Administering Avaya IP Office™ Platform with Manager

Release 9.1.0
Issue 10.03
February 2015

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: Introduction

Related Links

Purpose

This document contains descriptions of the configuration fields and the configuration procedures for administering Avaya IP Office using the Manager application.

Related Links

Introduction on page 18

Intended audience

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

Related Links

Introduction on page 18

Documentation resources

For a listing of documentation resources related to IP Office, see *IP Office Documentation Library*. Download documents from the Avaya Support website at http://support.avaya.com.

Related Links

Introduction on page 18

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Related Links

Introduction on page 18

Document changes since last issue

New Reference Documents

Content previously included in this document has been moved into separate reference documents. This content is available in pdf format from the Avaya support site and in the IP Office Knowledge Base.

Short Codes and Button Actions:

Detailed information on short codes and button actions has been moved to *Avaya IP Office Platform™ Short Code and Button Action Reference*.

This document continues to contain overview and configuration information:

- Short Code Overview on page 749
- Button Programming Overview on page 768

Locales:

Locale information has been moved to *Avaya IP Office Platform™ Locale Settings Reference*.

Table 1: Changes summary for release 9.0.0

Section	Summary of changes
Incoming Call Route	In the *Incoming Call Route* section, under the subtitle *Outgoing Caller ID Matching*, the following statement has been added. 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

Table continues…

Section	Summary of changes
	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.
Incoming Call Route consolidated records	Starting with release 9.1, Incoming Call Routes are not longer supported as consolidated records. This change is reflected in the description for File | Preferences | Consolidate Solution to Primary Settings and in the description for Record Consolidation in the chapter Working with the Server Edition Manager User Interface.
NoUser User Source Numbers	The following NoUser User Source Number has been added: REPEATING_BEEP_ON_LISTEN
Configuring General System Settings	Template information has been consolidated in the Configuring General System Settings, under Working with Templates on page 547.
Configuration Mode Field Descriptions	Default settings on **System | Telephony | Telephony** The following settings are now set by default to On. • **Inhibit Off-Switch Forward/Transfer** • **Drop External Only Impromptu Conference**
	The following statement has been added to the field **Line | SIP Line | Transport | Use Network Topology Info**. If no STUN server address is set for the interface, then the **Binding Refresh Time** (**System | LAN | Network Topology**) is ignored by SIP Lines when calculating the periodic OPTIONS timing unless the **Firewall/NAT Type** is set to **Open Internet**.
	The tab **System | ACCS** has been renamed **System | Contact Center**.
Security Mode Field Descriptions	The field description information for the tab **System | Certificates** has been revised and updated.
File | Advanced | Initial Configuration	The Initial Configuration section now contains the following note. **Note:** The Initial Configuration utility changes the security settings. Therefore, the user running the utility must have security read/write rights.

Related Links

Introduction on page 18

What's New in Release 9.1

SIP Line Simplification

SIP Line configuration parameters have been reorganized. The standard line tabs now contain only those parameters that are commonly used for most deployment scenarios. A new SIP Advanced tab and a new SIP Engineering tab now contain the less common configuration parameters, usually reserved for expert users and support personnel. See SIP Line on page 336.

SIP Line Silence Suppression

The **SIP Line | Advanced** tab now contains a **Send SilenceSupp=Off** check box. This is used for the G711 codec. When checked, the silence suppression off attribute is sent in SDP on this trunk.

IP DECT Line Resiliency

The **IP DECT Line | Gateway** tab now contains configuration fields for **Enable Resiliency**.

If resiliency is enabled, you can enable the option **Backs up my IP DECT Phones** on the **IP Office Line tab**.

Suppress NoCallerId Alarm

The NoCallerId alarm can be suppressed using a NoUser source number. For a description of source numbers, see **User | Source Numbers**.

For the procedure to suppress the alarm, see Suppressing the NoCallerId Alarm on page 660.

Directory Overrides Barring

Call barring can be overridden for numbers entered in the external directory. The configuration setting Directory Overrides Barring has been added to the **System | Telephony | Telephony** tab.

For configuration information, see Overriding Call Barring on page 606.

Message Waiting Indicator for Analog Trunks

A Message Waiting Indicator (MWI) using a Bellcore FSK MWI signal is now supported for analog trunks that terminate on an ATM4U-V2 card.

The configuration setting is located at **Extension | Analog | Message Waiting Lamp Indication Type**.

For a configuration procedure, see Message Waiting Indication for Analogue Trunks on page 657.

Toll Bypass Prevention

A configuration procedure has been added for preventing toll bypass. See PreventingToll Bypass on page 605.

Web Collaboration

The **User | User** tab, now contains a **Web Collaboration** check box. When enabled, it allows the user to use the Web Collaboration application.

Answer and Disconnect Supervision

The **System | Telephony | Tones and Music** tab now contains a **Analog Trunk VAD** check box. Select this option to enable Voice Activity Detection (VAD) for analog trunks terminating on the ATM4U-V2 card. VAD functionality provides a Call Answer signal triggered by voice activity.

Third Party Voice Quality Monitoring

The **RTCP collector IP address for phones** field has been added to the **LAN | VoIP** tab. This setting enables you to send the RTCP data collected to a third party QoS monitoring application.

Enable Remote Working

On the **User | User** tab, 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.

Outcalling Control

On the **System | Voicemail** tab, you can use the **Outcalling Control** setting to enable or disable system wide outcalling on Voicemail Pro.

Authorization Codes

The following changes have been made to authorization codes.

- Authorization codes are now enabled by default.
- SMDR field 19 shows n/a regardless of whether an authorization code was used.
- Authorization codes can no longer be associated with User Rights. An authorization code must be associated with a user.

Note:

In release 9.1, authorization codes can no longer be associated with User Rights. If an authorization code was configured in relationship with User Rights in an earlier release configuration, this authorization code will be lost during upgrade. The administrator must re-configure the authorization code, after upgrade. The authorization code must be associated with a user.

The authorization code configuration settings are described on the page for the **Authorization Code** tab.

For a configuration procedure, see Configuring Authorization Codes on page 590.

Mergeable Settings

On the **System | LAN1 | VoIP** tab, under the **SIP Registrar Enable** settings, the **Auto-create Extn/User** setting is now mergeable. Changing this setting does not require a reboot.

When creating an IP DECT line, the settings are now mergeable. You can also remove an IP DECT line without rebooting.

Support for IP400 and IP500 Hardware Discontinued

The IP400 and IP 500 platforms are not supported in release 9.1.

Alarms

The following alarms have been added. For details, see **System | System Events**.

- Log stamped
- CPU warning/critical
- Memory use warning/critical

Security

User accounts:

- The Manager and Operator default service users have been removed.
- The following administrative accounts are disabled by default:
  - IPDECTService
  - BranchAdmin
  - BuisinessPartner

- Maintainer

Phone Login PIN:

Voicemail PIN:

You can now configure a phone login PIN using the **Login Code Complexity** fields on the **System | Telephony** tab.

You can now configure a voicemail PIN using the **Voicemail Code Complexity** fields on the **System | Voicemail** tab.

Auto-create User and Auto-create Extension:

The default setting is now **Off** for all Auto-create fields.

LAN Settings:

On the System | LAN1 / LAN2 tabs, the following settings have changed.

Field	Default
SIP Registrar Enable	Default = Off.
RTP Port Number Range	IP 500 v2 default = 4000. Range = 46750 to 50750. Linux default = 10000. Range = 40750 to 50750

Security General Settings:

On the **Security Settings | General Settings** tab, the following default values have been changed.

Field	Default
Security Administrator	
Password	Range = 8 to 31 characters.
Minimum Password Complexity	Default = Medium.
Previous Password Limit (Entries)	Default = 4.
Service User Details	
Minimum Password Length	Range 8 to 31 characters.
Password Reject Action	Default = Log and Temporary Disable.
Minimum Password Complexity	Default = Medium.
Expiry Reminder Time	Default = 10.
IP Office User Details	
Password Enforcement	Default = On.
Minimum Password Length	Range 8 to 31 characters.
Minimum Password Complexity	Default = Medium

Table continues…

Field	Default
Password Reject Limit	Default = 5.
Password Reject Action	Default = Log and Temporary Disable.

Security Settings | System | Unsecured Interfaces:

The following values have changed.

Field	Default
The fields **TFTP Configuration Read** and **TFTP Configuration Write** replaced with **TFTP Server**	Default = On. This setting enables or disables the TFTP server.
TFTP Directory Read	Default = Off. Also disabled if **TFTP Server** is set to **Off**.
TFTP Voicemail	Disabled if **TFTP ServerIt** is set to **Off**.
The **EConf** field has been removed.	
DevLink	Default = On.
The **Real Time Interface** field has been removed.	

Related Links

Introduction on page 18

Chapter 2: Overview

This documentation covers the use of the Avaya IP Office Manager. Manager runs on a Windows PC and connects to the IP Office system via Ethernet LAN or WAN connections.

Important:

Manager is an off-line editor. It receives a copy of the system's current configuration settings. Changes are made to that copy and it is then sent back to the system for those changes to become active. This means that changes to the active configuration in the system that occur between Manager receiving and sending back the copy may be overwritten. For example, this may affect changes made by a user through their phone or voicemail mailbox after the copy of the configuration is received by Manager.

Related Links

Manager Modes on page 25

Manager Modes

The menus and options displayed by Manager vary depending on the actions you are performing. Manager runs in the following modes.

Basic Edition Mode

This is the mode used when a Basic Edition configuration is opened. Basic Mode includes systems running Partner, Norstar, or Quick Mode. For information on administering a Basic Edition system, see the *IP Office Basic Edition Manager*.

Security Configuration Mode

Manager can be used to edit the security settings of IP Office systems.

Standard Mode Configuration Mode

This is the mode used when a Standard Mode configuration is opened. Standard Mode includes systems running Standard, Preferred, or Advanced Edition.

Server Edition Configuration Mode

This is the mode used when a Server Edition network configuration is opened.

Small Community Network Management

Manager supports loading the combined configurations from systems in a Small Community Network.

IP Office Shell Server Mode

The IP Office Shell Server is a single installation of selected IP Office applications running on Linux. You can use Manager to administer an IP Office Shell Server.

Embedded File Management

For systems with a memory card installed, Manager can be used to view and manage the files stored on the card. Embedded File Management can be accessed by selecting **File | Advanced | Embedded File Management**.

Upgrade Wizard

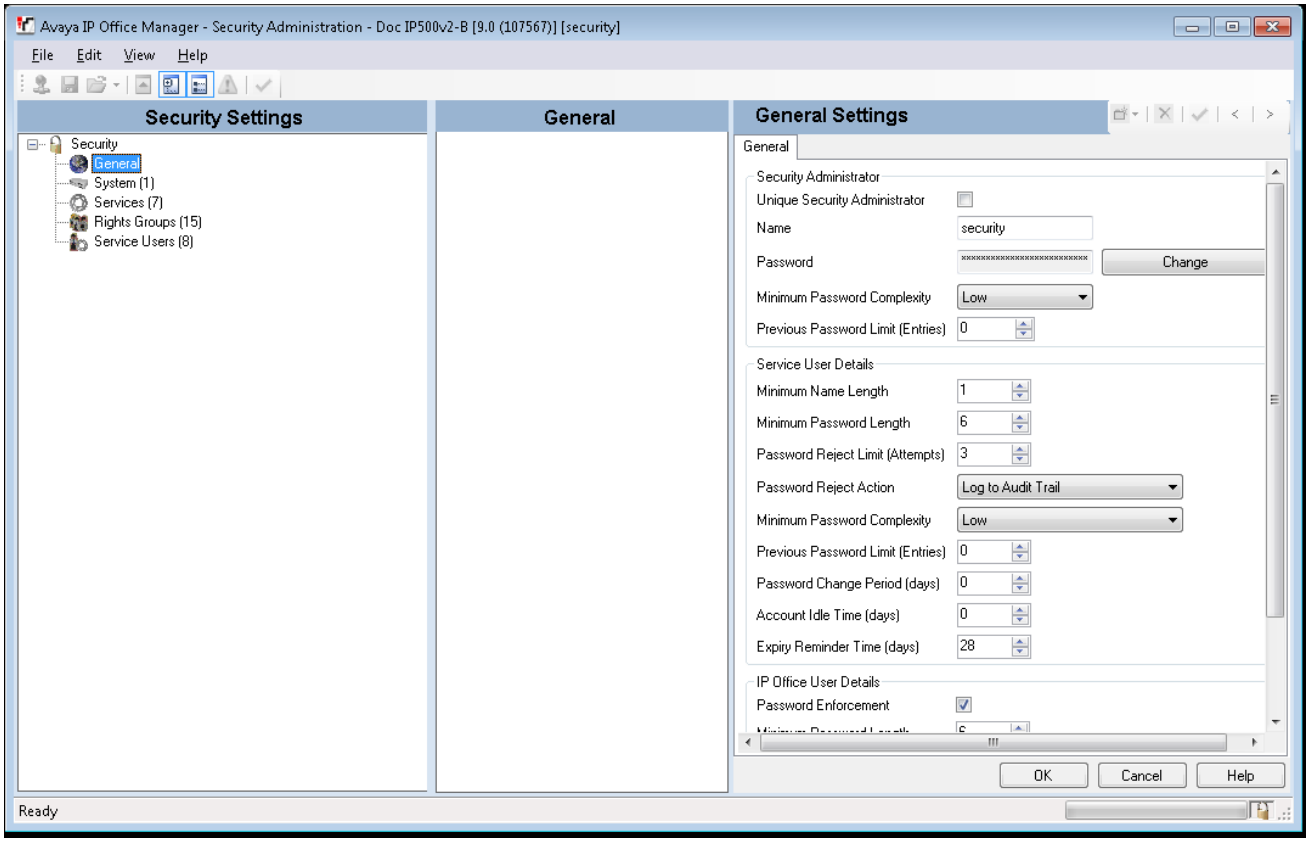
The Upgrade Wizard is a component of Manager used to upgrade the firmware run by the system.

Related Links

Overview on page 25
Security Configuration Mode on page 26
Standard Mode Configuration Mode on page 27
Server Edition Configuration Mode on page 29
Shell Server Mode on page 30
Backward Compatibility on page 31

Security Configuration Mode

When Manager is in Security Mode, the screen elements shown are available.

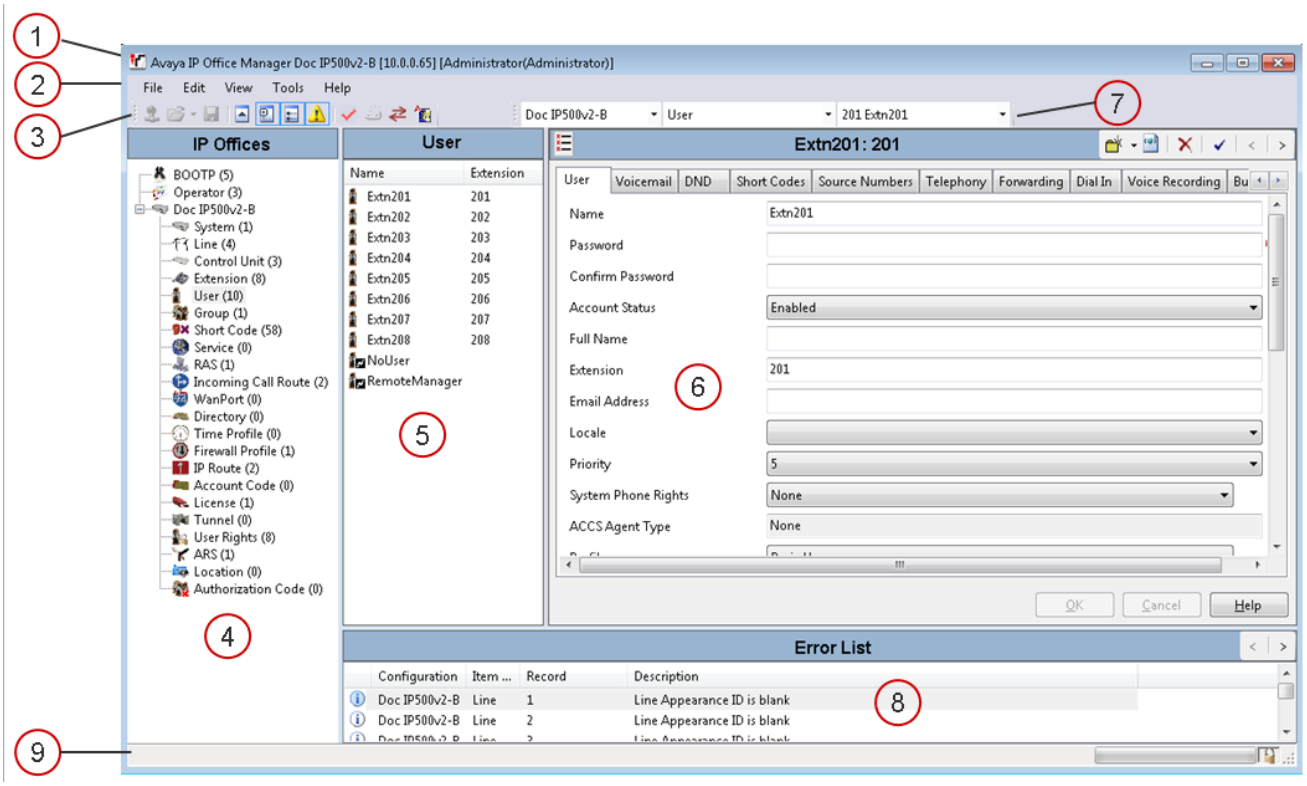


Related Links

[Manager Modes](#) on page 25

Standard Mode Configuration Mode

When Manager is in configuration mode, the screen elements shown are available. Some of these elements can be customized, moved and hidden.



Manager Configuration Mode Screen Elements

1	Title Bar In addition to the application name, when configuration settings are loaded from a system, the title bar displays the user name used to load the settings and the operator view applied.
2	Menu Bar The options available with the drop down menus provided here change according to whether Manager has a set of configuration or security settings loaded or not.
3	Main Toolbar This toolbar provides icon shortcuts to the most frequently required configuration setting actions.
4	Navigation Pane This pane shows icons for the different types of record that the configuration can contain. Each type is followed by the number of records of that type already in the configuration. Selecting an icon displays the matching records in the group pane and navigation toolbar.
5	Group Pane This pane lists all the records that match the type selected in the navigation pane or navigation toolbar. The list can be sorted by clicking on column heading. Selecting a record in this pane displays its details in the details pane.
6	Details Pane

Table continues…

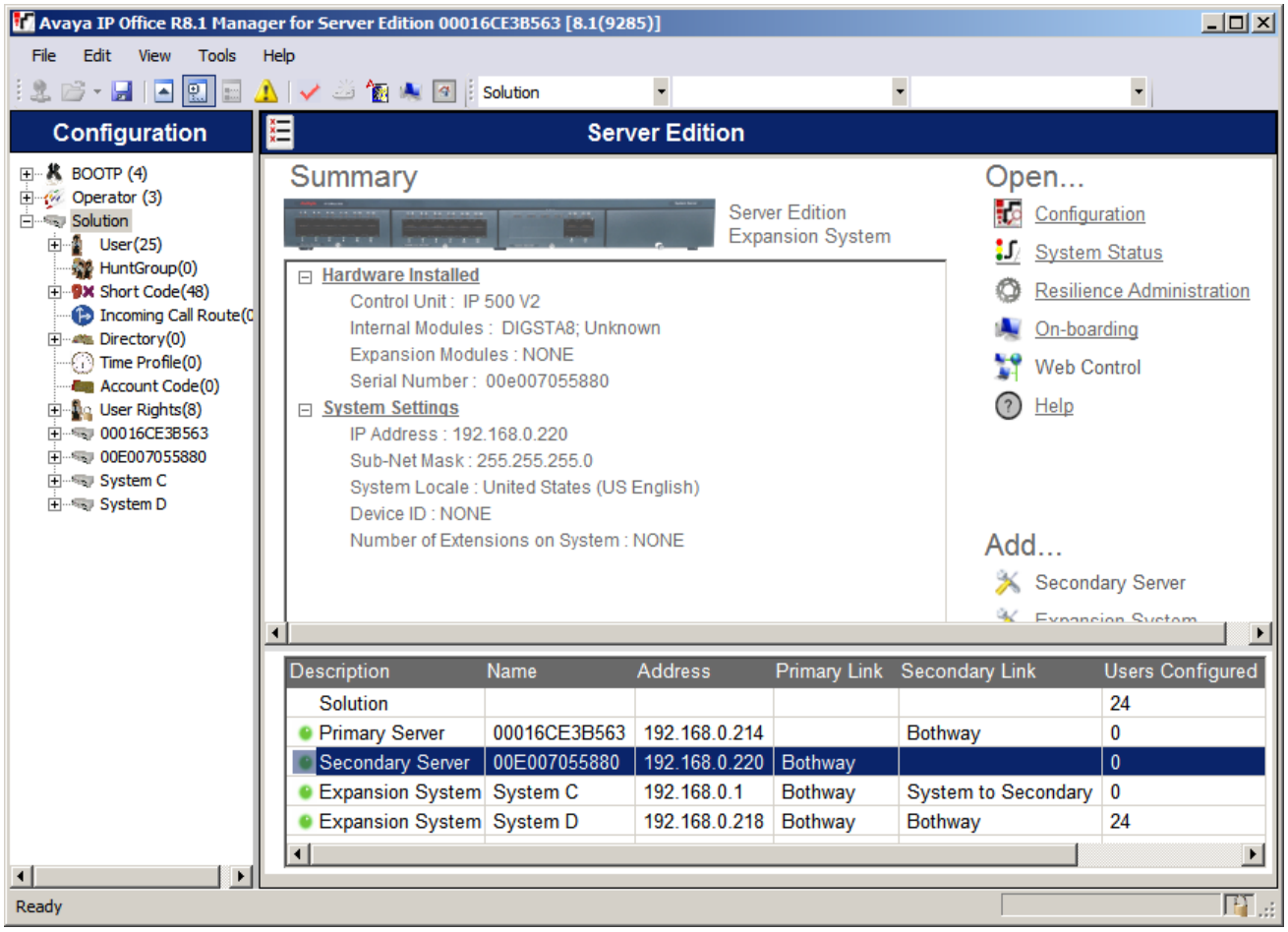
	This pane shows the configuration settings for a particular record within the configuration. The record is selected using the navigation toolbar or using the navigation pane and group pane.
7	Navigation Toolbar This toolbar provides a set of drop downs which can be used to navigate to particular records in the configuration settings. The selected options in the navigation pane, the group pane and the details pane are synchronized with the navigation toolbar and vice versa. This toolbar is particularly useful if you want to work with the group pane and or navigation pane hidden in order to maximize the display space for the details pane.
8	Error Pane This pane shows errors and warnings about the configuration settings. Selecting an item here loads the corresponding record into the details pane.
9	Status Bar This bar display messages about communications between Manager and systems. It also displays the security level of the communications by the use of a padlock icon.

Related Links

Manager Modes on page 25

Server Edition Configuration Mode

When the configuration from a Server Edition solution is loaded into Manager, Manager switches to Server Edition mode operation.



Related Links

Manager Modes on page 25

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

Manager Modes on page 25

Backward Compatibility

Manager is part of the IP Office Admin Suite of programs. The Manager application can be used to manage configurations from systems running earlier software releases. Manager adjusts the settings and fields that it shows to match the core software level of the system.

Manager is able display systems with software levels it does not support in the **Select IP Office** discovery menu, however those systems are indicated as not supported.

Backwards compatibility is only supported for General Availability releases of IP Office software. It is not supported for private builds.

Note that this document describes the current release. If you are running an earlier software release, obtain the Manager document for the specific release from the Avaya support site. The Configuration mode field descriptions from the previous release are included in this document.

Related Links

Manager Modes on page 25

Chapter 3: Getting Started

Related Links

PC requirements on page 32
Installing Manager on page 33
Starting Manager on page 34
Opening a Configuration on page 35
Changing the Manager Language on page 37

PC requirements

Supported Operating Systems

- Windows 7 (32/64 bit)
- Windows 8.1 (32/64 bit)
- Server 2008 R2 (32/64 bit)
- Server 2112 R2 (64 bit)

Minimum PC Requirements

IP Office System	System RAM (minimum or higher)	Available memory required for Manager operations	Minimum free hard disk space	Processor (similar or higher)	Network size supported
Standard Mode	4 GB	2 GB	6 GB	Intel® Core™ i3 or equivalent, 2 GHz minimum	Not applicable.
Server Edition	4 GB (32 bit OS)	2 GB	6 GB	Intel® Core™ i3 or equivalent, 2 GHz minimum	Up to 32 nodes
Server Edition	8 GB (64 bit OS)	4 GB	6 GB	Intel® Core™ i5 or equivalent, 2 GHz minimum	Up to 150 nodes

Applications

If not already present, the .NET Framework 4.0 application is installed with Manager.

