present on the target system, 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. 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:

  backup of an Avaya Linux server does not include any local backup data.

- Security of backup data communication
- Backup prior to any software upgrade
- Retention of backup data for older software versions should a *downgrade* need to be considered.

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 and a single manual backup instance, after which thesystem overwrites the oldest set. These instances are for each backup server and regardless of the backup data set; for example two weekly separate backup tasks of all IP Office configurations and Voicemail configuration overwrite the first set after 7 weeks.

Related links

Backup overview on page 203

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
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,	SFTP supported by Linux-based components. Enabled by default.

Table continues…

			Root (not recommended)	
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 203

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
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	

Table continues…

	• Call flows • Voice mailbox contents • Call recordings	
Selective Voicemails		

Related links

Backup overview on page 203

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 2: Server disk capacity

Server	R620	DL360	DL120	R210	OVA (default)	OVA (max supported) [1]	UCM
Nominal disk capacity (GB)	600	300	250	500	100	166	32
Max solution users	2,500	2,000	1,500	1,500	750	2,500	50

1. Requires disk size increase.

Table 3: 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

Table continues…

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 4: 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 203

Managing Disk Space for Backup and Restore

Except for a UCM server, 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:

- one-X Portal is not active.
- VMPro is un-installed.

  Note:

  Use the Web Control application to un-install Voicemail Pro.
- The disk capacity (total disk space) is 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 virtual machine solely as a backup server if:

- one-X Portal is not active.
- VMPro is un-installed.

Note:

Use the Web Control application to un-install Voicemail Pro.

Related links

Backup overview on page 203

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 backup, 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 backup 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 backup immediately:
     a. In **Select Remote Server** drop down list, select the remote server that you have set.
   - To backup 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 backup 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 backup 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 backup.
- To backup 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 backup.
- To backup 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 backup.
- To backup Contact Recorder sets:
  a. In the **Select Remote Server** drop down list, select the remote server that you have set.
  b. In the **Select Contact Recorder Sets** list, select the CSIPO set that you want to backup.

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 backup 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 more information about installing, configuring IP Office Server Edition using ignition process and Manager, see Chapter 2 of this document.

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: LDAP Synchronization

Related links

[Performing LDAP Synchronization](#) on page 212
[Creating a User Provisioning Rule for LDAP Synchronization](#) on page 213

Performing LDAP Synchronization

Procedure

1. 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 212

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. 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.
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 212

Chapter 11: 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 214

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 214

Index

A

B

C

D

E

F

G

I

L

M

N

O

P

R

S

T

U

V

W