Ports

For information on port usage see the IP Office Avaya Port Matrix document on the Avaya support site at https://support.avaya.com/helpcenter/getGenericDetails?detailId=C201082074362003

Related Links

Getting Started on page 32

Installing Manager

Manager is a component of the IP Office Admin suite of applications. This suite is supplied on the Software DVD (Disk 1). Alternatively, the IP Office Admin Suite can be downloaded from Avaya's support website http://support.avaya.com.

In addition to Manager, the Admin suite includes options to install the following applications:

- **System Monitor** This is a tool for system installers and maintainers. Interpreting the information output by System Monitor requires detailed data and telecoms knowledge.
- **System Status Application** This is a Java application that can be used to monitor the status of the system such as extension, trunks and other resources. It displays current alarms and most recent historical alarms.

Note:

This installation process will install Windows .NET2 if not already present. The installation of .NET2 may require some systems to restart and the installation process to then be restarted.

Procedure

1. If installing from the Admin DVD, insert the DVD and when the page is displayed click on the link for the Admin suite.

   This will open a file windows showing the installation files for the suite. Locate and double-click on the `setup.exe` file.

2. Select the language you want to use for the installation process.

   This does not affect the language used by Manager when it is run. Click **Next >**.

3. If an upgrade menu appears, it indicates that a previous installation has been detected.

   Select **Yes** to upgrade the existing installed applications.

4. If required select the destination to which the applications should be installed.

   We recommend that you accept the default destination. Click **Next >**.

5. The next screen is used to select which applications in the suite should be installed.

   Clicking on each will display a description of the application. Click on the ▼ next to each application to change the installation selection. When you have selected the installations required, click **Next >**.

6. The applications selected are now ready to be installed.

   Click **Next >**.

7. Following installation, you will be prompted whether you want to run Manager.

   Selecting **Yes** runs Manager.

8. On some versions of Windows, you may be required to restart the PC.

   Allow this to happen if required.

Related Links

Getting Started on page 32

Starting Manager

No name or password is required to start Manager. A name and password is only required when connecting with a system.

When started, by default Manager will attempt to discover any systems on the network. If it finds any it will display a list from which you can select the system required.

1. Select **Start** and then **Programs** or **All Programs** depending on the version of Windows. Select the **IP Office** program group.
2. Select  **Manager**. If a Windows Security Alert appears select **Unblock** to allow Manager to run.
3. By default Manager will scan the network for any systems. What appears next depends on whether it finds any systems.

- If Manager finds multiple systems, the Select IP Office window displays a list of those systems from which you can select the one whose configuration you want to edit. If you want to open a configuration go to Opening a Configuration. If you don't want to load a configuration click on **Cancel**.
- If it finds a single system, it will attempt to open the configuration of that system by displaying the Configuration Service User Login window..
- If no systems are found or you cancel the steps above, the Manager simplified view is displayed.

Use the simplified view to select one of the following action.

- Create an Offline Configuration
- Open a Configuration from a System
- Read a Configuration from a File

Related Links

Getting Started on page 32

Opening a Configuration

The initial IP address ranges in which Manager searches for systems is set through the **File | Preferences | Discovery**. By default, Manager scans the local network of the Manager PC.

1. Start Manager. If Manager is already started and a configuration is open in it, that configuration must be closed first.

   If Manager is set to Auto Connect on start up, it will scan for systems automatically and either display the list of systems discovered or automatically start login to the only system discovered.

   Otherwise, select **File | Open Configuration**.

2. The Select IP Office window opens, listing those systems that responded.

   - If Server Edition systems are detected, they are grouped together. By default the configuration of those systems cannot be opened using Manager in **Advanced View** mode and the configuration of a Primary Server can only be opened if the **Open with Server Edition Manager** option is also selected.
   - If Manager has been set with **SCN Discovery** enabled, systems in a Small Community Network are grouped together. The checkbox next to the network name can be used to load the configurations of all the configurations into Small Community Network management mode.
   - If the system required was not found, the **Unit/Broadcast Address** used for the search can be changed. Either enter an address or use the drop-down to select a previously used address. Then click **Refresh**to perform a new search.
   - A list of known systems can be stored using **Known System Discovery**.
   - Manager can be configured to search using DNS names.
   - Systems found but not supported by the version of Manager being used will be listed as **Not Supported**.
   - If the system detected is running software other than from its primary folder, a  warning icon will be shown next to it. The configuration can still be opened but only as a read-only file.

3. When you have located the system required, check the box next to the system and click **OK**.

   If the system selected is a Server Edition system and Manager is not running in Server Edition mode, an **Open with Server Edition Manager** checkbox is shown and pre-selected. Clicking **OK** will switch Manager to its Server Edition mode before loading the configuration.

4. The system name and password request is displayed. Enter the required details and click **OK**.

   The name and password used must match a service user account configured within the system's security settings.

5. Additional messages will inform you about the success or failure of opening the configuration from the system.

The method of connection, secure or insecure, attempted by Manager is set the applications Secure Communications preferences setting.

- When **Secure Communications** is set to **On**, a  padlock icon is displayed at all times in the lower right Manager status field.
- New installations of Manager default to having **Secure Communications** enabled. This means Manager by default attempts to use secure communications when opening a configuration.
- For Server Edition systems, Manager will always attempt to use secure communications regardless of the **Secure Communications** setting.
- If no response to the use of secure communication is received after 5 seconds, Manager will offer to fallback to using unsecured communications.

6. Following a successful log in, the configuration is opened in Manager. The menus and options displayed will depend on the type of system configuration loaded.

Related Links

Getting Started on page 32
Login messages on page 36

Login messages

While attempting to login to a system, various messages may be displayed.

Configuration Not Loaded Messages

Access Denied

Displayed as the cause if the service user name/password were incorrect, or the service user has insufficient rights to read the configuration. The Retry option can be used to log in again but multiple rejections in a 10 minute period may trigger events, such as locking the user account, set by the Password Reject Limit and Password Reject Action options in the systems security settings.

Failed to communicate with system

Displayed as the cause if the network link fails, or the secure communication mode is incorrect (for example Manager is set to unsecured, but the system is set to secure only).

Account Locked

The account of the service user name and password being used is locked. This can be caused by a number of actions, for example too many incorrect password attempts, passing a fixed expiry date, etc. The account lock may be temporary (10 minutes) or permanent until manually unlocked. An account can be enabled again through the system's security settings.

Additional Messages

Your service user account will expire in X days

Indicates that an Account Expiry date has been set on the system service user account and that date is approaching. Someone with access to the system's security settings will be required unlock the account and set a new expiry date.

Your password will expire in X days. Do you wish to change it now?

Indicates that password ageing has been configured in the system's security settings. If your password expires, someone with access to the system's security settings will be required to unlock the account.

Change password

Through the system's security settings, a service user account can be required to change their password when logging in. The menu provides fields for entering the old password and new password.

Contact Information Check - This configuration is under special control

This message displays if a Manager user with administrator rights has entered their contact information into the configuration. For example to indicate that they do not want the configuration altered while a possible problem is being diagnosed. The options available are:

- **Cancel** Select this option to close the configuration without making any changes.
- **Set configuration alteration flag** Select this option if the configuration is being opened because some urgent maintenance action. When the configuration is next opened, the fact that it has been altered will be indicated on the System | System tab.
- **Delete Contact Information** Select this option to take the system out of special control.
- **Leave contact information and flags unchanged (Administrators only)** This option is only available to service users logging in with administrator rights.

Related Links

Opening a Configuration on page 35

Changing the Manager Language

About this task

The Manager application can run in multiple languages. By default it tries to use the best match to the PC's regional location settings, otherwise it will use UK English.

The process below can be used to run Manager in one of its supported languages. However it does not change the language used for help file content.

Procedure

1. Create a Windows shortcut to the Manager application .exe file. By default this file is located in **C:\Program Files\Avaya\IP Office\Manager\Manager.exe**.
2. Right-click on the shortcut and select **Properties**.
3. The **Target** field can be used to specify the locale setting that Manager should use.

   For example, for Italian the Target should have **-locale:it-IT** added to the end. For example: **"C:\Program Files\Avaya\IP Office\Manager\Manager.exe" -locale:it-IT**.
4. Click **OK**.

5. Manager should now run in the selected language when launched using the updated shortcut.

Example

Table 2: Manager Locales

Manager Language	Shortcut Locale Setting
Brazilian Portuguese	locale:pt-Br
Chinese (Simplified)	-locale:zh-Hans
French	-locale:fr-FR
German	-locale:de-DE
Italian	-locale:it-IT
Mexican Spanish	-locale:es-MX
Russian	-locale:ru-RU
US English	-locale:en-US

Related Links

Getting Started on page 32

Chapter 4: Menu Bar Commands

The commands available through the Manager's menu bar change according to the mode in which Manager is running. Commands may also be grayed out if not currently applicable. For some commands, an arrow symbol indicates that there are sub-commands from which a selection can be made.

The following sections outline the functions of each command. The **Edit** and **Help** menus are not included.

Related Links

File Menu on page 39
View Menu on page 69
Tools Menu on page 70
Security Mode Menus on page 75
Embedded File Management Menus on page 76

File Menu

Related Links

Menu Bar Commands on page 39
File | Open Configuration on page 40
File | Close Configuration on page 40
File | Save Configuration on page 40
File | Save Configuration As on page 40
File | Change Working Directory on page 41
File | Preferences on page 42
File | Offline on page 50
File | Advanced on page 51
File | Backup/Restore on page 68
File | Import/Export on page 68
File | Exit on page 69

File | Open Configuration

This command displays the Select IP Office window used to receive a systems configuration settings.

The same action is performed by the  icon in the Main Toolbar.

The **Select IP Office** menu is also used for other actions such as reboot and sending a configuration. If the unit required is not found, the Unit/Broadcast Address can be changed and then Refresh clicked. To change the TCP addresses scanned, select **File | Preferences | Discovery** and enter the required addresses in the IP Search Criteria.

Known Units is not available unless configured

Related Links

File Menu on page 39

File | Close Configuration

This command closes the currently loaded configuration without saving it.

Related Links

File Menu on page 39

File | Save Configuration

The **File | Save** command saves the amended configuration.

If the configuration has been received from a system, the Send Config menu is displayed.

If the configuration file has been opened offline or created from new, the file is saved to disk only.

Related Links

File Menu on page 39

File | Save Configuration As

The **File | Save Configuration As** command allows you to save a configuration a file on the Manager computer. Note that dynamic configuration data, for example hunt groups advertised from other systems in a network, are not included in a configuration file saved onto PC and then reopened.

The command displays the Save As window. Select the drive and directory. and then enter the new file name. Once you have entered the file name, the Save Configuration File window opens, where

you have the option to encrypt the file by entering a password. Leave the password blank if you do not want to encrypt the file.

Important:

Encrypted configuration files can only be opened with Manager 9.1 or later. In earlier versions of Manager, the file will open but it is empty.

Configurations saved onto the PC in this way can be reopened using the icon or the **File | Offline | Open File** command. If the file has been encrypted, you must enter the password.

When Manager is running in Server Edition mode, the Save command operates differently. Multiple files are saved, one `.cfg` file for each server in the network plus a single `.cfi` file for the whole network.

The .cfi file can be used with the **File | Offline | Open File SetFile | Offline | Open File Set** command to open the whole set of files in a single action.

Related Links

File Menu on page 39

File | Change Working Directory

These settings allow you to change the default locations where Manager looks for and saves files.

These fields set the default location where Manager will look for and save files.

Directory	Description
Working Directory (.cfg files)	Sets the directory into which Manager saves `.cfg` files. By default this is the Manager application's program directory. **Note:** On Windows 7 systems, the default folder for Manager .cfg files is C:\Program Files (x86)\Avaya\IP Office\Manager. On some Windows 7 systems, the file is saved to the user's profile folder at C:\Users\<user_name>\AppData\Local\VirtualStore\Program Files (x86)\Avaya\IP Office\Manager. You must turn on Show hidden files to access this folder. Alternatively, you can set the working directory to an alternate location.
Binary Directory (.bin files)	Sets the directory in which the Manager upgrade wizard, HTTP, TFTP and BOOTP functions look for firmware files requested by phones and other hardware components. That includes `.bin` file, `.scr` files and `.txt` files. By default this is the Manager application's program directory. **Tip:** In the Upgrade Wizard, right-clicking and selecting **Change Directory** also changes this setting.

Table continues…

Directory	Description
	Warning: Historically, by default the **Working Directory** and **Binary Directory** are the same. This is deprecated as it potentially allows remote TFTP/HTTP file access to the folder containing copies of configuration files. Therefore it is recommended that either of the folders is changed to an alternate location.
Known Units File	Sets the file and directory into which Manager can record details of the systems it has discovered. Once a file location has been specified, a Known Units button becomes available on the discovery menu used for loading system configuration. Pressing that button displays the known units file as a list from which the required system can be selected. It also allows sorting of the list and records to be removed.

Related Links

File Menu on page 39

File | Preferences

This command displays a window for configuring various aspects of Manager's operation. The window is divided into a number of tabs.

Related Links

File Menu on page 39
File | Preferences | Preferences on page 42
File | Preferences | Directories on page 44
File | Preferences | Discovery on page 45
File | Preferences | Visual Preferences on page 46
File | Preferences | Security on page 46
File | Preferences | Validation on page 49

File | Preferences | Preferences

This tab is accessed through **File | Preferences** and then selecting the **Preferences** tab.

Setting	Description
Edit Services Base TCP Port:	Default = On. This field shows or hides the base communication port settings.
Service Base TCP Port	Default = 50804. Access to the configuration and security settings on a system requires Manager to send its requests to specific ports. This setting allows the TCP Base Port used by Manager to be set to match the TCP Base Port setting of the system. The system's TCP Base Port is set through its security settings.
Service Base HTTP Port	Default = 80.

Table continues…

Setting	Description
	Access to the HTTP server on a system requires Manager to send its requests to specific ports. This setting allows the HTTP Base Port used by Manager to be set to match the HTTP Base Port setting of the system. The system's HTTP Base Port is set through its security settings.
Enable Time Server	Default = On. This setting allows Manager to respond to RFC868 Time requests from systems. It will provide the system with both the UTC time value and the local time value of the PC on which it is running.
Enable BootP and TFTP Servers	Default = Off. This setting allows Manager to respond to BOOTP request from systems for which it also has a matching BOOTP record. It also allows Manager to respond to TFTP requests for files.
Enable Port for Serial Communication	Not used. This is a legacy feature for some older control units that were managed via the serial port rather than the LAN.
Enter Port Number to be used for Serial Communication	Used with the setting above to indicate which serial port Manager should use.
Auto Connect on start up	Default = On If on, when Manager is started it will automatically launch the **Select IP Office** menu and display any discovered systems. If only one system is discovered, Manager will automatically display the login request for that system or load its configuration if the security settings are default.
Set Simplified View as default	Default = On If on, the Manager will start in simplified view mode if no configuration is loaded.
Default to Standard Mode	Default = Off If on, when a configuration from a new or defaulted system running in Basic mode is loaded, Manager will automatically convert the configuration to Standard mode. Sending the configuration back to the system will restart it in Standard mode. Only select this option if the only systems you expect to install are Standard systems. This setting does not affect existing systems with non-default configurations.
Use Remote Access for Multi-Site	Default = Off. If selected, access to all the configurations of a multi-site network is allowed via remote access to the primary server on the multi-site network. When selected, an additional **Use Remote Access** check box option is displayed on the Select IP Office menu when the **Open with Server Edition Manager** checkbox option is selected or if Manager is already running in Server Edition mode.
Consolidate Solution to Primary Settings	This setting is used by Manager when in Server Edition mode. 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.

Table continues…

Setting	Description
	• 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

File | Preferences on page 42

File | Preferences | Directories

These settings allow you to change the default locations where Manager looks for and saves files.

These fields set the default location where Manager will look for and save files.

Directory	Description
Working Directory (.cfg files)	Sets the directory into which Manager saves `.cfg` files. By default this is the Manager application's program directory. **Note:** On Windows 7 systems, the default folder for Manager .cfg files is C:\Program Files (x86)\Avaya\IP Office\Manager. On some Windows 7 systems, the file is saved to the user's profile folder at C:\Users\<user_name>\AppData\Local\VirtualStore\Program Files (x86)\Avaya\IP Office\Manager. You must turn on Show hidden files to access this folder. Alternatively, you can set the working directory to an alternate location.
Binary Directory (.bin files)	Sets the directory in which the Manager upgrade wizard, HTTP, TFTP and BOOTP functions look for firmware files requested by phones and other hardware components. That includes `.bin` file, `.scr` files and `.txt` files. By default this is the Manager application's program directory.

Table continues…

Directory	Description
	Tip: In the Upgrade Wizard, right-clicking and selecting **Change Directory** also changes this setting. **Warning:** Historically, by default the **Working Directory** and **Binary Directory** are the same. This is deprecated as it potentially allows remote TFTP/HTTP file access to the folder containing copies of configuration files. Therefore it is recommended that either of the folders is changed to an alternate location.
Known Units File	Sets the file and directory into which Manager can record details of the systems it has discovered. Once a file location has been specified, a Known Units button becomes available on the discovery menu used for loading system configuration. Pressing that button displays the known units file as a list from which the required system can be selected. It also allows sorting of the list and records to be removed.

Related Links

File | Preferences on page 42

File | Preferences | Discovery

These settings affect the **Select IP Office** menu used by Manager to discovery systems.

Setting	Description
TCP Discovery	Default = On. This setting controls whether Manager uses TCP to discover systems. The addresses used for TCP discovery are set through the IP Search Criteria field below.
NIC IP/NIC Subnet	This area is for information only. It shows the IP address settings of the LAN network interface cards (NIC) in the PC running Manager. Double-click on a particular NIC to add the address range it is part of to the IP Search Criteria. Note that if the address of any of the Manager PC's NIC cards is changed, the Manager application should be closed and restarted.
IP Search Criteria	This section is used to enter TCP addresses to be used for the TCP discovery process. Individual addresses can be entered separated by semi-colons, for example 135.164.180.170; 135.164.180.175. Address ranges can be specified using dashes, for example 135.64.180.170 - 135.64.180.175.
UDP Discovery	Default = On This settings controls whether Manager uses UDP to discover systems.
Enter Broadcast IP Address	Default = 255.255.255.255 The broadcast IP address range that Manager should used during UDP discovery. Since UDP broadcast is not routable, it will not locate systems that are on different subnets from the Manager PC unless a specific address is entered.

Table continues…

Setting	Description
Use DNS	Selecting this option allows Manager to use DNS name (or IP address) lookup to locate a system. Note that this overrides the use of the TCP Discovery and UDP Discovery options above. This option requires the system IP address to be assigned as a name on the users DNS server. When selected, the **Unit/Discovery Address** field on the Select IP Office window is replaced by a **Enter Unit DNS Name or IP Address** field.
SCN Discovery	If enabled, when discovering systems, the list of discovered systems will group systems in the same Small Community Network and allow them to be loaded as a single configuration. At least one of the systems in the Small Community Network must be running Release 6.0 or higher software. See Small Community Network Management. This does not override the need for each system in the Small Community Network to also be reachable by the **TCP Discovery** and or **UDP Discovery** settings above and accessible by the router settings at the Manager location.

Related Links

File | Preferences on page 42

File | Preferences | Visual Preferences

Setting	Description
Icon size	Sets the size for the icons in the navigation pane between **Small**, **Medium** or **Large**.
Multiline Tabs	Default = Off. In the details pane, for record types with more than two tabs, Manager can either use  buttons to scroll the tabs horizontally or arrange the tabs into multiple rows. This setting allows selection of which method Manager uses.
Enable Template Options	Default = On. When enabled, the Manager can be used to apply trunk templates. SIP trunk templates can be used to add SIP trunks. Analog trunk templates can also be applied to existing analog trunks. This option does not affect the additional template options used for Server Edition mode.
Enable Template Creation	Default = Off. When enabled, you can use templates to provision the system.

Related Links

File | Preferences on page 42

File | Preferences | Security

Controls the various security settings of Manager. To control the security settings of the system, see the information on Security mode.

All settings, except **Secure Communications**, can only be changed when a configuration has been opened using a user name and password with Administrator rights or security administration rights.

Setting	Description
Request Login on Save	Default = On By default a valid user name and password is required to receive a configuration from a system and also to send that same configuration back to the system. Deselecting this setting allows Manager to send the configuration back without having to renter user name and password details. This does not apply to a configuration that has been saved on PC and then reopened. This setting can only be changed when a configuration has been opened using a user name and password with Administrator rights or security administration rights.
Close Configuration/ Security Settings After Send	Default = On. When selected, the open configuration file or security settings are closed after being sent back to the system. This is the normal default. This setting does not affect multi-site network modes of Manager which always close the configuration after saving. Before disabling this setting, you should recall that the configuration held by a running system can be changed by actions other than Manager, for example changes made by users through their phone. Keeping a configuration open in Manager for longer than necessary increases the chances that that copy of the configuration differs from the current configuration of the running system and will overwrite those changes when sent back to the system.
Save Configuration File After Load	Default = Off. When selected, a copy of the configuration is saved to Manager's working directory. The file is named using the system name and the suffix **.cfg**. This setting can only be changed when a configuration has been opened using a user name and password with Administrator rights or security administration rights.
Backup Files on Send	Default = Off. If selected, whenever a copy of a configuration is sent to a system, a backup copy is saved in Manager's working directory. The file is saved using the system name, date and a version number followed by the **Backup File Extension** as set below. This setting can only be changed when a configuration has been opened using a user name and password with Administrator rights or security administration rights.
Backup File Extension	Default = .BAK Sets the file extension to use for backup copies of system configurations generated by the Backup Files on Send option above.
Number of Backup Files to keep	Default = Unlimited. This option allows the number of backup files kept for each system to be limited. If set to a value other then **Unlimited**, when that limit would be exceeded, the file with the oldest backup file is deleted.
Enable Application Idle Timer (5 minutes)	Default = On. When enabled, no keyboard or mouse activity for 5 minutes will cause the Manager to grey out the application and re-request the current service user password. This setting can only be changed when a configuration has been

Table continues…

Setting	Description
	opened using a user name and password with Administrator rights or security administration rights.
Secure Communications	Default = On When selected, any service communication from Manager to the system uses the TLS protocol. This will use the ports set for secure configuration and secure security access. It also requires the configuration and or security service within the system's security configuration settings to have been set to support secure access. Depending on the level of that secure access selected, it may be necessary for the **Manager Certificate Checks** below to be configured to match those expected by the system for configuration and or security service. See Security Administration. • When **Secure Communications** is set to **On**, a padlock icon is displayed at all times in the lower right Manager status field. • For Server Edition systems, Manager will always attempt to use secure communications regardless of the **Secure Communications** setting. • If no response to the use of secure communication is received after 5 seconds, Manager will offer to fallback to using unsecured communications.
Manager Certificate Checks	When the Secure Communications option above is used, Manager will process and check the certificate received from the system. This setting can only be changed when a configuration has been opened using a user name and password with Administrator rights or security administration rights. The options are: • **Low**: Any certificate sent by the system is accepted. • **Medium**: Any certificate sent by the system is accepted if it has previously been previously saved in the Windows' certificate store. If the certificate has not been previously saved, the user has the option to review and either accept or reject the certificate. • **High**: Any certificate sent by the system is accepted if it has previously been previously saved in the Windows' certificate store. Any other certificate cause a log in failure.
Certificate Offered to IP Office	Default = none Specifies the certificate used to identify Manager when the Secure Communications option is used and the system requests a certificate. Use the **Set** button to change the selected certificate. Any certificate selected must have an associated private key held within the store: • Select from Current User certificate store - Display certificates currently in the currently logged-in user store. • Select from Local Machine certificate store. • Remove Selection – do not offer a Manager certificate.

:

Security – Registry Settings

Warning:

Avaya accept no liability for any issues arising from the editing of a PC's registry settings. If you are in any doubt about how to perform this process you should not proceed. It is your responsibility to ensure that the registry is correctly backed up before any changes are made.

Note:

Before manually editing any registry entry, the following Microsoft support articles should be read:

- http://support.microsoft.com/kb/256986
- http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/regedit_permit_key.mspx

Manager stores it's security preferences in the Windows Registry. The following key affects manager security operation; it's values may only be changed by a configuration or security administrator:

`HKEY_CURRENT_USER\Software\Avaya\IP400\Manager\Security\`

In order to prevent circumvention by manual editing of the Windows Registry, Regedt32.exe, the native registry editor, allows an operator user (with Full Control permissions) to edit permissions on a per key basis.

To prevent a user from manually editing the security preferences, the `HKEY_USERS\User GUID \Software\Avaya\IP400\Manager\Security` key permission should be set to 'Read' only for that user. Ensure that all child object permissions are replaced as well by using the 'Advanced' button.

To allows the security policy of all local PC users to be fixed, a set of values in the key `HKEY_CURRENT_USER\Software\Avaya\IP400\Manager\Security\` may be created. This is tested and used in preference to any value found under `HKEY_CURRENT_USER\Software\Avaya \IP400\Manager\Security\`.

This key is not created by the manager application.

Related Links

File | Preferences on page 42

File | Preferences | Validation

By default Manager validates the whole configuration when it is loaded and individual fields whenever they are edited. This tab allows selection of when automatic validation should be applied to configuration files loaded into Manager.

Setting	Description
Validate configuration on open	Automatically validate configuration files when they are opened in Manager.

Table continues…

Setting	Description
Validate configuration on edit	Validate the whole configuration when **OK** is clicked after editing a record. For large configurations, disabling this option removes the delay caused by validating the configuration after every edit.
Prompt for configuration validation on save or send	If selected, when saving or sending a configuration, a prompt is displayed asking whether the configuration should be validated. If validation is selected and error are found, the send or save process is canceled. This option is disabled if Validate configuration on edit is selected.

Related Links

File | Preferences on page 42

File | Offline

Related Links

File Menu on page 39
File | Offline | Create New Config on page 50
File | Offline | Open File on page 50
Open File Set on page 50
File | Offline | Send Config on page 51
File | Offline | Receive Config on page 51

File | Offline | Create New Config

Used to create an offline configuration.

This command starts a dialog that allows you to create a default offline configuration by specifying the system locales, the type of control unit and expansion modules and the trunk cards fitted. The same action is performed by the  icon in the Main Toolbar.

Related Links

File | Offline on page 50

File | Offline | Open File

This command allows a configuration file stored on PC to be opened in Manager.

Related Links

File | Offline on page 50

Open File Set

This command is only available when manager is running in Server Edition mode. It can be used to load a set of files previously saved offline using the **File | Save Configuration As** command.

When selected, browse to the location of the saved `.cfi` file and associated `.cfg` files and select the `.cfi` file.

Related Links

File | Offline on page 50

File | Offline | Send Config

This command is used to send an offline configuration to a system.

Warning:

After this command is completed, the system is rebooted. This will end all calls and services in progress.

After sending the configuration, you should receive the configuration back from the system and note any new validation errors shown by Manager. For example, if using Embedded Voicemail, some sets of prompt languages may need to be updated to match the new configurations locale setting using the Add/Display VM Locales option.

Related Links

File | Offline on page 50

File | Offline | Receive Config

This command displays the **Select IP Office** menu used to receive a systems configuration settings.

Once the configuration has been received, you are prompted to save it on the PC.

Related Links

File | Offline on page 50

File | Advanced

Related Links

File Menu on page 39
File | Advanced | Erase Configuration on page 52
File | Advanced | Reboot on page 52
File | Advanced | System Shutdown on page 53
File | Advanced | Upgrade on page 54
File | Advanced | Change Mode on page 56
File | Advanced | Switch to Standard Mode on page 57
File | Advanced | Audit Trail on page 58
File | Advanced | Security Settings on page 59
File | Advanced | Erase Security Settings (Default) on page 59
File | Advanced | Embedded File Management on page 59
File | Advanced | Format IP Office SD Card on page 60
File | Advanced | Recreate IP Office SD Card on page 61
File | Advanced | Memory Card Command on page 63
File | Advanced | Launch Voicemail Pro on page 63

File | Advanced | System Status on page 63
File | Advanced | LVM Greeting Utility on page 64
File | Advanced | Initial Configuration on page 64
File | Advanced | Add/Display VM Locales on page 68

File | Advanced | Erase Configuration

This 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.

When this command is used, the **Select IP Office** menu is displayed. Once a system is selected, a valid configuration user name and password are required to complete the action.

IP500 V2 systems using **IP Office A-Law** or **IP Office U-Law** System SD cards will default to Quick mode. Loading the configuration will switch Manager to simplified view. To change the system back to operating in Standard mode, use either of the following methods:

- **Change Mode**

  This will change the operating mode of the system and create a default configuration appropriate to that mode. For example, this method can be used to change a Standard mode system to a Basic Edition system.

- **Switch to Standard Mode**

  This option (only shown in Manager simplified view) will change the operating mode of a Basic Edtion system to Standard mode.

  For systems running in Server Edition mode, this command can normally only be used when Manager is also running in Server Edition mode.

Related Links

File | Advanced on page 51

File | Advanced | Reboot

When this command is used, the **Select IP Office** window is displayed. Once a system is selected, a valid user name and password are required. The type of reboot can then be selected in the Reboot window.

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. This mode can be combined with the **Call Barring** options.
- **Timed** The same as When Free but waits for a specific time after which it then wait for there to be no calls in progress. The time is specified by the **Reboot Time**. This mode can be combined with the **Call Barring** options.

  Reboot Time This setting is used when the reboot mode **Timed** is selected. It sets the time for the reboot. If the time is after midnight, the system's normal daily backup is canceled.

Call Barring These settings can be used when the reboot mode **When Free** is selected. They bar the sending or receiving of any new calls.

Related Links

File | Advanced on page 51

File | Advanced | System Shutdown

This command can be used to shutdown systems. The shut down can be either indefinite or for a set period of time after which the system will reboot. For Linux based telephone systems, the shutdown command is applied to the telephony service on the server and not to the whole sever. In that case, if the system is shutdown indefinitely, it can be restarted using the server's web control pages to either restart the service or to restart the whole server.

Warning:

A shutdown must always be used to switch off the system. Simply removing the power cord or switching off the power input may cause the loss of configuration data.

This is not a polite shutdown, any user calls and services in operation will be stopped. Once shutdown, the system cannot be used to make or receive any calls until restarted.

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

When shutdown, the LEDs shown on the system are as follows. Do not remove power from the system or remove any of the memory cards until the system is in this state:

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

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

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

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

Related Links

File | Advanced on page 51

File | Advanced | Upgrade

Note:

This command is not used with Linux based systems. Linux systems are updated through the server's webcontrol menus.

This command starts the **Upgrade Wizard** tool. The **Upgrade Wizard** is used to compare the software level of the control unit and modules within systems against the software level of the .bin binary files Manager has available. The Upgrade Wizard can then be used to select which units to upgrade.

Warning:

- Incorrect use of the upgrade command can halt system operation and render units in the system unusable. You must refer to the Technical Bulletins for a specific release for full details of performing software upgrades to that release. There may be additional steps required such as defaulting the security settings.
- Performing any other actions on a system during an upgrade or closing the upgrade wizard and Manager during an upgrade may render systems unusable.
- During an upgrade the system may restrict calls and services. It will reboot and disconnect all current calls and services.
- The **Validate** option must remain selected wherever possible. Use of unvalidated upgrades is subject to a number of conditions outlined in the IP Office Installation Manual and Technical Bulletins.

The list area shows details of systems found by the Upgrade Wizard and the software currently held by those systems. The check boxes are used to select which units should be upgraded. Upgrading will require entry of a valid name and password for the selected system.

Column	Description
Name	The name of the system as set in its configuration (**System | System | Name**) .
IP Address	The IP address of the system.
Type	The type of system and the names of the various firmware files used by external expansion systems supported by the system type.
Version	Details the current software each unit in the systems is running.
Edition	Indicates the operation mode of the system.
Licensed	Indicates the highest value software upgrade license present in the system's configuration. The IP Office Release that is supported by that license is also indicated in brackets.
Required License	Indicates the software upgrade license required for the current level of software the system is running. The IP Office Release that is supported by that license is also indicated in brackets.

Table continues…

Column	Description
	It does not refer to the software upgrade license required for the level of software which is available for upgrade. The system must include a license for the specific level of software it is required to run. For IP500 V2 systems, a value of 255 indicates that the control unit is still in its initial 90 days where it can be upgraded to a higher level without requiring an upgrade license.
Available	Shows the version of the matching firmware files that Manager has available (a – indicates no file available) in its current working directory. Upgrading to a release higher than that supported by the current Licensed level will leave the system unable to support any functions until the appropriate upgrade license is added to the system configuration.

The Upgrade Wizard includes a number of check boxes that can be used to include other actions as part of the upgrade process:

- **Validate**
- The Validate option should remain selected wherever possible. When selected, the upgrade process is divided as follows: transfer new software, confirm transfer, delete old software, restart with new software. If **Validate** is not selected, the old software is deleted before the new software is transferred.
- **Backup System Files**
- For any IP500 V2 systems being upgraded, the **Backup system files** option will cause the system to backup its memory card files as part of the upgrade.
- **Upload System File**
- For any IP500 V2 system being upgraded, the **Upload system files** option will upload various files:
  - It copies the binary files for the system control unit and possible external expansion modules.
  - It copies the firmware files used by phones supported by the system.
  - For systems running Basic Edition, the files for Basic Edition Web Manager are copied.
  - For systems configured to run Embedded Voicemail, the Embedded Voicemail prompts for those supported languages set as the system locale, user locales, incoming call route locales and short code locales are upgraded. In addition the English language prompts are upgraded as follows: **IP Office A-Law/Norstar SD Cards** - UK English, **IP Office U Law/ PARTNER SD Cards** - US English.
- **Restart IP Phones** For Manager 8.1 and higher the Restart IP Phones option can be used. This will cause those phone to load any upgrade phone firmware included in the system upgrade (if using the system's memory card as their firmware file source).

Related Links

File | Advanced on page 51

Searching for Systems

The default address used by the Upgrade Wizard is the address shown in the Manager title bar, which is selected through File | Preferences. If the unit required is not found, the address used can be changed.

Procedure

1. Enter or select the required address in the **Unit/Broadcast Address** field.
2. Click **Refresh**to perform a new search.

Changing the .bin File Directory

The directory in which the Upgrade Wizard looks for .bin files is set through Manager's Binary Directory setting. This can be changed using **Files | Change Working Directory** or **File | Preferences | Directories**.

Use this procedure to change it directly from the Upgrade Wizard.

Procedure

1. Right-click on the list area.
2. Select **Select Directory**.
3. Browse to and highlight the folder containing the .bin files. Click **OK**.
4. The list in the **Available** column will be updated to show the .bin files in the selected directory that match units or modules listed.

File | Advanced | Change Mode

This command can be used to change the operating mode of an IP500 V2 System SD card and thus of the system. For example, it can be used to switch a system currently running Standard Mode to Basic Mode.

Important:

Using this command will default the configuration. Therefore ensure that you have a backup copy of the configuration before using this command in case it is necessary to return to the previous mode.

Do not use this command if the system includes components not supported by the mode to which you want to switch. If that is the case, the system may not restart correctly. For example, BRI cards are not supported by Basic Edition Partner mode.

In order to use this command, the system security settings must be at their default settings. The current setting can be defaulted using the Erase Security Settings (Default) command.

Follow the command, the system is restarted.

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

For the mode change, you should perform a system upgrade or upload system files action as the files included in any previous upgrade or upload will have been based on the system's previous mode setting and configuration settings.

After a mode change, the system restarts. If the system does not restart, the most likely cause is that the systems security settings were not at their default settings.

The window that opens after selecting a system will indicate the modes available.

Standard mode

Mode selection is only possible for systems fitted with **IP Office A-Law** or **IP Office U-Law** SD cards. For systems fitted with **IP Office Partner Edition** or **IP Office Norstar Edition** SD cards, the systems will default to the respective mode of that card regardless of the mode selection.

Note that this process does not change the formatted type of the System SD card. For example, if a system fitted with an **IP Office A-Law** card has its mode changed to Standard mode, if that system is then defaulted again it will restart as a Basic Edition system as appropriate to the card type.

Basic Edition

There is no mode selection. The system will be changed to a defaulted Standard mode configuration

Related Links

File | Advanced on page 51

File | Advanced | Switch to Standard Mode

This option will change the operating mode of the configuration loaded in Manager to that of a Standard Mode system. Manager will automatically switch to its advanced view mode. When the configuration is sent back to the system, it will restart in Standard Mode.

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

The command provides two options:

- **Default** Using this method will default the configuration. It is the recommended method for installation of a new installation or for when a Standard Mode system has been defaulted and needs to be returned to Essential Edition operation.
- **Best Match** Using this method will attempt to preserve configuration settings; for examples user names, extension numbers, licenses, SIP trunks, etc. However, many settings will be flagged as errors by Manager. These errors should then be resolved before sending the configuration to the system.

If this is an existing system, it is recommended that you first use Manager to receives and save a copy of the current configuration locally using **Save Configuration As**. This process does not default the security settings of the system.

Do not use this command if the system includes components not supported by the Essential Edition. (currently IP500 ETR6 base cards for ETR phones). The system may not restart correctly if that is the case.

When this command is selected, Manager will first browse for available systems. When a system is selected from those found, load its configuration. If this cannot be done using the default password (**password**) it may not be possible to complete the process.

! Automatic Conversion to Standard Mode This process can be applied automatically when a configuration for a new or defaulted system running in Basic Edition — Quick mode is loaded. This is done by selecting the **Default to Standard Mod**e option in the Manager Preferences. Only select this option if the only systems you expect to install are Standard mode systems.

Related Links

File | Advanced on page 51

File | Advanced | Audit Trail

The audit trail lists the last 16 actions performed on the system from which the configuration loaded into Manager was received. It includes actions by service users such as getting the configuration, sending a configuration back, reboots, upgrades and default the system. .

Audit trail events can be output to a Syslog server through the system's **System | System Events** settings.

The last failed action is always recorded and shown in red. It is kept even if there have been 16 subsequent successful actions.

The Audit Trail is part of the system configuration file received from the system. If the configuration is kept open between send and reboot operations (ie. if Close Configuration/Security Setting After Send is not selected), the Audit Trail will not show details of those operations. It will only show details of those operations if the configuration is closed and then a new copy of the configuration is received from the system.

Audit Details

When a specific access event is selected from the list, the following information is shown in the Audit Details section:

- The **Security User** shows the service user name used for the access action.
- The **Data and Time of Access** indicate the local system time when the recorded event occurred.
- The **PC Login** is the computer name of the PC used for the access.
- The **PC IP Address** and **PC MAC Address** are the IP address and MAC address of the PC used for access.
- The **Access Type** details the type of action that was performed.
- The **Outcome** shows the system's response to the access. The outcome **Success (Warning)** refers to the sending of a configuration that contains fields marked as errors or warnings by Manager's validation function. **Success (Clean)** refers to the sending of a configuration that does not contain any validation errors or warnings.

Items Changed

The Items Changed area summarizes the changes contained in a sent configuration. Where changes to a single record of a particular type are made, the Item Name field lists the individual

record changed. Where changes are made to several records of the same type, the Item Name field displays Multiple items.

Related Links

File | Advanced on page 51

File | Advanced | Security Settings

This command is used to switch the Manager application to security mode. In that mode, Manager is used to edit the security settings of a system.

Related Links

File | Advanced on page 51

File | Advanced | Erase Security Settings (Default)

This 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. When this command is used, the **Select IP Office** menu is displayed. Once a system is selected, a valid security user name and password are required to complete the action.

The system's security settings are returned to their defaults as indicated in the Security Mode chapter.

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

For Standard mode and Server Edition systems, the name and password used for this command are those required for security configuration access which are different from those used for normal configuration access.

For Basic Edition systems, the name and password required are those of the **Administrator** account used for configuration access.

For 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

File | Advanced on page 51

File | Advanced | Embedded File Management

For control units with a memory card installed, the contents of the card can be viewed using Manager. This view can also be used to add and remove files from the card. This may be useful when the memory card is being used to store Music on Hold or IP phone firmware files.

For Linux based systems, the folder `/opt/ipoffice` is used as the file repository for embedded file management actions.

Related Links

File | Advanced on page 51

File | Advanced | Format IP Office SD Card

This command allows suitable SD cards to be formatted by the Manager PC. The system supports SD cards with the following format: SDHC minimum 4GB FAT32 format (Single partition, SDHC, class2+, FAT32, SPI & SD bus). Non-Avaya supplied cards of the same format can be used a system's **Optional SD** slot for additional actions such as backup.

Warning:

- Do not re-purpose a Enterprise Branch SD card for use with any other IP Office mode. Doing so may damage the SD card and make it unusable for your Enterprise Branch system.
- **All File Will Be Erased** Note that this action will erase any existing files and folders on the card. If the requirement is just to update the card, use Recreate IP Office SD Card without reformatting. Once a card has been formatted, the folders and files required for operation can be loaded onto the card from the Manager PC using the Recreate IP Office SD Card command.
- Avaya supplied SD cards should not be formatted using any other method than the format commands within Manager and System Status Application. Formatting the cards using any other method will remove the feature key used for system licensing from the card.

Related Links

File | Advanced on page 51
Formating the SD card on page 60

Formating the SD card

Procedure

1. Insert the SD card into a reader slot on the Manager computer.
2. Using Manager, select **File | Advanced | Format IP Office SD Card**.
3. Select the type of card.

   This selection just sets the card label shown when viewing the card details. It does not affect the actual formatting. Select the label that matches the file set you will be placing on the card.

   - **IP Office A-Law** A system fitted with this type of card will default to A-Law telephony. The system will default to IP Office Basic Edition - Quick Mode **PBX System** operation.
   - **IP Office U-Law** A system fitted with this type of card will default to A-Law telephony. The system will default to IP Office Basic Edition - Quick Mode **Key System** operation.
   - **IP Office Partner Edition** A system fitted with this type of card will default to A-Law telephony and IP Office Basic Edition - PARTNER® Mode operation.
   - **IP Office Norstar Edition** A system fitted with this type of card will default to U-Law telephony and IP Office Basic Edition - Norstar® Mode operation.

- **Enerprise Branch** Use this option for an SD card intended to be used with an IP Office system running in Enterprise Branch Mode. There is a separate SD card for Enterprise Branch. The Enterprise Branch SD card can only be used for Enterprise Branch operation and cannot be used to change modes to IP Office. You also cannot use or change an IP Office SD card for use with an Enterprise Branch system.

  Warning:

  Do not re-purpose a Enerprise Branch card for use with any other IP Office mode. Doing so may damage the SD card and make it unusable for your Enterprise Branch system.

4. Browse to the card location and click **OK**.
5. The status bar at the bottom of Manager will display the progress of the formatting process.
6. When the formatting is complete, you can use the Recreate IP Office SD Card command to load the system folders and files onto the card from the Manager PC.

Related Links

File | Advanced | Format IP Office SD Card on page 60

File | Advanced | Recreate IP Office SD Card

This command can beused with the System SD cards used by IP500 V2 control units. It allows Manager to copy allthe files and folders used by a system when starting onto the card that has been place intothe card slot of the PC running Manager. It updates the card with the version of those files installed with the Manager application. It includes the binary files for the system, externalexpansion modules and phones. The command also copies all language prompt sets used byEmbedded Voicemail.

If the card contains dynamic system files such as SMDR records, they are temporarily backedup by Manager and then restored after the card is recreated. For the card to be used in asystem's **System SD** slot the card must be Avaya SD Feature Key card. The card must becorrectly formatted (see Format IP Office SD card), however a reformat of an existing workingcard is not necessary before using recreate to update the card contents.

The source for the files copied to the SD card are the sub-folders of the **\Memory Cards** folder under Manager's Working Directory (normally **C:\Program Files\Avaya\IPOffice\Manager**). However, if the Working Directory is changed to a location without an appropriate set of **\Memory Cards** sub-folders, the required set of files will not becopied onto the SD card.

Related Links

File | Advanced on page 51
Recreating the IP Office SD Card on page 62

Recreating the IP Office SD Card

About this task

Note:

This process can take up to 20 minutes depending on the PC. Once started, the process should not be interrupted.

Procedure

1. Insert the SD card into a reader slot on the Manager computer.
2. Using Manager, select **File | Advanced | Recreate IP Office SD Card**.
3. Select the type of system for which the card is intended.

   This selection will affect how the system operates when defaulted with this card present in its **System SD** card slot.

   - **IP Office A-Law** A system fitted with this type of card will default to A-Law telephony. The system will default to IP Office Basic Edition - Quick Mode **PBX System** operation.
   - **IP Office U-Law** A system fitted with this type of card will default to ULAW telephony. The system will default to IP Office Basic Edition - Quick Mode **Key System** operation.
   - **IP Office Partner Edition** A system fitted with this type of card will default to A-Law telephony and IPOffice Basic Edition - PARTNER® Mode operation.
   - **IP Office Norstar Edition** A system fitted with this type of card will default to U-Law telephony and IPOffice Basic Edition - Norstar® Mode operation.
   - **Enterprise Branch** Use this option for an SD card intended to be used with an IP Office system running in Enterprise Branch mode. There is a separate SD card for IP Office. The Enterprise Branch SD card can only be used for IP Office operation and cannot be used tochange modes to IP Office. You also cannot use or change an IP Office SD card for use withan Enterprise Branch system.

     Warning:

     Do not re-purpose a Enterprise Branch SD card for use with any other IP Office mode. Doing so may damage the SD card and make it unusable for your Enterprise Branch system.
4. Browse to the card location and click **OK**.
5. Manager will prompt whether you want to include Basic Edition Web Manager files as part of the recreate process.
6. For systems that will be running in Basic Edition mode, these files are necessary if you want to use Web Manager to configure the system.
7. For all systems, these files are necessary if you want to go through the process of on-boarding registration.
8. Manager will start creating folders on the SD card and copying the required files into those folders.

9. Do not remove the card until the process is completed and Manager displays a message that the process has been completed.

Related Links

File | Advanced | Recreate IP Office SD Card on page 61

File | Advanced | Memory Card Command

These commands are used with the memory cards installed in IP500 V2 control units.

Shutdown

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

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

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

Start Up

This command can be used to restart operation of an IP500 V2 memory card that has been shut down. >The command will start the **Select IP Office** discovery process for selection of the system.

Related Links

File | Advanced on page 51

File | Advanced | Launch Voicemail Pro

If the Voicemail Pro client is installed on the same PC as Manager, this link can be used to launch the Voicemail Pro client. This can also be done by clicking on the  icon in the Manager toolbar.

Related Links

File | Advanced on page 51

File | Advanced | System Status

System Status is an application that can be used to monitor and report on the status of a system.

This is a separate application from Manager but if installed on the same PC, it can be started using the **File | Advanced | System Status** link within Manager. Use of the application requires a service user name and password configured on the system for System Status Access within the system's security settings.

Related Links

File | Advanced on page 51

File | Advanced | LVM Greeting Utility

This command launches a utility that can be used to convert .wav files to the formats used by Embedded Voicemail (**c11**). The source file must be in the standard format used for all system applications: PCM, 8kHz 16-bit, mono.

The resulting named greeting files can then be transferred to the Embedded Voicemail memory card and selected as auto attendant greetings. That is done using the Recording Name field on the Auto Attendant | Auto Attendant tab. The same named greeting file can be used in several auto attendants.

The utility can be run separately using the file **LVMGreeting.exe** found in the **LVMGreeting** sub-folder of the Manager application.

Note:

The LVM Greeting Utility option is not selectable (grayed out) when Voicemail Pro is selected as the system's voicemail type.

Related Links

File | Advanced on page 51

File | Advanced | Initial Configuration

Note:

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

Basic Mode and Standard Mode Initial Configuration

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

.

For Quick Mode, Partner Mode and Norstar Mode, leave the selection set to **Basic Mode**.

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

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

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

Server Edition Initial Configuration

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

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

Once the menu is completed and **Save** is clicked, the values entered are written into the system configuration and the system is restarted. The menu is also displayed when creating an offline configuration for a Server Editionsystem. The configuration of an existing non-Server Edition system can be converted to a Server Edition configuration, invoking this menu, using the **File | Advanced | Initial Configuration** menu option.

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

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

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

If selected, the existing configuration is retained. However, some elements of that configuration may be invalid or ignored in a Server Edition solution. It is the installers responsibility to ensure that the final configuration is valid for use in the solution. See IP500 V2 Conversion.

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

Table continues…

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

Enterprise Branch Initial Configuration

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

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

7. In the **DHCP Mode** section, if you selected LAN1, select the appropriate DHCP option. If you selected LAN2, DHCP Mode is disabled.
8. Select the **Under Centralized Management?** check box if you want the IP Office system to be managed by System Manager.
9. If you selected the **Under Centralized Management?** check box, a number of additional fields are shown, configure these additional fields as appropriate:

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

Select **Save**.

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

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

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

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

Related Links

File | Advanced on page 51

File | Advanced | Add/Display VM Locales

This option is only displayed displayed when the configuration from an IP500 V2 systems with its **Voicemail Type** set to **Embedded Voicemail** is received in Manager. It is not shown for off-line configuration or configurations loaded from a PC file.

Selecting this option displays a list of the Embedded Voicemail prompt languages. Those languages already present on the System SD card or not supported are greyed out. Additional languages can be selected and then uploaded from Manager to the system.

When editing the system configuration in Manager, if the locale language selected for the system, a user, a short code or an incoming call route is not already present on the System SD card, Manager will display an error. **Add/Display VM locales** can then be used to upload the prompts for the required language in order to correct the error.

You can reload languages that are already installed on the System SD card. For example, you may want to reload the languages if new prompts have been added in a maintenance release. To reload existing languages, upgrade the system (**File | Advanced | Upgrade**) with the Upload System Files option checked. You can also choose **Upload System Files** from the Embedded File Management utility (**File | Advanced | Embedded File Management**).

The Recreate IP Office SD Card command can be used to locally load all available languages onto an SD card.

Related Links

File | Advanced on page 51

File | Backup/Restore

Backup Binaries and Configurations

This command copies all configuration files (.cfg) and software binary files (.bin) stored in Manager's working directory to a selected folder.

Restore Binaries and Configurations

This command copies all configuration files (.cfg) and software files (.bin) stored in a selected folder to the Manager's working directory.

Related Links

File Menu on page 39

File | Import/Export

Export

This command allows you to export the selected parts of the configuration to either a set of CSV text files (.csv) or a single binary file (.exp).

The display shows those exportable record types for which the configuration contains records. The File Type and the Save In path can be selected at the base. The default location used is sub-directory of the Manager application directory based on system name of the currently loaded system.

Manager imports and exports CSV files using UTF8 character encoding which uses a double byte to support characters with diacritic marks such as ä. Other applications such as Excel, depending on the user PC settings, may use different single-byte encoding which will cause such characters to be removed. Care should be taken to ensure that any tool used to create or edit a CSV supports all the characters expected and is compatible with UTF8.

Import

This command allows you to import configuration settings. Two formats are supported. Binary files (.exp) are settings previously exported from a system using File | Import /Export | Export. CSV text files (.csv) can also be exported from a system or can be created using a plain text editor.

For the selected File Type and the Look In path, the window displays the file or files found. The default location used is sub-directory of the Manager application directory based on system name of the currently loaded system.

Manager imports and exports CSV files using UTF8 character encoding which uses a double byte to support characters with diacritic marks such as ä. Other applications such as Excel, depending on the user PC settings, may use different single-byte encoding which will cause such characters to be removed. Care should be taken to ensure that any tool used to create or edit a CSV supports all the characters expected and is compatible with UTF8.

Related Links

File Menu on page 39

File | Exit

The **File | Exit** command exits the Manager application.

Related Links

File Menu on page 39

View Menu

Toolbars

Allows selection of which toolbars should be shown or hidden in configuration mode. A tick mark is displayed next to the name of those toolbars that are currently shown.

Tooltip

Controls whether additional tooltips are displayed when Manager is running in simplified view mode.

Navigation Pane

Shows or hides the Navigation Pane. A tick mark appears next to the command when the pane is shown.

Group Pane

Shows or hides the Group Pane. A tick mark appears next to the command when the pane is shown.

Details Pane

Sets the location of the Details Pane when the Group Pane is also shown. The Details Pane can be placed either below or to the right of the Group Pane.

Error Pane

Shows or hides the Error Pane. A tick mark appears next to the command when the pane is shown.

Advance View

Causes Manager to switch from its simplified view to advanced view mode. Manager automatically switches to advanced view mode if a Standard Edition configuration is loaded.

Hide Admin Tasks

This settings shows or hides the Admin Tasks List available when Manager has a Basic Edition configuration loaded.

Simplified View

If Manager has no configuration loaded, this command switches it from advanced view to simplified view.

TFTP Log

This command displays the TFTP Log window. This window shows TFTP traffic between Manager and devices that uses TFTP to send and receive files. For example, the TFTP Log below shows an Avaya IP phone requesting and then being sent its software files.

Related Links

Menu Bar Commands on page 39

Tools Menu

Related Links

Menu Bar Commands on page 39
Tools | Extension Renumber on page 71
Tools | Line Renumber on page 71
Tools | Connect To on page 71
Tools | Export | User on page 72
Tools | SCN Service User Management on page 72
Tools | Busy on Held Validation on page 73

Tools | MSN Configuration on page 73
Tools | Print Button Labels on page 74
Tools | Import Templates on page 75

Tools | Extension Renumber

This command allows the extension numbering of user extensions to be changed. The existing extension number range to be adjusted can be specified followed by the new start point for the range after renumbering.

The command does not alter the extension number used for hunt groups but does adjust the extension numbers of hunt group members.

Related Links

Tools Menu on page 70

Tools | Line Renumber

On external trunks Line appearance ID numbers can be assigned to each channel supported in order to allow that channel or line to be associated with a Line Appearance button on phones that support button programming. By default all lines are automatically numbered from 701 upwards when added to the system. This command allows the lines to be renumbered from a different starting point.

Related Links

Tools Menu on page 70

Tools | Connect To

This option can be used to create H.323 IP line connections between two systems in a multi-site network, one being the system with its configuration currently loaded in Manager, the other being selected from a discovery dialog. This option is not available for Server Edition mode.

Important:

This process will require the systems to be rebooted.

Procedure

1. With the configuration of the first system received from that system and displayed in Manager, clicking on or **Tools | Connect To**
2. A discovery menu is displayed and will list any other systems discovered.
3. Select the system to which connection is required.
4. Enter the login name and password for configuration access to that system.

5. Manager will switch to Small Community Network management mode, displaying the configuration of both systems.
6. Click  to save the new configuration back to each system.

Related Links

Tools Menu on page 70

Tools | Export | User

When performing an upgrade from B5800 Branch Gateway 6.2 or IP Office 8.1 to IP Office 9.0, users are not automatically created in System Manager. Before an upgrade, IP Office users must be exported to a file and then the file must be imported to System Manager. This feature allows you to export all users or selected users from a loaded configuration to an XML file that is then imported in System Manager. The default filename is <SystemName>_Users.xml.

User Name – select this check box to export all users.

User Name/Extension – select the appropriate check boxes to export those users.

Related Links

Tools Menu on page 70

Tools | SCN Service User Management

When managing multiple systems, it may be useful to create a common user name and password on all the systems for configuration access. This tool can be used to create a new service user account, **SCN_Admin**, for configuration access.

This process requires you to have a user name and password for security configuration access to each of the systems.

Select **Tools | SCN Service User Management**.

The option is not shown if a Basic Mode system configuration is loaded. If no configuration is loaded, and the option is not shown, select **View | Advanced View**.

Procedure

1. The **Select IP Office** menu displays the list of discovered systems.
2. Select the systems for which you want to create a common configuration account.

   Click **OK**.
3. A user name and password for security configuration access to each system is requested.

   Enter the values and click **OK**. If the same values can be used for all systems enter those values, select **Use above credentials for all remaining, selected IPOs**. If each system requires a different security user names and password, deselect **Use above credentials for all remaining, selected IPOs**.

4. The systems will be listed and whether they already have an **SCN_Admin** account is shown.
5. To create the **SCN_Admin** account on each system and set the password for those account click on **Create Service User**.
6. Enter the common password and click **OK**.
7. The password can be changed in future using the Change Password option.
8. Click **Close**.

Related Links

Tools Menu on page 70

Tools | Busy on Held Validation

Busy on Held is a user feature where, when the user has a call on hold, the system indicate the user as being busy to any further calls.

The use of **Busy on Held** in conjunction with multiple call appearance buttons is deprecated. This command can be used to identify those users who have multiple call appearance buttons and for whom Busy on Held is currently set.

When run, it shows a list of the users affected and if selected their Busy on Held setting will be switched off.

Related Links

Tools Menu on page 70

Tools | 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

Tools Menu on page 70

Tools | Print Button Labels

This option is only enabled if a version of DESI software is also installed on the same PC as Manager. It can then be used when a system configuration is loaded in Manager.

DESI software can be obtained from the Avaya support web site (http://support.avaya.com) or from DESI (http//www.desi.com). Currently, though all users are shown, only ETR, M Series, T-Series, 1400 and 1600 phones are supported by DESI templates.

The text used on the labels:

- If a text label has been added in the user's Button Programming settings, that text label is passed to the DESI application.
- Note that the DESI application cannot import non-ASCII characters and may render them incorrectly.
- Manager will display a warning if it estimates that the user's current text for some buttons may exceed the label space of the phone type.
- If no text label has been set, the default label for the action currently assigned to the button is passed to the DESI application.
- Once the labels are shown in the DESI application, the label text can be changed.

1. Load the configuration of the system for which you want to print button labels.
2. Select **Tools** and then **Print Button Labels**.

- **Name/Extn** These are the user name and extension number details of the users in the system configuration currently loaded in Manager.
- **Phone Type** This field shows the type of phone, if known, that the user is currently associated with. The drop down can be used to change the selection if required.
- **Expansion Modules** If the phone type supports additional button modules, this drop down can be used to select the type and number of button modules.
- **Print Extn** This check box is used to select whether the phone button details should be included in the output passed to the DESI software.
- **Print BM1/Print BM2/Print BM3** These check boxes are used to select whether button module button details should be included in the output passed to the DESI software. These button will only be selectable if the user's **Expansion Modules** is set to the number of button modules.

Click **Print via DESI**to transfer the information to the DESI application. Within DESI, edit the labels as required and then print the labels.

Related Links

Tools Menu on page 70

Tools | Import Templates

Manager can be used to import and use trunk templates. SIP trunk templates can be used to add SIP trunks. Analog trunk templates can also be applied to existing analog trunks. This option does not affect the additional template options used for Server Edition mode.

The templates need to be stored in a specific Manager sub-folder **\Templates**.

Some templates may be supplied with the Manager application and will be automatically installed to the correct location. This command can be used to select a folder containing other template files and will copy those files into the correct Manager sub-folder.

Related Links

Tools Menu on page 70

Security Mode Menus

These commands are available when the Manager is in security configuration mode.

Open Security Settings

Displays the **Select IP Office** menu to select and load a system's security settings. This requires entry of a user name and password with rights to access security settings of the selected system.

This behavior changes when configuration settings have already be received from a system using a service user name and password that also has security access rights for that system. In that case, the system's security settings are automatically loaded without requiring name and password entry.

Close Security Settings

Close the currently open set of security settings received from a system without saving those settings.

Save Security Settings

Send edited security settings back to the system. Requires re-entry of a service user name and password with access rights for security settings.

Reset Security Settings

Reset the security settings of the selected system to defaults. Requires entry of a service user name and password with access rights for resetting the security settings. This option is not usable while a set of security configuration settings is loaded.

The command **File | Advanced | Erase Security Settings (Default)** performs the same action from Manager configuration mode.

Preferences

Displays a window for configuring various aspects of Manager's operation. The window is divided into a number of tabs.

For a description of the Preferences options, see **File | Preferences**.

Exit

This command closes Manager.

Configuration

Returns Manager to configuration mode.

Related Links

Menu Bar Commands on page 39

Embedded File Management Menus

For control units with a memory card installed, the contents of the card can be viewed using Manager. This view can also be used to add and remove files from the card. This may be useful when the memory card is being used to store Music on Hold or IP phone firmware files. For Linux based systems access to the /opt/ipoffice folder is provided.

Embedded Voicemail Files

When viewing the memory card, the files related to Embedded Voicemail are visible, however these files are greyed out (ie. cannot be deleted, downloaded or overwritten).

- Mailbox greetings and messages are shown as `.clp` files.
- The language prompts for Embedded Voicemail functions are stored in separate language sub-folders of **lvmail**. These are `.c11` files.
- Named prompt files for use by Embedded Voicemail auto attendants are stored in the `lvmail \AAG` folder and use the same **.c11** or `.c23` file formats as the language prompts. These files can be created from standard .wav files before being downloaded to the memory card by using the LVM Greeting Utility.

Avaya IP Phone Files

The memory card can be used as the source of files requested by IP Phones when rebooting. For phones using system DHCP, once the files are loaded onto the card, the TFTP Server IP Address and HTTP Server IP Address on the System | System tab must be set to match the system's LAN address.

Viewing a Memory Card

When **Advanced | Embedded File Management** is selected, the Manager will go through normal system discovery but will only allow selection of systems which can support a memory card. When a system is selected, a valid service user name and password for configuration access to that system is requested. If the system selected does not have a memory card installed, the files view remains blank and the message **TFTP:Received TFTP Error "Not Found"** appears in Manager's status bar.

Changing the Files View

The type of display used in the **Files** pane can be changed by selecting from the **View** menu in the toolbar.

Open File Settings

Select a system and display the contents of its memory cards if any are present and in use.

Close File Settings

Close the current memory card contents listing without exiting embedded file management mode.

Refresh File Settings

This command can be used to request a file update from the system.

Upload File

This command can be used to select and upload a file to the memory card in the system.

Upload System Files

This command is available with IP500 V2 systems. When this command is selected, Manager will upload the software files for operation to the System SD card.

Warning:

After this command is completed, the system is rebooted. This will end all calls and services in progress.

- It copies the binary files for the system control unit and possible external expansion modules.
- It copies the firmware files used by phones supported by the system.
- For systems configured to running in Basic Edition mode, the files for Basic Edition Web Manager are copied.
- For systems configured to run Embedded Voicemail, the Embedded Voicemail prompts for those supported languages set as the system locale, user locales, incoming call route locales and short code locales are upgraded. In addition the English language prompts are upgraded as follows: **IP Office A-Law/Norstar SD Cards** - UK English, **IP Office U Law/PARTNER SD Cards** - US English.

Backup System Files

This command is available with IP500 V2 systems. When selected, Manager copies the folders and files from the **System SD** card's `/primary` folder to its `/backup` folder. Any matching files and folders already present are overwritten. This action can be included as part of the system's automatic daily backup process (System | System | Automatic Backup).

Restore System Files

This command is available with IP500 V2 systems. When selected, Manager copies the folders and files from the **System SD** card's `/backup` folder to its `/primary` folder. Any matching files and folders already present are overwritten.

Warning:

After this command is completed, the system is rebooted. This will end all calls and services in progress.

Upgrade Binaries

This command is available for IP500 V2 systems that have a system SD card and Optional SD card installed.

When this command is selected, all files except **config.cfg** and `keys.txt` files in the Optional SD card's `\primary` folder are copied to the System SD card.

Warning:

After this command is completed, the system is rebooted. This will end all calls and services in progress.

Upgrade Configuration

This command is not used with IP Office systems. This command is available for IP500 V2 systems that have a system SD card and Optional SD card installed.

When this command is selected, any **config.cfg** and `keys.txt` files in the Optional SD card's `\primary` folder are copied to the System SD card.

Warning:

After this command is completed, the system is rebooted. This will end all calls and services in progress.

Upload Phone Files

This command is available for IP500 V2 control units. When this command is selected, Manager copies the software files relating to phone firmware to the memory card. For IP500 V2 control units, use Upload System Files.

Copy System Card

This command is available for IP500 V2 systems that have an Optional SD card installed in addition to the mandatory System SD card. When this command is selected, the system will copy the folders and files on its **System SD** card to the **Optional SD** card. Any matching files and folders already present on the **Optional SD** card are overwritten.

This process takes at least 90 minutes and can take longer.

Configuration

This command will exit Embedded File Management and return Manager to configuration editing mode.

Related Links

Menu Bar Commands on page 39

Chapter 5: Manager User Interface

This section of the documentation covers the operation of Manager when being used to edit the configuration of a system running in Standard Mode. Much of it is also applicable for when also editing the configuration of systems running in Server Edition mode. Additional Server Edition Mode functions are detailed in the next chapter.

Related Links

Title Bar on page 79
Toolbars on page 79
The Navigation Pane on page 81
The Group Pane on page 82
The Details Pane on page 84
The Error Pane on page 86
The Status Bar on page 88

Title Bar

The Manager title bar shows the following information.

- The Manager application version.
- The system name of the system from which the currently loaded configuration was received.
- The software level of the system's control unit.
- The service user name used to receive the configuration and that user's associated operator rights.

Related Links

Manager User Interface on page 79

Toolbars

Manager displays the following toolbars:

- Main Toolbar

- Navigation Toolbar
- Details Toolbar

Related Links

Manager User Interface on page 79

The Main Toolbar

The Main toolbar is displayed at the top of the Manager window, just below the menu bar. This toolbar is also available when Manager is in security mode. However many of the controls will not function in security mode.

Open Configuration from a System Advertises to the address currently shown in the Manager's title bar for any available systems. A list of responding systems is then displayed. When a system is selected from this list, a valid user name and password must be entered. Equivalent to **File | Open Configuration**.

Open Configuration File Open a configuration file stored on a PC. The button can be clicked to display a browse window. Alternatively the adjacent ▾ arrow can be used to drop-down a list of the last 4 previously opened configuration files. Equivalent to **File | Offline | Open File**.

Save Configuration File The action of this icon depends on whether the currently loaded configuration settings were received from a system or opened from a file stored on PC. If the former applies, the menu sending the configuration back to the system is displayed. In the latter case, the file changes are saved to the original file. Equivalent to **File | Save Configuration**.

Collapse All Groups Causes all ⊟ symbols in the navigation pane to be collapsed to ⊞ symbols.

Show/Hide the Navigation Pane

Show/Hide the Group Pane

Show/Hide the Error Pane

Validate Configuration Runs a validation on all the currently loaded configuration settings. The results appear in the error pane. By default the configuration is automatically validated when loaded and changes are validated when made, however the validation preferences can be changed through File | Preferences | Validation.

Create New Configuration Runs a series of dialogs that create a new configuration from scratch.

Connect To For a standalone system, start the process of adding it to a multi-site network. Not available in Server Edition mode.

Voicemail Pro Client Launch the Voicemail Pro client if also installed on the Manager PC.

Server Edition Solution View Switch to the solution view. This option is only shown when Manager is running in Server Edition mode.

The Navigation Toolbar

This toolbar provides drop down lists which can be used to navigate to particular records in the configuration settings. The selected options in the navigation pane, group pane and the details pane are synchronized with the navigation toolbar and vice versa. This toolbar is particularly useful if you want to work with the group pane and or navigation pane hidden in order to maximize the display space for the details pane.

This toolbar is not available when Manager is in security mode.

The Details Toolbar

This toolbar is shown in the top-right of the details pane. The options within the toolbar may vary or be greyed out depending on the actions allowed for a particular configuration record.

Create a New Record The ▾ arrow is used to select the record type to be created. For example; when adding an extension clicking ▾ may allow selection of a VoIP Extension or IP DECT Extension.

Export as Template (Binary) This option is shown for Server Edition mode. It allows certain types of records to be saved as templates. These can then be used to create new records.

Delete Current Record Delete the currently displayed record.

Validate Current Record By default records are validated when opened and when edited. This is set through the Manager application's validation settings.

< > **Previous Record/Next Record** Click < or > at the top-right to move to the previous or next record.

The Navigation Pane

This pane shows icons for the different types of record that the configuration can contain. Each type is followed by the number of records of that type already in the configuration. When Manager is used in security mode, this pane is also used by Manager in security mode to display records for security settings.

Selecting an icon displays the matching records in the group pane, navigation toolbar and details pane. Note that Manager is used to configure different types of system. Therefore the icons shown may vary depending on the type of system you are configuring. For descriptions of the different icons refer to Configuration Settings.

The information in the pane also depends on whether the group pane is visible or not. If the group pane is visible, the navigation pane just shows icons for accessing which types of records should be shown in the group pane. The group pane can then be used to select which of those records is currently shown in the details pane. If the group pane is not visible, the navigation pane shows icons for each type of records and under those icons for each individual record. The navigation pane can then be used to select which of those records is currently shown in the details pane.

Related Links

Manager User Interface on page 79

Expanding and Collapsing the Navigation Tree

Where ⊞ or ⊟ icons appear in the pane, they allow the structure to be expanded or collapsed. When the group pane is hidden, ⊞ and ⊟ icons are shown for each record type and allow the record type to be expanded to display all the existing records of that type.

The  icon in the main toolbar can also be used to collapse all the expanded record types shown in the navigation pane.

The Group Pane

This pane lists all the records that match the type selected in the navigation pane or navigation toolbar. The list can be sorted by clicking on a column heading. Selecting a record in this pane displays its details in the details pane.

The icons used in the pane may vary according to the state of the record. For example, some of the users shown in this example have been configured for hot desking. This pane is also used by Manager in security mode to display records for security settings.

Related Links

Manager User Interface on page 79

Sorting the List

About this task

The records shown in the group pane can be sorted using any of the columns displayed.

Procedure

1. To sort the list using the details in a particular column, click on the column header.
2. Clicking on the same column header again reverses the sort order.

Customizing the Columns Displayed

About this task

For each record type, which details are shown in the group pane can be customized. Also the order of the column can be adjusted.

Procedure

1. Right-click on the pane and select **Customize Columns**.
2. To add a column, selects its name in the left-hand Available Columns list and click **>>**to move it to the right-hand **Selected Columns** list.
3. To remove a column, select its name in the right-hand **Selected Columns** list and click **^lt;^lt;** to move it to the left-hand **Available Columns** list.
4. To change the order of the **Selected Columns**, click on a column name and use the **^** and **V** controls.
5. Click **OK**.

Changing the Column Widths

About this task
Procedure

1. In the column headers, place the cursor over the border between two columns.
2. When the cursor changes to a double headed arrow with a bar through it, click and hold the cursor.
3. Drag the border to the required position and release the cursor.

Adding a New Record

About this task

The group pane can be used to add a new record of the type currently displayed.

Right-click on the pane and select **New**.

A ▸ arrow symbol next to **New** indicates that you can select a particular type of new record to create. Click the arrow and select an option from the list.

Procedure

1. Use the details pane to configure the new record.
2. Click **OK**in the details pane.

Deleting an Record

About this task
Procedure

1. Select the record to be deleted by clicking on it.
2. Right-click on the pane and select **Delete**.

Validating an Record

About this task
Procedure

1. Select the record to be validated by clicking on it.
2. Right-click on the pane and select **Validate**.

Show in Groups

About this task

This command groups the items shown in the group pane. The grouping method will vary depending on the record type being listed. For example, short codes are grouped based on short code feature type such as all forwarding short codes together.

Procedure

Right-click on the pane and select **Show In Groups**.

The Details Pane

Whenever a selection is made through the group pane or the navigation toolbar, the settings for the matching record are shown in the details pane. This pane is also used by Manager in security mode to display records for security settings.

The details are grouped into tabs. The tabs available may vary depending on what particular type of record is being viewed.

Individual settings may also be grayed out. This indicates that they are either for information only or that they cannot be used until another setting is enabled.

The top-left icon indicates the following:

	**Locked** Indicates that you can view the settings but cannot change them.
	**Editable** Indicates that you can change the settings if required.
	**Changed** Indicates that the settings have been changed since the tab was opened. Click OK to save the changes or Cancel to undo.

Various icons may appear adjacent to settings:

	**Locked Setting** The setting cannot be changed through this tab. This icon appears on user settings where the user is associated with User Rights that controls the setting.
	**Information** Indicates a value which does not have to be set but may be useful if set.
	**Warning** A warning indicates a configuration setting value that is not typical and may indicate misconfiguration.
	**Error** An error indicates a configuration setting value that is not supported by the system. Such settings may cause the system to not operate as expected.

Related Links

Manager User Interface on page 79
Managing Records on page 85

Managing Records

Procedure

1. Edit a record
   a. The method of entering a record varies as different fields may use different methods. For example text record boxes or drop down lists.
   b. By default when changes are made, they are validated once another field is selected. See **File | Preferences | Validation**.
   c. Click on **OK** at the base of the details pane to accept the changes or click on **Cancel** to undo the changes.
2. Add a record.
   a. Click  at the top-right of the details pane.

b. Select the type of record required. For example, with extensions you can select from **H.323 Extension** or **SIP Extension**.

3. Delete a record.

   Click ✕ at the top-right of the details pane.

4. Validate a record.

   Click ✓ at the top-right of the details pane.

5. Move to the previous or next record.

   Click **<**or **>** at the top-right to move to the previous or next record.

6. Select a new tab.

   a. To view the detail stored on a particular tab, click on the name of that tab.

   b. If the tab required is not shown, use the  controls if shown on the right to scroll through the available tabs. The tabs available may vary depending on what particular type of record is being viewed.

Related Links

The Details Pane on page 84

The Error Pane

Validation is a process where Manager checks configuration records for errors or for values for which it regards as requiring a warning. The results of this checking are shown by icons next to the field that caused the error or warning, All errors and warnings are also listed in the Error Pane.

By default validation is performed automatically whenever a configuration file is opened and when any field is edited. However, if required, the use of automatic validation can be controlled through the settings on the File | Preference | Validation tab.

Icons

The icons used for errors and warnings are as follows. These are shown in the error pane and also next to the related field in the details pane. In the details pane, the error or warning description is shown when the cursor is hovered over the icon.

Error An error indicates a configuration setting value that is not supported by the system. Such settings are likely to cause the system to not operate as expected.

Warning A warning indicates a configuration setting value that is not typical and may indicate misconfiguration.

Information Typically indicates a setting which may be useful to set.

Related Links

Manager User Interface on page 79

Altering the Automatic Validation Settings

About this task

The settings for automatic validation are adjustable.

Procedure

1. Select **File | Preferences**.
2. Select the **Validation** tab.

   Select the options required.

   - **Validate configuration on open** Automatically validate configuration files when they are opened in Manager.
   - **Validate configuration on edit** Validate the whole configuration when **OK** is clicked after editing a record. For large configurations, disabling this option removes the delay caused by validating the configuration after every edit.
   - **Prompt for configuration validation on save or send** If selected, when saving or sending a configuration, a prompt is displayed asking whether the configuration should be validated. If validation is selected and error are found, the send or save process is canceled. This option is disabled if Validate configuration on edit is selected.
3. Click **OK**.

Revalidating Configuration Settings

About this task

If necessary, you can force a validation check of the whole configuration or of the current record shown in the details pane.

Procedure

1. To validate the whole configuration, click ✓ in the main toolbar.
2. For a particular record, click ✓ in the details pane.

Viewing an Error or Warning

About this task
Procedure

1. Clicking on an error or warning in the error pane will load the matching record tab into the details pane.
2. The **^lt;** and **>** can be used to move to the next error or warning in the error pane.

The Status Bar

The status bar at the base of the Manager screen is used to display icons and messages about communications between Manager and systems. If the Manager is also acting as a BOOTP and TFTP server it will also show BOOTP and TFTP messages.

A padlock icon is displayed whenever the Manager communications settings are set to secure. This indicates all attempted configuration and security settings exchanged will be attempted over a secure TLS link:

Status bar messages display information about communications the Manager application receives. Some typical status bar messages are listed below.

Ready

This message is normally seen when Manager has just started and no configuration has been received.

Received BOOTP request for 001125465ab2, unable to process

Manager is acting as a BOOTP server. It has received a BOOTP request that does not match a system listed in its BOOTP records. The cause may be a device or application, other than an IP Office, that also uses BOOTP.

TFTP: Received TFTP Error "NotFound" from 192.168.42.1

An attempt to receive settings from or send settings to the system failed. The most probable cause is a name or password error.

TFTP: Received 17408 bytes for Marks_Test

Manager has received configuration settings from the named system using TFTP.

Sent 100% of C:\Program Files\Avaya\IP Office\Manager\b10d01b2_3.bin

Manager has sent the indicated file in response to a BOOTP request.

Related Links

Manager User Interface on page 79

Configuring the Interface

The Manager configuration settings interface can be customized in a number of ways. These changes are remembered the next time Manager is started.

Related Links

Manager User Interface on page 79

Resizing the Manager Window

About this task

When the Manager window is not maximized or minimized, it size can be adjusted.

Procedure

1. Place the cursor over the edge of the current window.
2. When the cursor changes to a double-headed arrow, click and hold the cursor.
3. Drag the edge to the required position and then release the cursor.

Moving the Border Between the Panes

About this task

The border between the visible panes can be adjusted. Note that this is a proportional rather than exact position. If the whole window size is altered, the border position may also move.

Procedure

1. Place the cursor over the border between two panes.
2. When the cursor changes to a double headed arrow with a bar through it, click and hold the cursor.
3. Drag the border to the required position and release the cursor.

Showing or Hiding Toolbars

About this task

The different toolbars can be hidden if not required.

Procedure

1. Select **View** and then **Toolbars**.

   Those toolbars currently shown are indicated by a tick mark.
2. To show or hide a toolbar, click on its name.

Moving Toolbars

About this task

The position of the Manager toolbars can be moved. Note that when moving a toolbar, the other toolbars and panes may adjust their size or position to ensure that all the toolbar icons remain visible.

Procedure

1. Place the cursor over the end of the toolbar.
2. When the cursor changes to a four-way arrow, click and hold the cursor.
3. Move the toolbar to the required position and release the cursor.

Showing or Hiding Panes

About this task

The details pane cannot be hidden. The navigation pane, group pane and error pane can be shown or hidden. To do this use either of the following methods.

From the main toolbar, use the following icons:

- **Hide/Show Navigation Pane**.
- **Hide/Show Group Pane**.
- **Hide/Show Error Pane**.

or

Procedure

1. Select **View**.

   Those panes currently shown are indicated by a tick mark.
2. To show or hide a pane, click on its name.

Changing the Position of the Details Pane

About this task

When the group pane is visible, the details pane is shown either below it or to its right. This position can be adjusted.

Procedure

1. Select **View** and then **Details Pane**.
2. The current position setting is indicated by a tick mark.

3. To select a position, click on it.

Changing the Size of Configuration Icons

About this task

The size of the icons used on the navigation pane and details pane can be adjusted.

Procedure

1. Select **File** and then **Preferences**.
2. Select the **Visual Preferences** tab.
3. Select the required icon size from **Small**, **Medium** or **Large**.
4. Click **OK**.

Changing Tab Display

About this task

For records with more than two tabs, you can select whether Manager should use  controls or arrange the tabs as multiple rows when necessary.

Procedure

1. Select **Files | Preferences | Visual Preferences**.
2. Select **Multiline Tabs**.
3. Click **OK**.

Chapter 6: Working with the Server Edition Manager User Interface

Related Links

Server Edition Solution View on page 92
System Inventories on page 94
Default Settings on page 94
Record Consolidation on page 95
Configuring Telephony Operation on page 96
Telephone Features Supported Across Server Edition and SCN Networks on page 123
IP500 V2 Conversion on page 125

Server Edition Solution View

When the configuration of a Server Edition solution is loaded into Manager, Manager starts with the **Server Edition Solution View** menu. This menu includes the system inventory of the servers, links for launching various functions and a summary table of the servers and the links between the servers.

Displaying the Server Edition Solution View

Manager normally starts with the Server Edition Solution View when the configuration for a Server Edition network is loaded. However, if required, to return to the solution view do one of the following.

- Click on the  **Server EditionSolution View** icon in the toolbar.
- Click on the  **Solution** icon in the navigation pane.

Interpreting and Using the Network Table

The table at the bottom of the solution view give a quick overview of all the servers and whether their configuration was loaded into Manager.

Description	This column describes the type of server being detailed by the row. It also includes a status indicator for the configuration file that Manager has loaded for the server. • **Green - Configuration Loaded** The configuration of the server has been successfully retrieved and can be edited in Manager.

Table continues…

	• **Yellow - Offline Configuration Loaded** The configuration loaded is an offline configuration. This will appear for a server that has been added to the solution when the physical server is not currently connected on the network and **Create Offline Configuration** was selected. The offline configuration file is stored on and retrieved from the primary server until it can be replaced by or replace the actual server configuration. • **Red - Configuration Not Loaded** There is no configuration for the system loaded even though the solution configuration includes an entry for the server. This will appear for a server that has been added to the network when the physical server is not currently connected on the network and **Create Offline Configuration** was not selected. If may also appear if the server is currently not contactable. • **Grey - No Connection** This icon is used in conjunctions with the others to indicate that there is no current connection to the server. For example: • In conjunction with a green icon, it indicates that the server for which a configuration has been loaded cannot be detected on the network. This may be a temporary issue caused by that particular server rebooting following a configuration change. • In conjunction with a red icon, it indicates that the server for which a configuration has not been loaded has now been detected on the network. Saving and reloading the solution configuration may resolve the issue.
Name	This is the server name as taken from its configuration file. **Offline** is shown if no configuration file is available.
Address	The IP address of the server. This is the address that is used when Manager attempts to retrieve the servers configuration when loading the solution configuration.
Primary Link	This value indicates the configuration settings of the H.323 IP trunk between the primary server and the server indicated by the row. It should state **Bothway**. If it states anything other, that indicates a mismatch in H.323 IP trunk configuration between the system and the primary server. To correct this, right-click on the row and select **Connect to Primary**.
Secondary Link	This column is only shown after a secondary server has been added to the configuration of the solution. The value indicates the configuration settings of the H. 323 IP trunk between the secondary server and the server indicated by the row. It should state **Bothway**. If it states anything other, that indicates a mismatch in H.323 IP trunk configuration between the system and the secondary server. To correct this, right-click on the row and select **Connect to Secondary**.
Users Configured	This column summarizes the number of users (other than **NoUser**) configured on the server. A total for the whole network is shown in the **Solution** row.
Extensions Configured	This column summarizes the number of extensions configured on the server. A total for the whole network is shown in the **Solution** row.

Right-clicking on a server in the table may present a number of action. The actions available vary with the current state of the network configuration.

- **Remove** Remove the server from the solution configuration.

- **Connect to Primary** Repair the configuration of the H.323 IP trunks between the server and the primary server.
- **Connect to Secondary** Repair the configuration of the H.323 IP trunks between the server and the secondary server.
- **Create Offline Configuration** Create an offline configuration file for a server for which no actual configuration has been loaded. The Offline Configuration menu will be displayed followed by the Initial Configuration menu for the server type. The offline configuration file is saved on the primary server.

Related Links

Working with the Server Edition Manager User Interface on page 92

System Inventories

Manager can be used to display a system inventory for any of the servers in the Server Edition solution. The system inventory is a quick summary of key settings and information about the server. It can also display an overview system inventory for the whole Server Edition solution.

Displaying a Server's System Inventory

The method for displaying the system inventory depends on what is currently being displayed by Manager.

In the Server Edition Solution View, using the table at the bottom of the menu, click on the server for which you want to display the system inventory. Click on **Network** for the inventory of the Server Edition network.

or

In the navigation pane, click on the  icon of the server for which you want to display the system inventory. Click on the  **Network** icon for the inventory of the Server Edition network.

Related Links

Working with the Server Edition Manager User Interface on page 92

Default Settings

Most of the defaults for systems in a Server Edition solution match those of individual IP Office systems as detailed in the Configuration Settings section. The table lists some differences.

All auto-create extension and auto-create user settings for IP devices are set to off.

Settings		Primary Server	Secondary Server	Expansion System
System	**Time Settings**	Hidden. Time taken from host server.	SNTP from the primary server.	
	Voicemail	Voicemail Pro	Centralized Voicemail to the primary server	
	Alarms	Syslog relay all alarms to the local host.	Syslog relay all alarms to the primary server.	
	IP Address	Specified during initial configuration menu.		
Lines	**Physical**	–	–	Auto-created
	IP Lines	H.323 line to the secondary and each expansion system. Backup to secondary.	H.323 line to the primary and each expansion system. Backup to primary.	H.323 line to the primary and to the secondary if present. No backup.
Extension	**Physical**	–	–	Auto-created but no base extension setting.
	IP	None	None	None
User		None	None	None
Hunt Group		None	Not allowed	Not allowed
Incoming Call Route		None	Replicated from primary.	
Directory		Stored on the primary	Configured to obtain system directory from the primary server.	
User Rights		None	Replicated from primary.	
ARS	**50:Main**	Short code to secondary	Short code to primary	Short code to primary and to secondary if present.

Related Links

Working with the Server Edition Manager User Interface on page 92

Record Consolidation

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

Working with the Server Edition Manager User Interface on page 92

Configuring Telephony Operation

Each server in the network acts as a separate telephone system and supports most of the features detailed for standalone IP Office systems in the Configuration Settings, Button Programming, Appearance Button Operation and Telephone Features sections of this documentation. For features that are supported between systems in the network, refer to Network Telephony Features.

Each system in the network automatically shares the extension numbers of users and hunt groups. These can be dialed by any user regardless of which system they are hosted on and appear in the internal directories on Avaya phones and applications.

The external system directory held by the primary server is shared with all systems on the network. It is accessible by all users through the directory on their Avaya phones and applications.

Related Links

Working with the Server Edition Manager User Interface on page 92
Incoming Call Routing on page 97

Outgoing Call Routing on page 102

Incoming Call Routing

The routing of incoming external calls is controlled by Incoming Call Route entries added to the configuration of the network.

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.

The entries are shared by all systems in the network. If a specific route is required for a particular system, it should be recalled that the Incoming Group ID assigned to a trunk or trunks can be used as one of the criteria that must be matched on an incoming call route for calls to use that route.

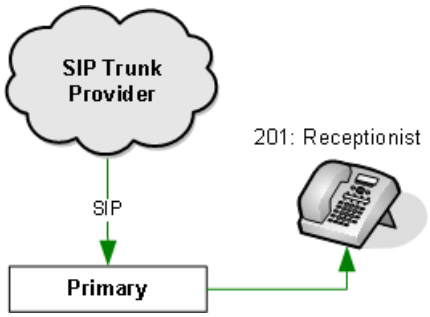
The following are a number of examples that summarize the configuration changes necessary for incoming call routing. These are simple examples and cannot cover all possible scenarios.

Related Links

Configuring Telephony Operation on page 96
Example 1: Routing All Calls to an Operator on page 97
Example 2: Routing All Calls to an Operator Group on page 99
Example 3: Routing DID Calls to Matching Extensions on page 100

Example 1: Routing All Calls to an Operator

In this scenario, all incoming external calls are routed to a single user extension number. Depending on the system licensing, that user can be configured as a receptionist, using the IP Office SoftConsole application in parallel with their phone to answer and distribute the incoming calls.



1. Setup the Trunk Incoming Group IDs.

The **Incoming Group** setting of the external line on the Primary Server has been set to **8**. The same incoming group ID can be used on multiple lines and on lines on different systems.

The location of the **Incoming Group** field varies depending on the type of trunk. For SIP trunks, it is set as part of the **SIP URI** settings used by the trunk.

2. Configure the Call Destinations.

   A new user with extension number **201** is added to the configuration of the primary, along with a matching extension for their IP phone.

   If the user is to use the IP Office SoftConsole application, they must be added to the configuration of the primary server. Receptionist users are not supported on other systems in the network. If the user is not intending to use IP Office SoftConsole, they could be located on any system in the network. External calls would be routed to the system hosting the user.

3. Create an Incoming Call Route to Match the Calls.

   A new **Incoming Call Route** record is added to the configuration settings. The key settings used in this scenario are listed below. All other fields are left at their defaults:

   a. The fields on the **Standard** tab are used to set the criteria that are used to match incoming calls to call routes.

      - **Bearer Capability**: **Any Voice** This will match the incoming voice calls.
      - **Line Group ID**: **8** This will match only calls on trunks where the trunk has its **Incoming Group** setting also set to **8**.
      - **Incoming Number**: blank This will match any call.

   b. The **Destination** tab is used to set the destination for calls that are matched to the incoming call route. If necessary multiple destinations can be set, with **Time Profiles** used to set when the different destinations are used. For this scenario we only have one destination we want to use.

      Using the **Destination** drop-down list, the **201 Receptionist** user has been selected as the destination for all calls. If they do not answer, the calls will go to their voicemail mailbox. This is the simplest form of call routing. If required options such as a fallback destination could be specified and different destinations to be automatically used outside the operators known hours of work.

4. Save the configuration.

Result

All incoming voice calls on the primary system's SIP trunks are now matched to the new incoming call route and are directed to the receptionist to be answered or to leave a message.

Since the **Incoming Call Route** entry is by default replicated as part of the configuration used by all the servers, applying the same **Incoming Group** setting to any trunk hosted by any other system in the network will route calls to the same destination without any further configuration.

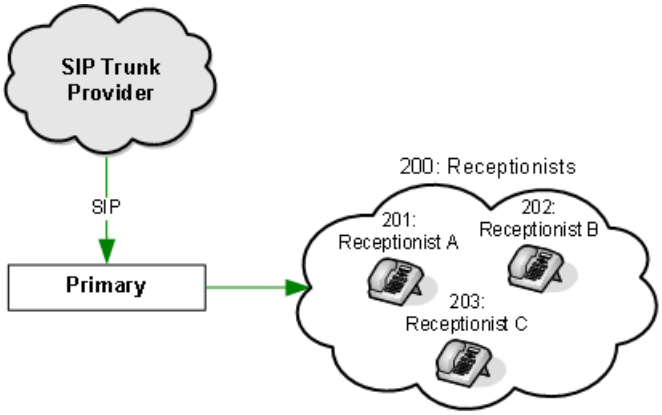
Related Links

Incoming Call Routing on page 97

Example 2: Routing All Calls to an Operator Group

In this scenario, all incoming external calls are routed to a single hunt group extension number. That hunt group can be used to contain a number of user extension numbers and to specify the order in which new calls should be presented to available users, whether calls should queue for an available user and a range of other features. This is an ideal solution for scenarios where you have several receptionists who can answer incoming external calls.

The configuration is very similar to that used in Example 1. Once the additional users have been added and the hunt group created, the hunt group extension number automatically becomes available as a selectable destination for **Incoming Call Routes**.



1. Setup the Trunk Incoming Group IDs

   The **Incoming Group** setting of the external line on the Primary Server has been set to **8**. The same incoming group ID can be used on multiple lines and on lines on different systems.

   The location of the **Incoming Group** field varies depending on the type of trunk. For SIP trunks, it is set as part of the **SIP URI** settings used by the trunk.

2. Configure the Call Destinations

   Any existing receptionist user plus any new receptionists need to be added as members of a hunt group.

   New extension users with extension numbers **201**, **202** and **203** are added to the configuration of the primary, along with a matching extension for their IP phones.

   A new hunt group with extension number **200** is added to the configuration of the primary and users **201**, **202** and **203** are specified as members of the group.

3. Create an Incoming Call Route to Match the Calls

   A new **Incoming Call Route** record is added to the configuration settings. The key settings used in this scenario are listed below. All other fields are left at their defaults.

   a. The fields on the**Standard** tab are used to set the criteria that are used to match incoming calls to call routes.

      - **Bearer Capability**: **Any Voice** This will match the incoming voice calls.

- **Line Group ID**: **8** This will match only calls on trunks where the trunk has its **Incoming Group** setting also set to **8**.
- **Incoming Number**: blank This will match any call.

b. The **Destination** tab is used to set the destination for calls that are matched to the incoming call route. If necessary multiple destinations can be set, with **Time Profiles** used to set when the different destinations are used. For this scenario we only have one destination we want to use.

Using the **Destination** drop-down list, the **200 Reception** group has been selected as the destination for all calls. If they do not answer, the calls will go to their voicemail mailbox. This is the simplest form of call routing. If required options such as a fallback destination could be specified and different destinations to be automatically used outside the operators known hours of work.

4. Save the configuration.

Result

All incoming voice calls on the primary system's SIP trunks are now matched to the new incoming call route and are directed to the receptionist to be answered or to leave a message.

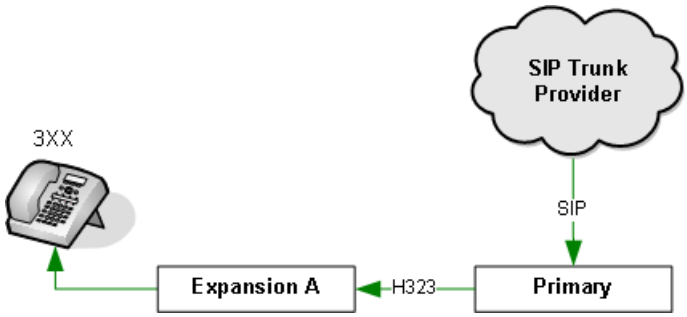
Since the **Incoming Call Route** entry is by default replicated as part of the configuration used by all the servers, applying the same **Incoming Group** setting to any trunk hosted by any other system in the network will route calls to the same destination without any further configuration.

Related Links

Incoming Call Routing on page 97

Example 3: Routing DID Calls to Matching Extensions

In this scenario, the customer has subscribed to receive incoming number digits in the range 300 to 399 on certain calls. They want those calls routed to match extension numbers on the system, ie. to users and hunt groups with the extension numbers in the range 300 to 399.



1. Setup the Trunk Incoming Group IDs

The **Incoming Group** setting of the external line on the Primary Server has been set to **8**. The same incoming group ID can be used on multiple lines and on lines on different systems.

The location of the **Incoming Group** field varies depending on the type of trunk. For SIP trunks, it is set as part of the **SIP URI** settings used by the trunk.

2. Configure the Call Destinations

   New extension users and hunt groups with extension numbers in the range 300 to 399 have been added to the configurations of the systems as required to meet the customers needs.

3. Create an Incoming Call Route to Match the Calls

   A new **Incoming Call Route** record is added to the configuration settings. The key settings used in this scenario are listed below. All other fields are left at their defaults.

   - The fields on the **Standard** tab are used to set the criteria that are used to match incoming calls to call routes.
     - **Bearer Capability**: **Any Voice** This will match the incoming voice calls.
     - **Line Group ID**: **8** This will match only calls on trunks where the trunk has its **Incoming Group** setting also set to **8**.
     - **Incoming Number**: **3XX** This will match any call where the incoming number received with the call ends in 300 to 399. If no **Incoming Number** match occurs, the call will be matched to a default incoming call route with a blank **Incoming Number** field as setup in examples 1 and 2.

       Note that this is acting of digits supplied by the line provider, it is not caller ID (ICLID) matching. Caller ID matching can be done using the Incoming CLI field.
   - The **Destination** tab is used to set the destination for calls that are matched to the incoming call route. If necessary multiple destinations can be set, with **Time Profiles** used to set when the different destinations are used. For this scenario we only have one destination we want to use.

     In the **Destination** field, manually enter 3#. When this route is matched by a call, the **#** in the destination is replaced by the incoming digits that matched the XX wildcards in the Incoming Number field.

4. Save the configuration.

Result

Any incoming voice calls on the primary system's SIP trunks that now include 3XX at the end of an incoming number supplied with the call are matched to this call route rather than to the route previously setup (Example 1 or Example 2) and are routed to the matching extension number. Calls where no incoming number match occurs are still matched to the previous incoming call route with a blank **Incoming Number** field.

Related Links

Incoming Call Routing on page 97

Outgoing Call Routing

When a user dials a number, it is checked in a number of ways:

- The number dialed is always checked first for a match to an extension number. If a match occurs, the call is routed to the matching user or hunt group. This matching is against any extension number in the network, not just local system extension numbers.
- If the dialing does not match an extension number, it is checked for a matching short code. Depending on the source of the dialing, the checking is made against user short codes, user rights short codes and finally against system short codes. See Short Codes for full details.
- Dialing that is matched to a short code that uses the **Dial** feature is assumed to potentially be an outgoing external call. The matching short code defines which where the call should be sent and what number to dial should be sent.
- The normal practice is to route calls that match a Dial feature short code to an ARS form. The ARS form can contain additional short codes to determine to which lines particular numbers are routed. Doing this also helps keep external call short codes separate from short codes for other functions and thus easier to maintain.

Call Routing Recommendations

Calls can be routed to a trunk using short codes set in the configuration of a particular user, users (using User Rights), system (using system short codes) or ARS short codes. The following are recommendations for the configuration on external call routing in a network:

1. Use ARS short codes wherever possible. This simplifies configuration and maintenance by keeping call routing short codes separate from any other short codes, making the configuration easier to implement and to understand. It also means that the full range of other ARS features such as overflow and fallback routing can be used.
2. By default all calls are routed to the primary server and then fallback to the secondary. Implementing as much call routing in the ARS settings of the primary as possible saves on having to implement multiple matching settings on all the expansion servers in the network. This eases maintenance and the addition of new expansion servers.

Short Codes and ARS Forms

Outgoing call routing relies on short codes and ARS records in the system configuration. Refer to the relevant chapters on Short Codes and ARS to understand how those types of configuration records are used.

The short method for describing short codes in this manual, for example **9N/Dial/./0**, indicates the settings of the following fields of a short code: **Code/Feature/Telephone Number/Line Group ID**. For a description of the individual fields see Short Code.

Related Links

Configuring Telephony Operation on page 96
Default Call Routing on page 103
Example 1: Using SIP Trunks Hosted by the Primary on page 105
Example 2: Primary Trunk Fallback to Secondary Trunks on page 108

Example 3: Using Trunks on an Expansion System (V2) on page 112
Example 4: Local Branch Override on page 116
Example 5: PSTN Tail-End-Hop-Off on page 119

Default Call Routing

For outgoing call routing, a combination of system short codes and ARS entries are used. The default operation is listed below. The default configuration is not sufficient to complete call routing, additional configuration is required to route the calls from the Primary Server to the external trunks hosted by the network.

The default settings send all potential external calls to the Primary Server where it is assumed those calls will be routed to SIP trunks hosted by the primary. Additional configuration is necessary to complete the routing from the Primary Server. The configuration to do that will vary depending on which system is hosting the external trunk or trunks. Examples of typical configuration changes required are given below.

The above default operation is achieved by the following defaults:

Primary Server:

The following external call routing is configured by default on the Primary Server:

- **Default System Short Code**
- The server has a default system short code that is used as a match for any dialing that does not match an extension number or any other short code. This default system short code is also used for matching to digits received on calls from other systems in the network. The default system short code used depends on the server's companding (A-Law or U-Law) setting.
  - **A-Law** On A-Law systems, a default **?** short code is used to route any external dialing to ARS record **50:Main**. This will include matching any digits received on calls from other servers in the network that don't match extension numbers.
  - **U-Law** On U-Law systems, it is assumed that external calls are indicated by a 9 prefix. A default short code **9N** is used to route the digits N to ARS record **50:Main**.
- **Default ARS 50:Main**

  A first **?** short code in the ARS form routes calls to the H.323 line that goes to the Primary Server server by using the **Line Group ID** of **0**.

All Other Servers:

On all other server types, the system and ARS defaults are set to route all potential external calls to the Primary Server.

- **Default System Short Code**
- A default system **?** short code is present in the configuration. This routes any dialing that has no other match to the ARS record **50:Main** in the configuration of the system where the dialing occurred.
- **Default ARS 50:Main**

A default ? short code in the ARS record is used to route all calls to the Primary Server. On expansion systems, an additional ? short code is used to route calls to the Secondary Server if the Primary Server is not available for some reason.

Default Settings Summary

The table below summarizes the settings described above.

A-Law	System Short Code	ARS 50:Main Short Codes	Description
Primary Server	?/Dial/./50:Main	?/Dial/./0	Send all calls with no other match to any trunks in with the **Outgoing Group** setting of **0**. Since **0** is not a valid value, this needs to be changed to match the Outgoing Group setting actually used for the external trunks hosted by the Primary Server.
Secondary Server	?/Dial/./50:Main	?/Dial/./99999	Send all calls with no other match to the Primary Server.
Expansion	?/Dial/./50:Main	?/Dial/./99999 ?/Dial/./99998	Send all calls with no other match to the Primary Server if available, else to the Secondary Server.

U-Law	System Short Code	ARS 50:Main Short Codes	Description
Primary Server	9N/Dial/N/50:Main	?/Dial/./0	Send all calls with no other match to any trunks in with the **Outgoing Group** setting of **0**. Since **0** is not a valid value, this needs to be changed to match the **Outgoing Group** setting actually used for the external trunks hosted by the Primary Server.
Secondary Server	?/Dial/./50:Main	?/Dial/./99999	Send all calls with no other match to the Primary Server.
Expansion	?/Dial/./50:Main	?/Dial/./99999 ?/Dial/./99998	Send all calls with no other match to the

Table continues…

U-Law	System Short Code	ARS 50:Main Short Codes	Description
			Primary Server if available, else to the Secondary Server.

The short method for describing short codes in this manual, for example **9N/Dial/./0**, indicates the settings of the following fields of a short code: **Code/Feature/Telephone Number/Line Group ID**. For a description of the individual fields see Short Code.

The different destinations used for the dialing short codes in the **Line Group ID** field are:

- **50:Main** Route the call to the ARS record 50:Main on the system where the short code match has occurred. If additional ARS records are created on a system they can also be selected as the destination for calls to be routed.
- **99999** Route the call to the Primary Server.
- **99998** Route the call to the Secondary Server.
- **999901 to 999930** Route the call to one of the expansion systems. These destinations can only be used on short codes on the Primary Server and Secondary Server.
- **0** Seize a trunk from those trunks on the system that have their Outgoing Group setting set to 0. Since **0** is not a valid value, this needs to be changed to match the **Outgoing Group** setting actually used for the external trunks hosted by the Primary Server.

Examples

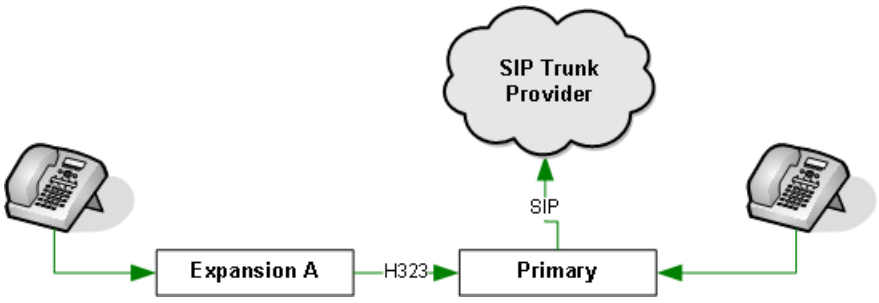
The following are a number of examples that summarize the configuration changes necessary for outgoing call routing. These are simple examples and cannot cover all possible scenarios. There are additional examples of how the settings in the ARS forms can be used in the ARS section of this document.

Related Links

Outgoing Call Routing on page 102

Example 1: Using SIP Trunks Hosted by the Primary

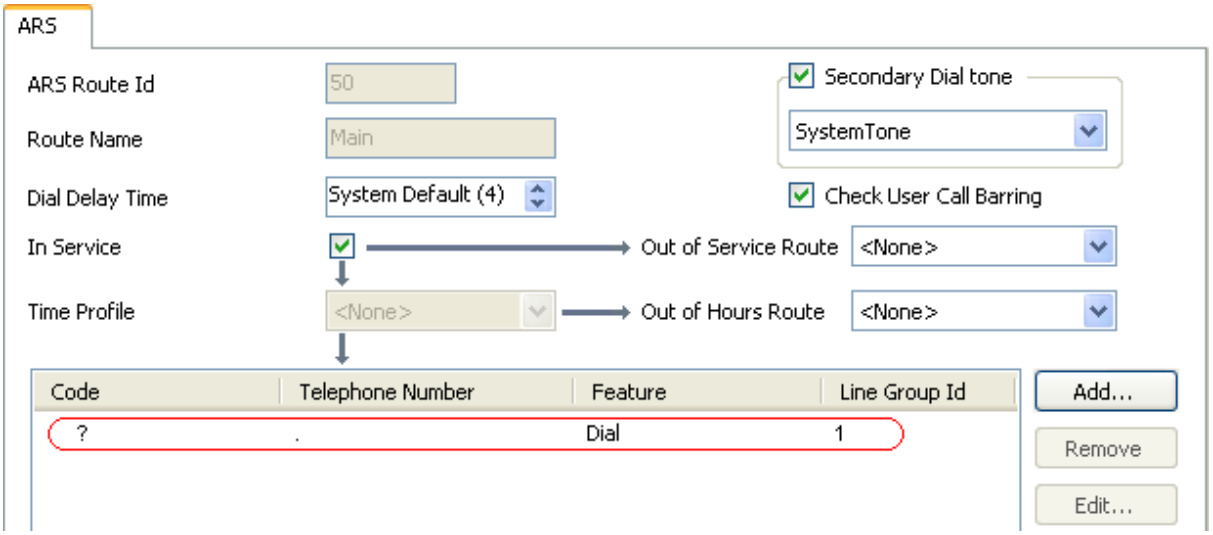
This is the simplest example. It assumes that a SIP trunk has been added to the configuration of the Primary Server, along with the necessary licenses.



In the Primary Server configuration:

1. In the configuration of the SIP trunk on the Primary Server, the SIP URI form includes a field for setting the **Outgoing Group**. Set this to a unique ID, by default it is set to **1**.

2. In the ARS record **50:Main** on the Primary Server, select and edit the exist **?** short code to change it from **Line Group ID** of **0** to a **Line Group ID** of **1**.



- **Code**: **?** The **?** short code character matches any digits for which no other short code match is present in this ARS form.
- **Feature**: **Dial**
- **Telephone Number**: **.** The **.** short code character matches all the digits dialled, not just those that matched the **Code** field.
- **Line Group ID**: **1** (or whichever number was set for the SIP trunk **Outgoing Group** on the Primary Server) This field is used to match outgoing calls (ie. calls using the Dial feature) to an available trunk on the system with the matching number as its **Outgoing Group** setting. Multiple trunks on the same system can have the same **Outgoing Group** setting.

3. Save the configuration.

Results: A-Law Systems

For systems operating in A-Law, it is assumed that no dialing prefix is used for external calls.

If a user hosted on an expansion system dials 555 123 4567:

Server	Event	Digits
Expansion System	A user dials 555 123 4567.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to the primary.	555 123 4567

Table continues…

Server	Event	Digits
Primary Server	The call is received on the H.323 line.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to an available SIP trunk channel.	555 123 4567

If a user hosted on the primary system dials 555 123 4567:

Server	Event	Digits
Primary Server	A user dials 555 123 4567.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to an available SIP trunk channel.	555 123 4567

Results: U-Law Systems

For systems operating in U-Law, it is assumed that a 9 prefix is used for external calls.

If a user hosted on an expansion system dials 9 555 123 4567:

Server	Event	Digits
Expansion System	A user dials 9 555 123 4567.	9 555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	9 555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to the primary.	9 555 123 4567
Primary Server	The call is received on the H.323 line.	9 555 123 4567
	The digits are matched to the **9N/Dial/N** system short code. This routes the call to ARS **50:Main**. having removed the 9 prefix.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to an available SIP trunk channel.	555 123 4567

If a user hosted on the primary system dials 9 555 123 4567:

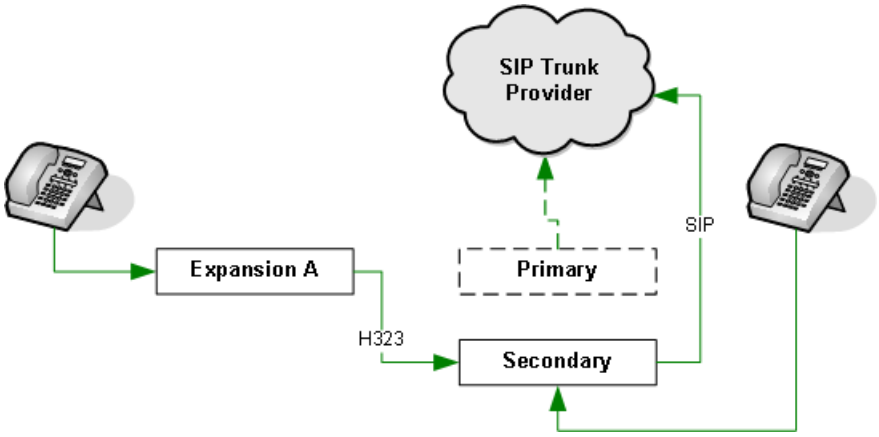
Server	Event	Digits
Primary Server	A user dials 9 555 123 4567.	9 555 123 4567
	The digits are matched to the **9N/ Dial/N** system short code. This routes the call to ARS **50:Main**. having removed the 9 prefix.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to an available SIP trunk channel.	555 123 4567

Related Links

Outgoing Call Routing on page 102

Example 2: Primary Trunk Fallback to Secondary Trunks

This example is builds on the previous example. In this case the network has also has a Secondary Server and SIP trunks have been added to the Secondary Servers configuration using the **Outgoing Group** setting of **2**.



In the Primary Server configuration:

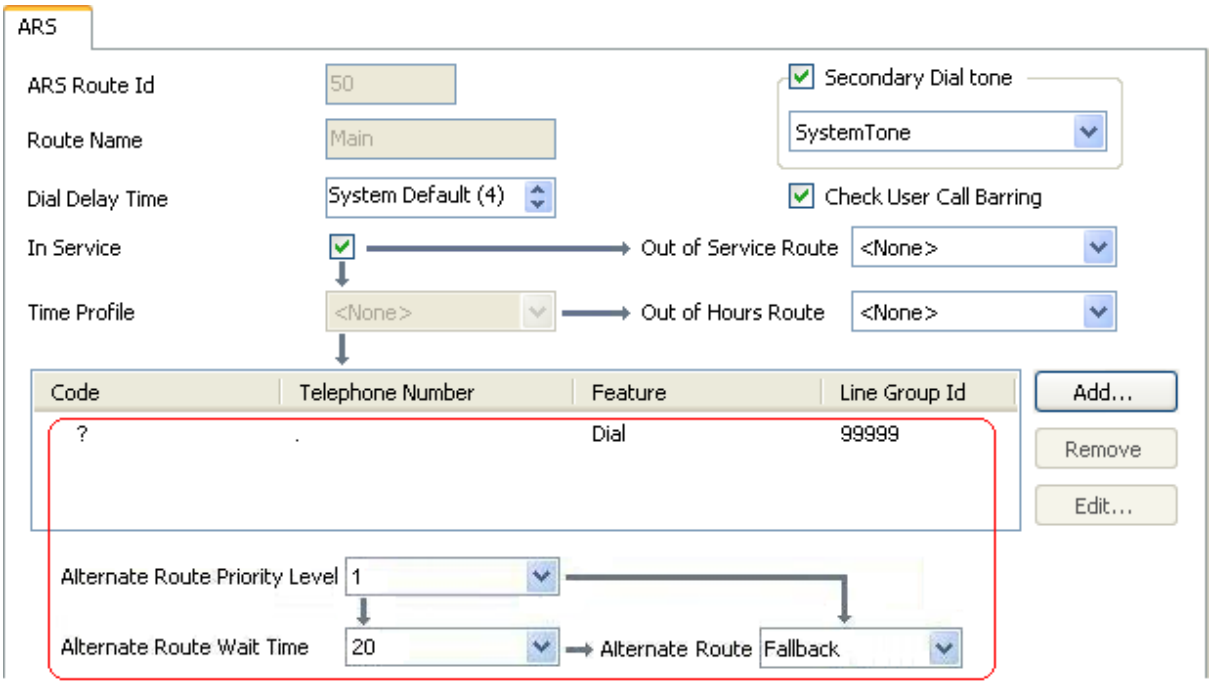
Configure the Primary Server as per example 1. This will route all outgoing calls to the SIP trunk hosted by the Primary Server.

In the Secondary Server configuration:

1. In the configuration of the SIP trunk on the Secondary Server, the SIP URI form includes a field for setting the **Outgoing Group**. Set this to a unique ID, for this example we assume it is **2**.
2. Select ARS and click on the icon to add a new ARS record.
3. Set the **Route Name** to something suitable descriptive such as **Fallback**.

4. Add a short code that will route calls that use this ARS record to the SIP trunk hosted by the secondary. The short code depends on whether we need to remove a dial 9 prefix or not:
   - If no dialing prefix is being used, add a **?/Dial/./2** short code.
   - If a dial 9 prefix is being used, add a **9N/Dial/N/2** short code.
5. Click **OK**.

   In the ARS record **50:Main** on the Secondary Server, we need to set the record to fallback to using the new ARS form when a route to the primary cannot be seized.



6. In the **Alternate Route** drop down select the fallback ARS.
7. Set the **Alternate Route Priority Level** to **1**. This is the lowest level of priority so no users will need to wait to use the alternate ARS is the connection to the primary is not available.
8. Save the configurations.

Results: A-Law Systems

For systems operating in A-Law, it is assumed that no dialing prefix is used for external calls.

If a user hosted on an expansion system dials 555 123 4567:

Server	Event	Digits
Expansion System	A user dials 555 123 4567.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567

Table continues…

Server	Event	Digits
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This tries to route the call to the primary (**99999**).	555 123 4567
	A trunk to the primary cannot be seized. The digits are matched to the next **?/Dial/.** short code in the ARS form. This routes the call to the secondary (**99998**).	555 123 4567
Secondary Server	The call is received on the H.323 line.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567
	The ARS cannot seize a trunk to the primary so fallback to its alternate ARS, **51:Fallback**.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to an available SIP trunk channel.	555 123 4567

If a user hosted on the secondary system dials 555 123 4567:

Server	Event	Digits
Secondary Server	A user dials 555 123 4567.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567
	The ARS cannot seize a trunk to the primary so fallback to its alternate ARS, **51:Fallback**.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to an available SIP trunk channel.	555 123 4567

Results: U-Law Systems

For systems operating in U-Law, it is assumed that a 9 prefix is used for external calls.

If a user hosted on an expansion system dials 555 123 4567:

Server	Event	Digits
Expansion System	A user dials 555 123 4567.	9 555 123 4567

Table continues…

Server	Event	Digits
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	9 555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This tries to route the call to the primary (**99999**).	9 555 123 4567
	A trunk to the primary cannot be seized. The digits are matched to the next **?/Dial/.** short code in the ARS form. This routes the call to the secondary (**99998**).	9 555 123 4567
Secondary Server	The call is received on the H.323 line.	9 555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	9 555 123 4567
	The ARS cannot seize a trunk to the primary so fallback to its alternate ARS, **51:Fallback**.	9 555 123 4567
	The digits are matched to the first **9N/Dial/N** short code in the ARS form. This routes the call to an available SIP trunk channel having removed the 9 prefix.	555 123 4567

If a user hosted on the secondary system dials 555 123 4567:

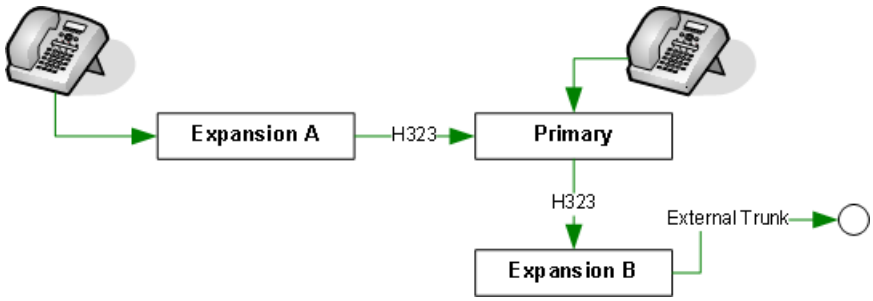
Server	Event	Digits
Secondary Server	A user dials 555 123 4567.	9 555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	9 555 123 4567
	The ARS cannot seize a trunk to the primary so fallback to its alternate ARS, **51:Fallback**.	9 555 123 4567
	The digits are matched to the first **9N/Dial/N** short code in the ARS form. This routes the call to an available SIP trunk channel having removed the 9 prefix.	555 123 4567

Related Links

Outgoing Call Routing on page 102

Example 3: Using Trunks on an Expansion System (V2)

Primary Server, Secondary Server and Linux Expansion systems only support SIP trunks for external trunk connections. An Expansion System (V2) must be used for other trunk types such as analog, BRI or PRI. In this example we assume that the Expansion System (V2) is being used for all outgoing external calls from the network.



1. In the Expansion A configuration: No changes are required, this and other expansion systems still send their calls to the primary which then routes the calls to the system which is hosting the external trunks.
2. In the configuration of the Primary Server, identify the H.323 IP trunk that is used for calls to the Expansion System (V2) and note the **Outgoing Group ID** setting, it will be in the range **99901** to **999930**. The trunk can be recognized by the **Gateway IP Address** on the VoIP Settings tab matching the IP address of the Expansion System (V2).
3. In the ARS record **50:Main** on the Primary Server, select and edit the default ? short code to route calls to the expansion system:
   - **Code**: **?**
   - **Feature**: **Dial**
   - **Telephone Number**: **.**
   - **Line Group ID**: **99901** (or whichever number was set for the **Outgoing Group ID** to the Expansion System (V2)).
4. In the configuration of the system hosting the external trunk:
   a. Set the **Outgoing Group ID** of the external trunks to a unique value. For this example we assume **3** is used. The field where this is set depends on the trunk type but always has the same name.
   b. [Optional] If the network expects a dial 9 prefix on external calls, we need to add a new system short code that matches and removes that prefix from calls dialed on the local system as for call made on other systems this prefix is removed by the primary. Add a system short code similar to the following:
      - **Code**: **9N**
      - **Feature**: **Dial**
      - **Telephone Number**: **N**
      - **Line Group ID**: **50:Main**

5. In the ARS record **50:Main**, select and edit the first default **?** short code to use the **Line Group ID** of **3**.
   - **Code**: **?**
   - **Feature**: **Dial**
   - **Telephone Number**: **.**
   - **Line Group ID**: **3** (or whichever number was set for the **Outgoing Group ID** on the system's external trunks).
6. Save the configuration.

Results: A-Law

For systems operating in A-Law, it is assumed that no dialing prefix is used for external calls.

If a user hosted on other expansion systems dials 555 123 4567:

Server	Event	Digits
Expansion System A	A user dials 555 123 4567.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to the primary.	555 123 4567
Primary Server	The call is received on the H.323 line.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to expansion system B.	555 123 4567
Expansion System B	The call is received on the H.323 line.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to an available trunk.	555 123 4567

If a user hosted on the primary server dials 555 123 4567:

Server	Event	Digits
Primary Server	A user dials 555 123 4567.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to expansion system B.	555 123 4567
Expansion System B	The call is received on the H.323 line.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to an available trunk.	555 123 4567

If a user hosted on expansion system B dial 555 123 4567:

Server	Event	Digits
Expansion System B	A user dials 555 123 4567.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to an available trunk.	555 123 4567

Results: U-Law

For systems operating in U-Law, it is assumed that a 9 prefix is used for external calls.

If a user hosted on other expansion systems dials 9 555 123 4567:

Server	Event	Digits
Expansion System A	A user dials 9 555 123 4567.	9 555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	9 555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to the primary.	9 555 123 4567

Table continues…

Server	Event	Digits
Primary Server	The call is received on the H.323 line.	9 555 123 4567
	The digits are matched to the **9N/Dial/N** system short code. This routes the call to ARS **50:Main**. having removed the 9 prefix.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to expansion system B.	555 123 4567
Expansion System B	The call is received on the H.323 line.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to an available trunk.	555 123 4567

If a user hosted on the primary server dials 9 555 123 4567:

Server	Event	Digits
Primary Server	A user dials 9 555 123 4567.	9 555 123 4567
	The digits are matched to the **9N/Dial/N** system short code. This routes the call to ARS **50:Main**. having removed the 9 prefix.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to expansion system B.	555 123 4567
Expansion System B	The call is received on the H.323 line.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to an available trunk.	555 123 4567

If a user hosted on expansion system B dial 9 555 123 4567:

Server	Event	Digits
Expansion System B	A user dials 9 555 123 4567.	9 555 123 4567
	The digits are matched to the **9N/ Dial/N** system short code. This routes the call to ARS **50:Main**. having removed the 9 prefix.	9 555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to an available trunk.	9 555 123 4567

Related Links

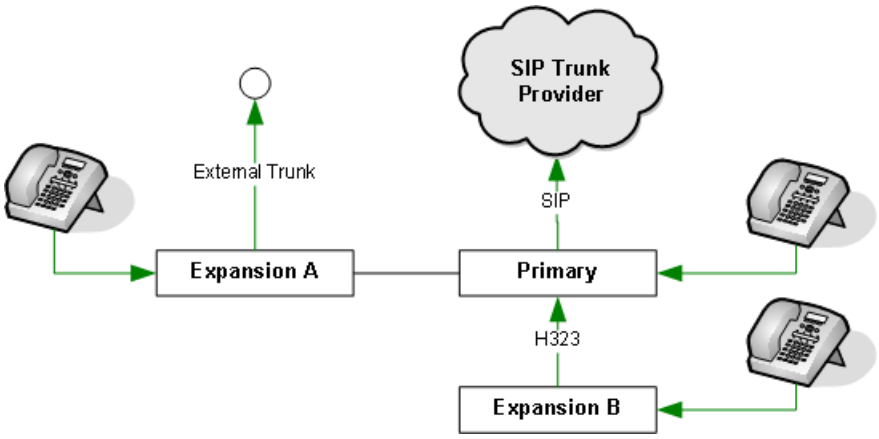
Outgoing Call Routing on page 102

Example 4: Local Branch Override

This example builds on Example 1 where all external calls are routed to SIP trunks hosted by the primary server.

There may be cases where an expansion system (Expansion System (L) and Expansion System (V2)) can route calls through its own local trunks more cheaply than through trunks located on another system such as the primary. For example, if the site where the expansion system is located can make local calls free of charge or at a much lower cost. If that is the case, then for certain dialing we would want to have those calls use the local trunk rather than following the default routing to the primary server.

Suppose for this example, expansion system A is in national area code 444. The customer wants any dialing of numbers prefixed with 444 by the users hosted on that system to be routed out on the external trunks connected to that expansion system. All other external dialing should continue to follow the defaults of being routed to the primary.



1. In the configuration of the expansion system, set the **Outgoing Group ID** of the external trunks to a unique value. For this example we assume **4** is used. The field where this is set depends on the trunk type but always has the same name.

2. In the ARS record **50:Main** on the expansion system we need to add a new short code that matches and routes calls that include the 444 area code. The short code required depend on whether an external dialing prefix is used or not.

   Add a new short code:

   - **Code**: **444N** (A-Law) or **9444N** (U-Law)
   - **Feature**: **Dial**
   - **Telephone Number**: **N**
   - **Line Group ID**: **4** (or whichever number was set for the **Outgoing Group ID** on the system's external trunks).

   The new code will match any dialing sent to the ARS prefixed with 444. Depending on local dialing patterns it may also be necessary to add similar codes to match dialing prefixed with a national prefix before the local area code. For example short codes for dialing prefixed **1444N** or dialing of a particular length that would imply its a local number, eg. **XXXXXXX**.

3. Save the configuration.

Results: A-Law Systems

For systems operating in A-Law, it is assumed that no dialing prefix is used for external calls.

If a user hosted on expansion system A dials 555 123 4567:

This routing matches the example setup in Example 1 where the main trunks and call routing settings for external calls by any system are configured on the primary server.

Server	Event	Digits
Expansion System A	A user dials 555 123 4567.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to the primary.	555 123 4567
Primary Server	The call is received on the H.323 line.	555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to an available SIP trunk channel.	555 123 4567

If a user hosted on expansion system A dials 444 123 4567:

Server	Event	Digits
Expansion System A	A user dials 444 123 4567.	444 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	444 123 4567
	The digits are matched to the first **444N/Dial/N** short code in the ARS form. This routes the call to the external trunk on the system.	444 123 4567

Results: U-Law

For systems operating in U-Law, it is assumed that a 9 prefix is used for external calls.

If a user hosted on expansion system A dials 9 555 123 4567:

This routing matches the example setup in Example 1 where the main trunks and call routing settings for external calls by any system are configured on the primary server.

Server	Event	Digits
Expansion System A	A user dials 9 555 123 4567.	9 555 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	9 555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to the primary.	9 555 123 4567
Primary Server	The call is received on the H.323 line.	9 555 123 4567
	The digits are matched to the **9N/Dial/N** system short code. This routes the call to ARS **50:Main**. having removed the 9 prefix.	555 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to an available SIP trunk channel.	555 123 4567

If a user hosted on expansion system A dials 9 444 123 4567:

Server	Event	Digits
Expansion System A	A user dials 9 444 123 4567.	9 444 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	9 444 123 4567

Table continues…

Server	Event	Digits
	The digits are matched to the first **9444N/Dial/N** short code in the ARS form. This routes the call to the external trunk on the system.	444 123 4567

Related Links

Outgoing Call Routing on page 102

Example 5: PSTN Tail-End-Hop-Off

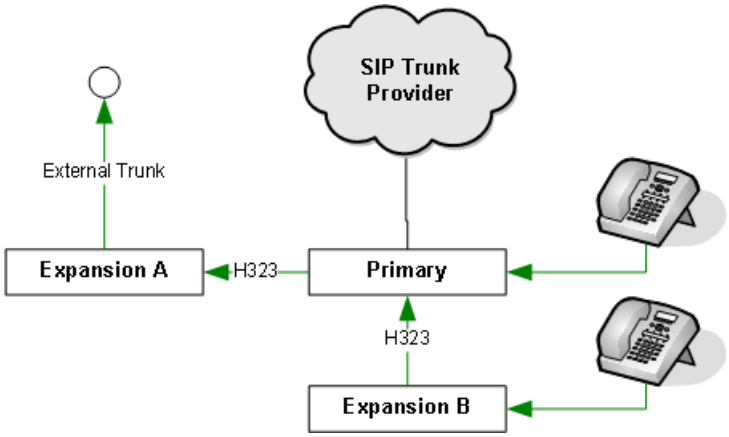
This example builds on Example 4 where calls local to a particular expansion system are routed to external trunks hosted by that expansion system. Having setup routing similar to that example, it may be advantageous to route any dialing of the same are code on other systems in the network to the trunks on the local expansion system.

Suppose for this example, we want users on any system in the network that dial a call prefixed with national area code 444 to have that call routed to external trunks on expansion system A which is in that local area. We can do this by adding additional short codes to the ARS on the primary system as the default routing on all systems already sends all calls to the primary.

Important:

Check Local and National Call Routing Regulations

This type of operation may be subject to nation restrictions, especially where the expansion system trunks are being used to make calls in a different country code to other systems in the network. Such operation is not allowed by the telecommunications regulations in some countries.



1. In the configuration of the Primary Server, identify the H.323 IP trunk that is used for calls to the expansion system and note the **Outgoing Group ID** setting, it will be in the range **99901** to **999930**. The trunk can be recognized by the **Gateway IP Address** on the VoIP Settings tab matching the IP address of the expansion system.
2. In the ARS record **50:Main** on the primary server:

Add a new short code:

- **Code**: **444N** (A-Law) or **9444N** (U-Law)
- **Feature**: **Dial**
- **Telephone Number**: **.**
- **Line Group ID**: **99901** (or whichever number was set for the **Outgoing Group ID** to the expansion system).

The new code will match any dialing sent to the ARS prefixed with 444. Again, as in Example 4, it may also be necessary to add similar codes to match dialing prefixed with a national prefix before the local area code. For example short codes for dialing prefixed **1444N** or dialing of a particular length that would imply its a local number, eg. **XXXXXXX**.

3. In the expansion system configuration, apply the same short codes as used for Example 4 to route dialing to area code 444 dialed by users on that system. Those short codes are also applied to calls received on the network trunks that arrive with those digits.
4. Save the configuration.

Results: A-Law Systems

Any dialing prefixed with 444 on any system is routed to the primary server from where it is rerouted to the expansion system hosting trunks local to that area code.

If a user hosted on expansion system A dials 444 123 4567:

Server	Event	Digits
Expansion System A	A user dials 444 123 4567.	444 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	444 123 4567
	The digits are matched to the first **444N/Dial/N** short code in the ARS form. This routes the call to the external trunk on the system.	444 123 4567

If a user hosted on the primary server dials 444 123 4567:

Server	Event	Digits
Primary Server	A user dials 444 123 4567.	444 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	444 123 4567
	The digits are matched to the first **444N/Dial/**. short code in the ARS form. This routes the call to expansion system A.	444 123 4567

Table continues…

Server	Event	Digits
Expansion System A	The call is received on the H.323 line.	444 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	444 123 4567
	The digits are matched to the first **444N/Dial/N** short code in the ARS form. This routes the call to the external trunk on the system.	123 4567

If a user hosted on other expansion systems dials 444 123 4567:

Server	Event	Digits
Expansion System B	A user dials 444 123 4567.	444 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	444 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to the primary.	444 123 4567
Primary Server	The call is received on the H.323 line.	444 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	444 123 4567
	The digits are matched to the first **444N/Dial/**. short code in the ARS form. This routes the call to expansion system A.	444 123 4567
Expansion System A	The call is received on the H.323 line.	444 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	444 123 4567
	The digits are matched to the first **444N/Dial/N** short code in the ARS form. This routes the call to the external trunk on the system.	123 4567

Results: U-Law Systems

Any dialing prefixed with 9444 on any system is routed to the primary server from where it is rerouted to the expansion system hosting trunks local to that area code.

If a user hosted on expansion system A dials 9 444 123 4567:

Server	Event	Digits
Expansion System A	A user dials 9 444 123 4567.	9 444 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	9 444 123 4567
	The digits are matched to the first **9444N/Dial/N** short code in the ARS form. This routes the call to the external trunk on the system.	123 4567

If a user hosted on the primary server dials 9 444 123 4567:

Server	Event	Digits
Primary Server	A user dials 9 444 123 4567.	9 444 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	9 444 123 4567
	The digits are matched to the first **9444N/Dial/**. short code in the ARS form. This routes the call to expansion system A.	9 444 123 4567
Expansion System A	The call is received on the H.323 line.	9 444 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	9 444 123 4567
	The digits are matched to the first **9444N/Dial/N** short code in the ARS form. This routes the call to the external trunk on the system.	123 4567

If a user hosted on other expansion systems dials 9 444 123 4567:

Server	Event	Digits
Expansion System B	A user dials 9 444 123 4567.	9 444 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	9 444 123 4567
	The digits are matched to the first **?/Dial/**. short code in the ARS form. This routes the call to the primary.	9 444 123 4567
Primary Server	The call is received on the H.323 line.	9 444 123 4567

Table continues…

Server	Event	Digits
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	9 444 123 4567
	The digits are matched to the first **9444N/Dial/**. short code in the ARS form. This routes the call to expansion system A.	9 444 123 4567
Expansion System B	The call is received on the H.323 line.	9 444 123 4567
	The digits are matched to the **?/Dial/**. system short code. This routes the call to ARS **50:Main**.	9 444 123 4567
	The digits are matched to the first **9444N/Dial/N** short code in the ARS form. This routes the call to the external trunk on the system.	123 4567

Related Links

Outgoing Call Routing on page 102

Telephone Features Supported Across Server Edition and SCN Networks

Each system running IP Office in a multi-site network acts as a self-contained IP Office telephone system. In addition to the remote systems sharing knowledge of user and hunt group extension numbers, the following additional telephony features are supported between systems in a multi-site network. Features not listed are not supported across the multi-site network.

Absence Text

Advertised Hunt Groups Hunt groups set to advertised can be dialed by users on other systems

Anti-tromboning Calls routed across the multi-site network and back to the originating system are turned back into internal calls on the originating system only.

Break Out Dialing

Call Park / Unpark Call

Call Pick-up Extension

Call Tagging

Callback When Free

Centralized Call Log

Centralized Personal Directory

Conference

Distributed Hunt Groups

Distributed Voicemail Server Support When using Vociemail Pro, each system can support its own Voicemail Pro server. See the Voicemail Pro Installation Manual.

Enable ARS / Disable ARS

Extension Dialing Each system automatically learns the user extension numbers available on other systems and routes calls to those numbers.

Fallback Server Edition Fallback SCN Fallback

Fax Relay

Follow Me Here / Follow Me To

Forwarding

Hold Held calls are signalled across the network.

Internal Twining

Intrusion Features

Mobile Call Control Licensed mobile call control users who remote hot desk to another system take their licensed status with them.

Music On Hold Source Selection

Relay On / Relay Off / Relay Pulse

Remote Hot Desking

Set Hunt Group Out of Service / Clear Hunt Group Out of Service

Transfer Calls can be transferred to network extensions.

User DSS/BLF Monitoring of user status only. The ability to use additional features such as call pickup via a USER button will differ depending on whether the monitored user is local or remote. Indication of new voicemail messages provided by SoftConsole user speed dial icon is not supported.

User Profile Resilence When a user hot desks to another system, they retain their Profile settings and rights.

Related Links

Working with the Server Edition Manager User Interface on page 92
Configuring Small Community Networking on page 729

IP500 V2 Conversion

When an IP500 V2 is added to a Server Edition solution as a Expansion System (V2), those parts of its configuration that do not match the default settings for an expansion system are overwritten. Settings are only retained where they don't conflict with those default settings. Beyond that, the range of settings retained depends on:

- Whether the Manager Preferences option **Consolidate Solution to Primary Settings** is selected.
- Whether **Retain Configuration Data** is selected in the **Initial Configuration** menu when the expansion system is added.

Consolidate Solution to Primary		On		Off	
Retain Configuration Data		Off	On **[1]**	Off	On
Lines	**Physical**	Yes	Yes	Yes	Yes
	IP Lines	IP DECT only	Yes	IP DECT only	Yes
Extension	**Physical**	Yes	Yes	Yes	Yes
	IP	Yes	Yes	Yes	Yes
User		–	Yes	–	Yes
Hunt Group		–	–	–	–
Short Code	**Dial, Dial Emergency**	Yes	Yes	Yes	Yes
	Other features	–	Yes	–	Yes
Service		Yes	Yes	Yes	Yes
RAS		Yes	Yes	Yes	Yes
Incoming Call Route		–	Yes	–	Yes
WAN Port		Yes	Yes	Yes	Yes
Directory		–	–	–	–
Time Profile		–	–	–	Yes
Firewall Profile		Yes	Yes	Yes	Yes
IP Route		Yes	Yes	Yes	Yes
Account Code		–	–	–	Yes
Licence		–	Yes	–	Yes
Tunnel		Yes	Yes	Yes	Yes
User Rights		–	–	–	Yes
Auto Attendant		–	–	–	–
ARS		Yes	Yes	Yes	Yes

This action retains more records than are actually visible in Manager due to the action of the **Consolidate Solution to Primary** setting. When the configuration is next loaded, the extra records cause reconsolidation warnings.

Related Links

Working with the Server Edition Manager User Interface on page 92

Chapter 7: Security Administration

The security settings are stored on the system and are separate from the system's configuration settings. To change a system's security settings, Manager must first be switched to security mode by selecting **File | Advanced | Security Settings** from the menu bar.

Security settings can only be loaded directly from a system. These settings cannot be saved as a file on the local PC, nor do they appear as a temporary file at any time. You can optionally secure the link between the system and Manager for configuration and security settings exchanges. By default Manager and the system will always attempt to use the original, unsecured link.

Administration security is achieved using a number of optional cryptographic elements:

- Access control to prevent unauthorized use.
- Encryption to guarantee data remains private.
- Message Authentication ensures data has not been tampered with.
- Identity assures the source of the data.

Related Links

Security Users on page 127
Access Control on page 133
Encryption on page 133
Message Authentication on page 134
Certificates on page 135
Implementing Security on page 140
SRTP on page 142

Security Users

Access to system settings is controlled by **Service Users** and **Rights Groups** stored in the control unit's security settings. These are stored separately from the system's configuration settings. All actions involving communications between Manager and the system require a service user name and password. That service user must be a member of a Rights Group with permissions to perform the required action.

Security Administrators:

By default the security administrator is the only user who can access the system's security settings using Manager's security mode.

Service Users:

Each service user has a name, a password and is a member of one or more Rights Groups.

Rights Groups:

The Rights Groups to which a service user belongs determine what actions they can perform. Actions available to Rights Groups include configuration actions, security actions and system status actions. Where a service user has been configured as a member of more than one Rights Group, they combine the functions available to the separate Rights Groups.

Related Links

Security Administration on page 127
Default Service Users and Rights Groups on page 128

Default Service Users and Rights Groups

Security Administrator Account

The following Security Administrator account is present on first startup and security settings reset.

Name	Default Account Status	Usage	Rights Group Membership	Notes
Security	Enabled, Force password change	This is the default security administration account. Has all rights to all security management and maintenance services	Implied all security rights	Cannot be removed or disabled Should not be renamed

Service User Accounts

The following Service User accounts are present on first start-up and security settings reset.

Name	Default Account Status	Usage	Rights Group Membership	Notes
Administrator	Enabled, Force password change	This is the default account used for system configuration using the IP Office and Web Manager applications, including one-X Portal/Voicemail Pro administration. Has all rights to all management and maintenance services including security settings.	Administrator, System Status, Business Partner	Should not be removed or disabled Should not be renamed

Table continues…

Name	Default Account Status	Usage	Rights Group Membership	Notes
EnhTcpaService	Enabled	This account is used for one-X Portal for IP Office connections to the system.	TCPA Group	Although not enforced, the password should be change as soon as possible in both IP Office and one-X Portal Enable only when one-X Portal deployed
IPDECTService	Disabled	This account is used for DECT R4 system provisioning	IPDECT Group	Enable only when DECT R4 deployed and provisioning mode active
BranchAdmin	Disabled	This account is used for System Manager (SMGR) access in a branch deployment	SMGR Admin	Enable only when SMGR deployed; will be enabled when the Initial Configuration Utility (ICU) run and SMGR administration selected. Must not be renamed
BusinessPartner	Disabled	Similar access rights to Administrator and can be used as a separate account for Business Partners	Business Partner	Should be removed/ disabled unless required
Maintainer	Disabled	Maintenance account without edit configuration or security access. Can be used for Manager (read-only), Web Manager (read-only), System Status Application (SSA), Backup/ Restore, System Monitor, Upgrade	Maintainer	Should be removed/ disabled unless required

Rights Groups

The following Rights Groups are present on first start-up and security settings reset.

Name	Usage	Rights Group User	Notes
Administrator Group	Allows full access to the IP Office Manager application to configure the system. No security or maintenance access	Administrator	All IP Office Manager operations are permitted

Table continues…

Name	Usage	Rights Group User	Notes
Manager Group	Allows limited access to the IP Office Manager application to configure the system.	–	All IP Office Manager operations permitted except: • Delete Short Code • View LAN2 Settings
Operator Group	Allows limited access to the IP Office Manager application to configure the system.	–	All IP Office Manager operations permitted except: • New object creations • View LAN2 Settings • Delete Directory • Delete ICR
System Status Group	Allows limited access to the SSA and Sys Monitor applications.	Administrator	Sys Monitor access right only checked when using service users with Sys Monitor
TCPA Group	This group is used by the one-X Portal for IP Office application.	EnhTcpaService	
IPDECT Group	This group is used by the DECT R4 master base station to extract DECT settings from IP Office.	IPDECTService	
SMGR Admin	This group is used by SMGR to configure IP Office.	BranchAdmin	Do not change the access rights
Security Admin	Allows access to security settings only	–	
Backup Admin	Allows access to all backup and restore services only, including one-X Portal	–	
Upgrade Admin	Allows access to the upgrade service	–	Allows upgrade of both IP Office applications and operating system
System Admin	Allows configuration of IP Office, one-X Portal and Voicemail Pro	–	
Maint Admin	Allows configuration of IP Office, one-X Portal and Voicemail Pro along with backup, restore and upgrade	–	Typically used for maintenance personnel

Table continues…

Name	Usage	Rights Group User	Notes
Business Partner	Full access to all configuration, security and maintenance services.	Administrator, BusinessPartner	
Customer Admin	Web Management , one-X Portal and Voicemail Pro administration	–	No IP Office manager access
Maintainer	Allows configuration view only, along with SSA, Sys Monitor backup, restore and upgrade		Typically used for maintenance personnel with no need for configuration changes

Rights Group Assignment

Service	Access Right	Rights Group						
		• 1 = Administrator Group • 2 = Manager Group • 3 = Operator Group • 4 = System Status Group			• 5 = TCPA Group • 6 = IPDECT Group • 7 = SMGR Admin			
		1	2	3	4	5	6	7
Configuration	Read all configuration	✓	✓	✓				
	Write all configuration	✓	✓	✓				
	Merge configuration	✓	✓	✓				
	Default configuration	✓	✓	✓				
	Reboot/Shutdown immediately	✓	✓	✓				
	Reboot when free	✓	✓	✓				
	Reboot at time of day	✓	✓	✓				
Security Admin	Read all security settings							
	Write all security settings							
	Reset all security settings							
	Write own service user password							
System Status	System Status Access				✓			
	Read all configuration				✓			

Table continues…

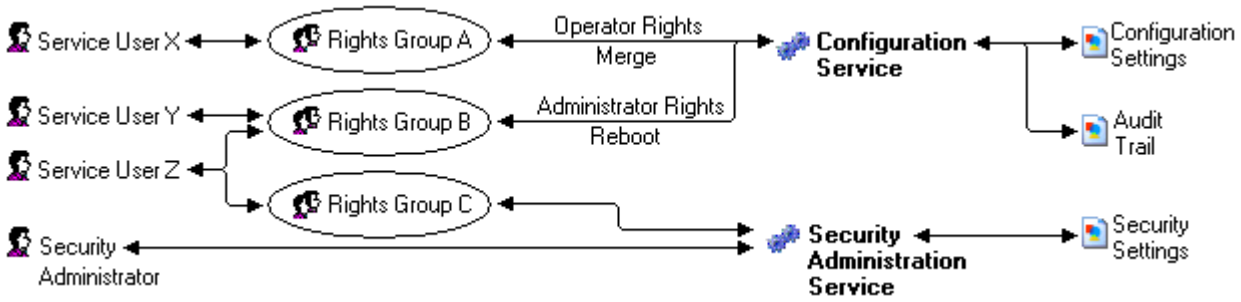
Service	Access Right	Rights Group						
		• 1 = Administrator Group • 2 = Manager Group • 3 = Operator Group • 4 = System Status Group			• 5 = TCPA Group • 6 = IPDECT Group • 7 = SMGR Admin			
		1	2	3	4	5	6	7
	System Control				✓			
	Sys Monitor				✓			
Enhanced TSPI	Enhanced TSPI Access					✓		
HTTP	DECT R4 Provisioning						✓	
Web Services	Security Read All							✓
	Security Write All							✓
	Security Write Own Password							✓
	Config Read All							✓
	Config Write All							✓
	Backup							✓
	Restore							✓
	Upgrade							✓
External	Voicemail Pro Basic							
	Voicemail Pro Standard							
	Voicemail Pro Administrator							✓
	One-X Portal Administrator							
	one-X Portal Super User							
	Web Control Administrator							
	Web Control Security							
	WebRTC Administrator							

Related Links

[Security Users](#) on page 127

Access Control

Access to configuration, security settings and SSA is controlled by the use of service users, passwords and Rights Groups. All actions involving communications between the Manager user and the system require a service user name and password. That service user must be a member of a Rights Group configured to perform the required action.



In the example illustrated above:

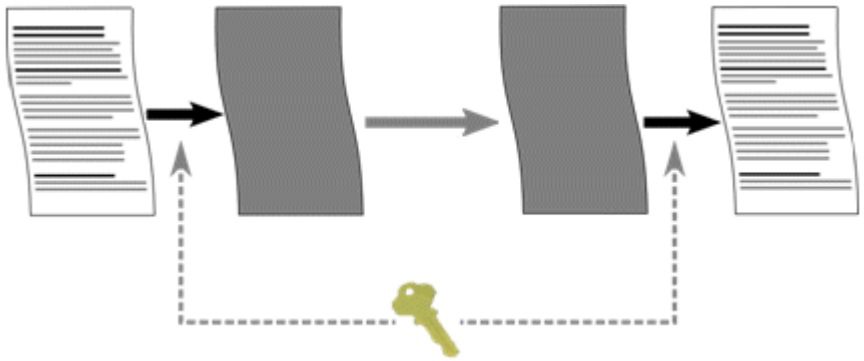
- Service user X can read and write the configuration. However they can only edit Operator settings and can only make changes that can be merged.
- Service user Y can read and write the configuration, edit all settings and make changes that require reboots.
- Service user Z can read and write the configuration, edit all settings and make changes that require reboots. They can also access the security settings.
- The Security Administrator can only access the security settings.

Related Links

Security Administration on page 127

Encryption

Encryption ensures that all data sent by either the system or Manager cannot be ‘read’ by anyone else, even another copy of Manager. Encryption is the application of a complex mathematical process at the originating end, and a reverse process at the receiving end. The process at each end uses the same ‘key’ to encrypt and decrypt the data:



Any data sent may be optionally encrypted using a number of well known and cryptographically secure algorithms:

Algorithm	Effective key size (bits)	Use
DES-40	40	Not supported.
DES-56	56	Not supported.
3DES	112	‘Minimal’ security.
RC4-128	128	‘Acceptable’ security.
AES-128	128	‘Strong’ security.
AES-256	256	‘Strong’ security.

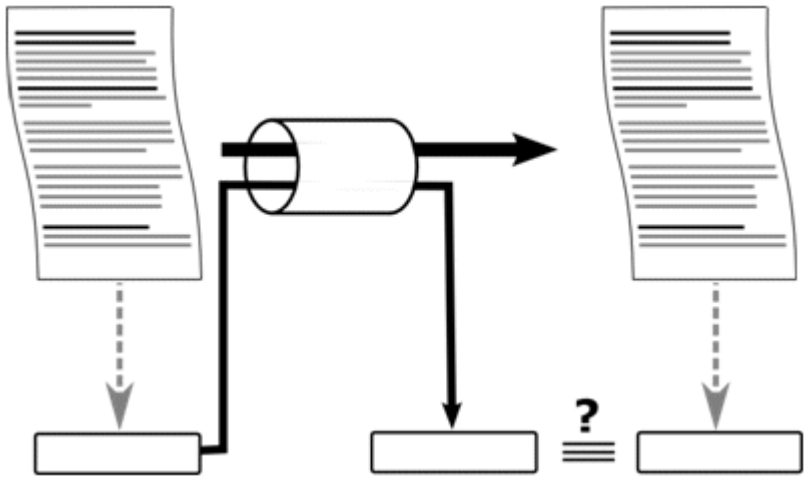
In general the larger the key size, the more secure the encryption. However smaller key sizes usually incur less processing. The system supports encryption using the Transport Layer Security (TLS) v1.0 protocol. In addition, many cryptographic components of the TLS module have been FIPS 140-2 certified, indicating the accuracy of implementation.

Related Links

Security Administration on page 127

Message Authentication

Message authentication ensures that all data sent by either the system or Manager cannot be tempered with (or substituted) by anyone else without detection. This involves the originator of the data producing a signature (termed a hash) of the data sent, and sending that as well. The receiver gets the data and the signature and check both match.



Any data sent may be optionally authenticated using a number of well known and cryptographically secure algorithms:

Algorithm	Effective hash size (bits)	Use
MD5	128	Not recommended.
SHA-1	160	'Acceptable' security.
SHA-2	224, 256, 384, 512	'Strong' security

In general the larger the hash size, the more secure the signature. However smaller hash sizes usually incur less processing.

IP Office supports message authentication using the Transport Layer Security (TLS) 1.0, 1.1, and 1.2 protocol. In addition, many cryptographic components of the TLS module have been FIPS 140-2 certified, indicating the accuracy of implementation.

Related Links

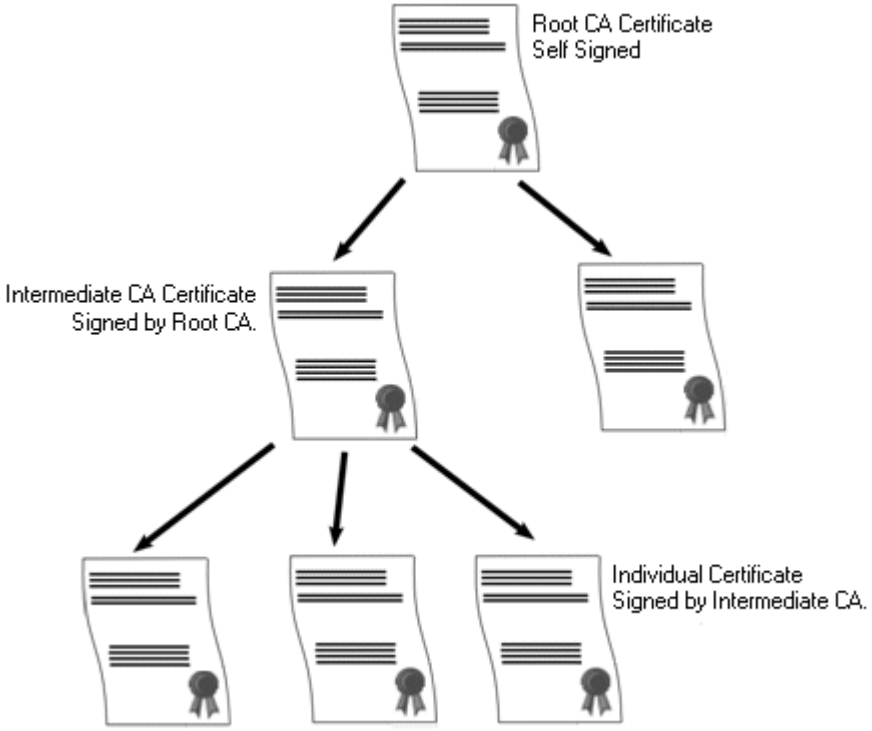
Security Administration on page 127

Certificates

Public key cryptography is one of the ways to maintain a trustworthy networking environment. A public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

The system used to provide public-key encryption and digital signature services is called a public key infrastructure (PKI). All users of a PKI should have a registered identity which is stored in a digital format and called an Identity Certificate. Certificate Authorities are the people, processes and tools that create these digital identities and bind user names to public keys.

There are two types of certificate authorities (CAs), root CAs and intermediate CAs. In order for a certificate to be trusted and for a secure connection to be established, that certificate must have been issued by a CA that is included in the trusted certificate store of the device that is connecting. If the certificate was not issued by a trusted CA, the connecting device then checks to see if the certificate of the issuing CA was issued by a trusted CA, and so on until either a trusted CA is found. The trusted certificate store of each device in the PKI must contain the required certificate chains for validation.



IP Office Root Certificate Authority

IP Office generates a self-signed certificate. For IP500 V2 systems, a certificate is generated automatically on the first start up. On Linux systems, a certificate is generated during the ignition process.

The following entities can act as the certificate authority.

- The Server Edition Primary Server, an Application Server, or a Unified Communication Module (UCM) can act as the root certificate authority for all nodes in the system.
- In Enterprise Branch deployments, the System Manager can act as the root certificate authority.
- Identity certificates can also be purchased and issued by a third party certificate authority.

Regardless of the method used to provide the IP Office identity, the certificate authority which signs the IP Office identity certificate must be trusted by all the clients and endpoints that need to establish a secure connection with IP Office. They must be a part of the PKI. Therefore, the root CA certificate must be downloaded to client devices and placed in the trusted certificate store. If there are intermediate CAs in the certificate chain, either the intermediate CAs must be added to the client device Trusted Certificate Store or the certificate chain must be advertised by IP Office in the initial TLS exchange.

Certificates and TLS

Telephony signaling like SIP messaging is secured using Transport Layer Security (TLS). TLS provides communication security using certificates to authenticate the other end of the IP Link.

The message exchange in TLS is aimed at verifying the identity of the communicating parties and establishing the keys that will be used to encrypt the signaling data between the two parties. Typically, the server sends its identity certificate, either self-signed or signed by the CA, to the client. The client must have the CA certificate in its trusted certificate store.

IP Office acts as the TLS server in its interactions with SIP telephony clients. This means that the TLS application on the IP Office must be configured to listen for client connections by enabling TLS in the SIP Registrar on the LAN1 and LAN2 interfaces.

Windows Certificate Store

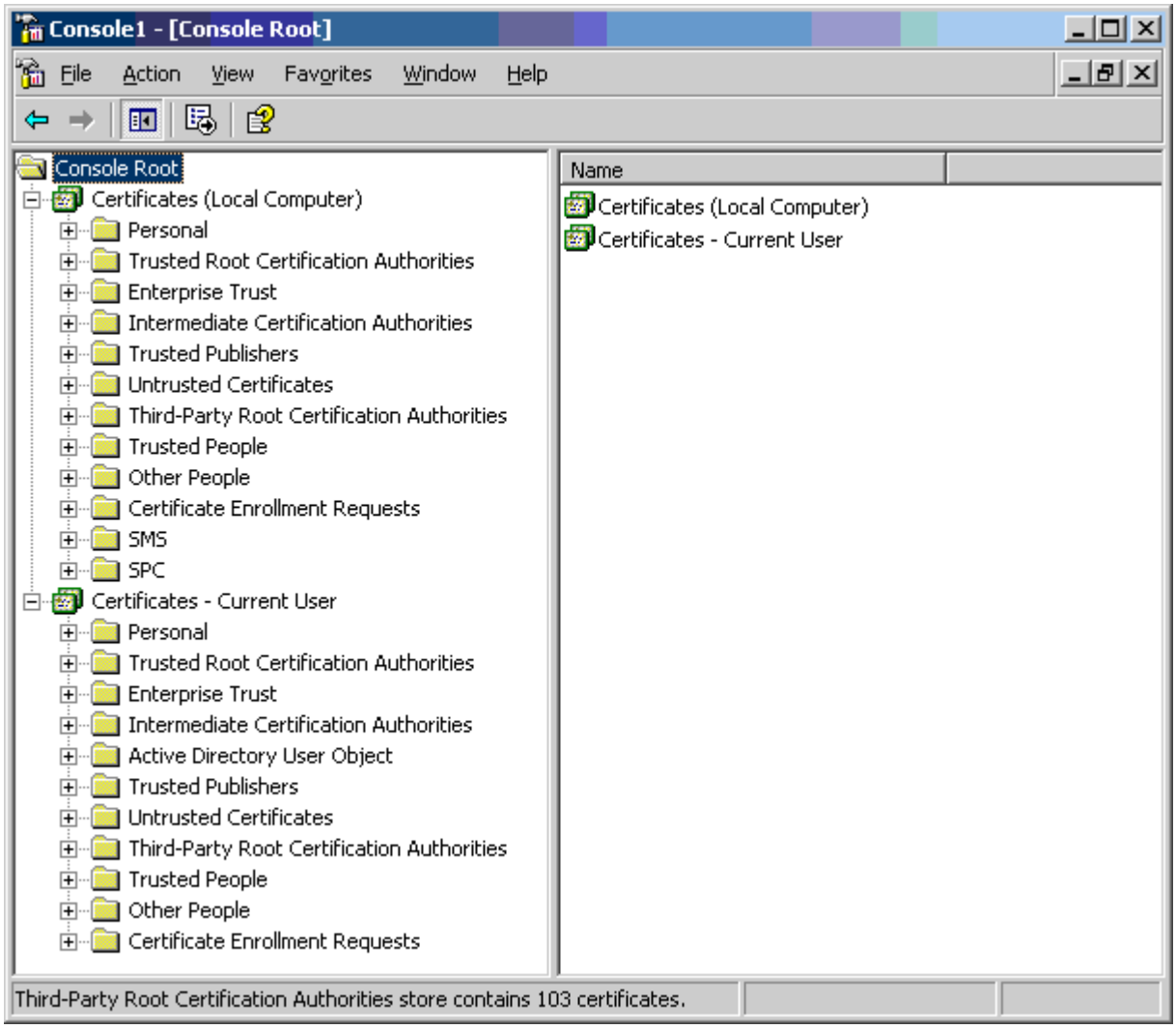
The certificate store used by Manager to save and retrieve X509 certificates is the default one provided by the Windows operating system. The Windows certificate store is relevant to any application running on Windows that uses certificates for security, either TLS or HTTPS. For example, the Avaya Communicator Client.

Warning:

Avaya accepts no responsibility for changes made by users to the Windows operating system. Users are responsible for ensuring that they have read all relevant documentation and are sufficiently trained for the task being performed.

Windows Certificate Store Organization

By default, certificates are stored in the following structure:



Each of the sub folders has differing usage. The Certificates - Current User area changes with the currently logged-in windows user. The Certificate (Local Computer) area does not change with the currently logged-in windows user.

Manager only accesses some of the certificate sub folder:

Certificates (Local Computer) Folder	Manager Use
Personal | Certificates	Folder searched by Manager 1st for matching certificate to send to the system when requested. Certificate matched by the subject name contained in **File | Preferences | Security | Certificate** offered to the system. Folder accessed whenever **'Local Machine certificate store'** used for Security Settings.

Table continues…

Certificates (Local Computer) Folder	Manager Use
	Folder searched by Manager for matching certificate when certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.
Trusted Root Certification Authorities | Certificates	Folder searched by Manager for matching parent certificates when non-self signed certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.

Certificates – Current User Folder	Manager Use
Personal | Certificates	Folder searched by Manager 2nd for matching certificate (subject name) to send to the system when requested. Certificate matched by the subject name contained in **File | Preferences | Security | Certificate** offered to the system. Folder accessed whenever **'Current User certificate store'** used for Security Settings. Folder searched by Manager for matching certificate when certificate received from IP Office, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.
Trusted Root Certification Authorities | Certificates	Folder searched by Manager for matching parent certificates when non-self signed certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.
Other People | Certificates	Folder searched by Manager for matching parent certificates when non-self signed certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.

Windows Certificate Store Import

In order to use certificates – either for security settings or Manager operation – they must be present in the windows certificate store. Certificates may be placed in the store by the Certificate Import Wizard. The Certificate Import Wizard can be used whenever a certificate is viewed. In order for Manager to subsequently access this certificate the **Place all certificate in the following store** option must be selected:

- If the certificate is to subsequently identify the system, the Other People folder should be used.
- If the certificate is to subsequently identify the Manager, the Personal folder should be used, and the associated private key saved as well.

Certificate Store Export

Any certificate required outside of the Manager PC must be first saved in the Certificate store, then exported.

If the certificate is to be used for identity checking (i.e. to check the far entity of a link) the certificate alone is sufficient, and should be saved in PEM or DER format.

If the certificate is to be used for identification (i.e. to identify the near end of a link) the certificate and private key is required, and should be saved in PKCS#12 format, along with a password to access the resultant .pfx file.

Related Links

Security Administration on page 127

Implementing Security

IP Office can be made a very secure. However, only a certain number of features are active by default in order to ease the initial installation. If all Manager and system security settings are left at default, no security mechanisms are active, other than the use of default service user names and passwords. In addition, all legacy interfaces are active, and all configuration and security data is sent unencrypted. Therefore, it is necessary to implement the configuration options listed here. Additional setting may be necessary to further secure the individual deployment. Avaya is presenting this information for guidance only; the customer is responsible for ensuring their system is secure.

To improve IP Office security in practice, two main mechanisms are used:

- Activation of IP Office security features.
- Reduction of exposure to external or internal attack.

Minimum Security

A minimum security scenario could be where configuration data is open, but the security settings are constrained: Any individual with the correct service user name and password can access the configuration from any PC installation of Manager, no logging of access: Passwords can be simple, and will never age.

- Change all default passwords of all service users and Security Administrator.
- Set the system Security Administration service security level to Secure, Low.
- Set the system service user Password Reject Action to None.
- Set the system Client Certificate Checks level to None (default).
- Set the system Minimum Password Complexity to Low (default).
- Set the system Previous Password Limit to zero (default).
- Set the system Password Change Period to zero (default).
- Set the system Account Idle Time to zero (default).
- Set certificate check level to low in Manager Security Preferences (default).

In addition, any PC installation of Manager can manage any IP Office.

Medium Security

A medium security scenario could be where both configuration and security settings are constrained and a level of logging is required: Any individual with the correct service user name and password

can access the configuration from any PC installation of Manager: Passwords cannot be simple, and will age.

- Change all default passwords of all service users and Security Administrator
- Set the system Security Administration service security level to Secure, Medium.
- Set the system Configuration service security level to Secure, Medium.
- Set the system service user Password Reject Action to Log to Audit Trail (default).
- Set the system Client Certificate Checks level to None (default).
- Set the system Minimum Password Complexity to Medium.
- Set the system Previous Password Limit to non zero.
- Set the system Password Change Period to non zero.
- Set the system Account Idle Time to zero (default).
- Disable all the system Unsecured Interfaces.
- Set certificate check level to low in Manager Security Preferences (default).

Maximum Security

A maximum security scenario could be where both configuration and security settings are constrained and a full level of logging is required: Certified individuals with the correct service user name and password can access the configuration from specific PC installations of Manager: Passwords cannot be simple, and will age: Manager can managed specific systems.

- Change all default passwords of all service users and Security Administrator
- Set the system Security Administration service security level to Secure, High.
- Set the system Configuration service security level to Secure, High.
- Set the system service user Password Reject Action to Log and Disable Account.
- Set the system Client Certificate Checks level to High.
- Set the system Minimum Password Complexity to High.
- Set the system Minimum Password Length to >8.
- Set the system Previous Password Limit to non zero (>5).
- Set the system Password Change Period to non zero.
- Set the system Account Idle Time to non zero.
- Set the system Session ID Cache to zero.
- Install valid, 1024 bits+, non self signed certificates (+private key) in all IP Office server certificates, derived from a trusted certificate authority.
- Install the corresponding trusted CA certificate in each of the Manager's windows certificate stores.
- Install valid, 1024 bits+, non self signed certificate (+ private key) in all Manager Certificate Stores.
- Install the corresponding certificates in all the system Certificate Stores of all permissible Manager entities, and the trusted CA certificate.

- Disable all the system Unsecured Interfaces.
- Set Manager Certificate Checks level to high in Manager Security Preferences.
- Set Certificate offered to the system in Manager Security Preferences.

The above essentially locks the systems and corresponding Managers together. Only recognized (by strong certificate) entities may communicate successfully on the service interfaces. All services use strong encryption and message authentication.

The use of intermediate CA certificates can be used to overcome the limit of 6 maximum certificates in each system Certificate Store.

Related Links

Security Administration on page 127

SRTP

Secure Real-Time Transport Protocol (SRTP) refers to the application of additional encryption and or authentication to VoIP calls (SIP and H.323). SRTP can be applied between telephones, between ends of an IP trunk or in various other combinations.

IP Office supports:

- Individual configuration for RTP and RTCP authentication and encryption
- HMAC SHA1 as the authentication algorithm
- AES-CM as the encryption algorithm
- 80 (default) or 32 bit authentication tag
- Master key length of 128 bits
- Master salt length of 112 bits.

Configuring the use of SRTP at the system level is done on the **System | VoIP Security** tab using the **Media Security** setting. The options are:

- **Best Effort**
- **Disabled (default)**
- **Enforced**

When enabling SRTP on the system, the recommended setting is **Best Effort**. In this scenario, IP Office uses SRTP if supported by the other end, and otherwise uses RTP. If the **Enforced** setting is used, and SRTP is not supported by the other end, the call is not established.

The system level setting can be overridden at the trunk or extension level. This can be used for special cases where the trunk or extension setting must be different from the system settings.

If the system level setting is **Enforced**, and devices that do not support SRTP are connected to the system, their extension level configuration must be **Disabled** or calls will fail. This extra configuration would typically not be required if the system level setting is **Best Effort**.

SRTP is supported on SIP Lines, SM Lines, and IP Office Lines. SRTP is not supported on H.323 IP trunks.

Encrypted RTCP

IP Office supports unencrypted RTCP by default. This default is compatible with most Avaya endpoints which do not currently support encrypted RTCP. To the extent possible, any type of endpoint using SRTP with IP Office should use unencrypted RTCP for consistency with other endpoints to allow for direct media.

IP Office supports RTCP encryption as a configurable option. In addition to system level configuration, it can be turned on at the trunk and extension level. Therefore, RTCP encryption can be configured as an exception for an entity which only supports encrypted RTCP. In such case there will be no direct media SRTP between that entity and one that does not support encrypted RTCP, and IP Office will relay the SRTP media.

Authentication

Authentication can be applied to both the voice part of calls (the RTP stream) and or to the control signal associated with the call (the RTCP stream). By default, IP Office supports RTP encryption, RTP authentication, RTCP authentication. Authentication is applied after encryption so that packets can be authenticated at the remote end without having to be decrypted first.

- The method used for the initial exchange of authentication keys during call setup depends on whether the call is using SIP or H.323. The IP Office system uses SDESC for SIP calls and H235.8 for H.323 calls.
- SRTP is only supported when using an addition method such as TLS or a VPN tunnel to establish a secure data path before call setup.
- A replay attack is when someone intercepts packets and then attempts to use them to for a denial-of-service or to gain unauthorized access. Replay protection records the sequence of packets already received. If a packed has been received previously, it is ignored. If packets arrive outside a specified sequence range, the security device rejects them. All packets in a stream (RTP and RTCP) have a sequential index number, however packets may not be received in sequential order. SRTP protects against replay attacks by using a moving replay window containing the index numbers of the last 64 authenticated packets received or expected. Any packet received that has an index older than the current window is ignored. Only packets with an index ahead of the window or inside the window but not already received are accepted. Separate replay protection is used for the RTP and the RTCP streams.
- Rekeying is the sending of new authentication keys at intervals during an secure call. This option is not supported by the IP Office system which just sends authentication keys at the start of the call.

SRTP sessions can use direct media between the devices or can be relayed via the IP Office system. In some scenarios the IP Office system can be one end of the SRTP part of a call that then continues to a non-SRTP destination.

If both the call originator and target require SRTP: A direct media is made if supported, using SRTP. If direct media is not supported, the call is relayed via the IP Office system. In either case SRTP parameters are negotiated end to end with the IP Office system translating and forwarding them from one end to other end if necessary.

If only the originator or target requires SRTP: A non-direct media call is setup with with SRTP negotiated between the IP Office system and the party which requires SRTP.

Emergency Calls

Emergency calls from an extension are not blocked even if SRTP is required but cannot be established.

Calls using SRTP do not use any special indication on the user's telephone. Normal call functions (conference, transfer, etc) remain available to the user. SRTP alarms and details of when SRTP is being used are shown by the System Status Application and System Monitor.

Related Links

Security Administration on page 127

Chapter 8: Editing IP Office Security Settings in Manager

The following conditions apply when editing the IP Office security settings.

- Editing of security settings may only be done online to a system.

  No offline saving or editing is allowed for security purposes.
- No errors in the security settings are allowed to persist.

  This prevents the system becoming inaccessible through operator error.
- Sets of changes to security objects may be made without the need for the OK button to be selected every time.

  This allows a coordinated set of changes to be accepted or canceled by the operator.

Loading Security Settings

About this task

The address ranges in which Manager searches for systems are set through the Manager preferences (File | Preferences | Discovery). The security mechanism used for security settings transfer between Manager and a system are set through the Secure Communications attribute of Manager preferences (**File | Preferences | Security**).

If not already done, switch Manager to security mode by selecting **File | Advanced | Security Settings**.

Note:

If the system's configuration settings have already been loaded using a service user name and Password that also has security access, then the security settings are automatically loaded when Manager is switched to security mode.

Procedure

1. If already in security mode, click  in the main toolbar or select **File | Open Security Settings** from the menu bar.
2. The Select IP Office window appears, listing those systems that responded.

   The list can be sorted by clicking on the column names.

3. If the system required was not found, the address used for the search can be changed.

   Enter or select the required address in the **Unit/Broadcast Address** field and then click Refresh to perform a new search.

4. When the system required is located, check the box next to the system and click **OK**.
5. The user name and password request for the system is then displayed.

   Enter the required details and click **OK**. By default this is a different user name and password from those that can be used for configuration access.

6. If the security settings are received successfully, they appear within Manager.
   - If the service user name/password is incorrect, or the service user has insufficient rights to read the security settings, **"Access Denied"** is displayed.
   - If the network link fails, or the secure communication mode is incorrect (for example Manager is set to unsecured, but the system is set to secure only), **"Failed to communicate with IP Office"** is displayed.

Saving Security Settings

About this task

Procedure

1. Click  in the **Main Toolbar** or select **File | Save Security Settings** from the menu bar. These options are only available when some change has been made.
2. The user name and password request for the system is then displayed.

   Enter the required details and click **OK**. By default this is a different user name and password from those that can be used for configuration access.

Resetting a System's Security Settings

About this task

Procedure

1. Select **File | Reset Security Settings** (if in security mode), or **File | Advanced | Erase Security Settings** (if in configuration mode).
2. The Select IP Office window appears, listing those systems that responded.

   The list can be sorted by clicking on the column names.

3. When the system required is located, check the box next to the system and click **OK**.
4. The user name and password request for the system is then displayed.

Enter the required details and click **OK**. By default this is a different user name and password from those that can be used for configuration access.

5. Manager will indicate if the security settings are reset successfully.

Chapter 9: Security Mode Field Descriptions

The Manager Security Mode is used to load and edit the security settings of a system. How the controls operate is similar to Manager in configuration mode.

To switch to Security Mode, select **File | Advanced | Security Settings**.

To switch back to Configuration Mode, select **File | Configuration**.

Security Mode Screen Elements

Table 3: Toolbar icons

Icon	Action
	Get the Security Settings
	Save the Security Settings
	Not Used in security mode
	Show/Hide the Navigation Pane
	Show/Hide the Group Pane
	Not used in security mode
	Not used in security mode

Security Settings Pane: This pane is used to select the type of security records that should be displayed in the group pane or details pane.

-  **General** Defines general security controls for the system. When selected, the settings are displayed in the details pane.
-  **System** Defines security settings for the system such as application access. When selected, the settings are displayed in the details pane.
-  **Services** Secure services supported by the system. Currently these are access to security settings and access to configuration settings.
-  **Rights Groups** Create groups with different access rights. When selected, the existing Rights Groups are displayed in the group pane.

-  **Service Users** Sets the name and password for an administrator. Also allows selection of the Rights Groups to which the user belongs. When selected, the existing service users are displayed in the group pane.

Group Pane: This pane is used to display the existing Right Groups or Service Users when those options are selected in the security settings pane.

Details Pane: This pane shows the settings selected in the security settings pane or the group pane.

Status Bar: This bar display messages about communications between Manager and systems. It also displays the security level of the communications by the use of a padlock icon.

Related Links

General Security Field Descriptions on page 149
System on page 153
Security Services Settings on page 160
Rights Groups on page 161
Service Users on page 166

General Security Field Descriptions

Field	Description
Security Administrator The Security Administrator is a special service user who does not belong to any **Rights Groups**. The Security Administrator is able to access the system's security settings but cannot access its configuration settings. By default they are the only service user able to access to the security settings.	
Unique Security Administrator	Default = Off When selected, only the Security Administrator is able to access the system's security settings. When this is selected, the security options for Rights Groups are disabled. When not selected, the ability to access security settings can also be assigned to Rights Groups.
Name:	Default = 'security'. Range = 6 to 31 characters. The name for the Security Administrator.
Password	Default = 'securitypwd'. Range = 8 to 31 characters. The password for the Security Administrator. In order to change the Security Administrator password, the current password must be known.
Minimum Password Complexity	Default = Medium. The password complexity requirements for the Security Administrator. This setting is active for attempted password changes on both Security Manager and the system. The options are:

Table continues…

Field	Description
	Low: Any password characters may be used without constraint. **Medium:** The password characters used must include characters from at least 2 of the 'code point sets' listed below. For example a mix of lower case and upper case. In addition, 3 or more consecutive identical characters of any type is not allowed. **High:** The password characters used must include characters from at least 3 of the 'code point sets' listed below. For example a mix of lower case, upper case and numbers. In addition, 3 or more consecutive identical characters of any type is not allowed. **Code Point Sets:** • Lower case alphabetic characters. • Upper case alphabetical character. • Numeric characters. • Non-alphanumeric characters, for example # or *.
Previous Password Limit (Entries)	Default = 4. Range = 0 (Off) to 10 records. The number of previous password to check for duplicates against when changing the password. When set to **0**, no checking of previous passwords takes place. This setting is active for attempted password changes on both Security Manager and the system.
Service User Details These settings control service user names and password/account policies. This setting is active for attempted password changes on all administration interfaces.	
Minimum Name Length	Default = 6, Range 1 to 31 characters. This field sets the minimum name length for service user names.
Minimum Password Length	Default = 8, Range 1 to 31 characters. This field sets the minimum password length for service user passwords.
Password Reject Limit	Default = 3, Range 0 to 255 failures. Sets how many times an invalid name or password is allowed within a 10 minute period before the Password Reject Action is performed. Selecting 0 indicates never perform the **Password Reject Action**.
Password Reject Action	Default = Log and Temporary Disable. The action performed when a user reaches the **Password Reject Limit**. The options are: • **No Action** • **Log to Audit Trail** Log to Audit Trail creates a record indicating the service user account name and time of last failure.

Table continues…

Field	Description
	• **Log and Disable Account**:. Log and Disable Account creates an audit trail record and additionally permanently disables the service user account. This account can only be enabled using the Security Manager Service User settings. • **Log and Temporary Disable**: Log and Temporary Disable creates an audit trail record and additionally temporarily disables the service user account for 60 seconds. This account can only be enabled using the Security Manager Service User settings.
Minimum Password Complexity	Default = Medium. The password complexity requirements for the Security Administrator. This setting is active for attempted password changes on both Security Manager and the system. The options are: **Low:** Any password characters may be used without constraint. **Medium:** The password characters used must include characters from at least 2 of the 'code point sets' listed below. For example a mix of lower case and upper case. In addition, 3 or more consecutive identical characters of any type is not allowed. **High:** The password characters used must include characters from at least 3 of the 'code point sets' listed below. For example a mix of lower case, upper case and numbers. In addition, 3 or more consecutive identical characters of any type is not allowed. **Code Point Sets:** • Lower case alphabetic characters. • Upper case alphabetical character. • Numeric characters. • Non-alphanumeric characters, for example # or *.
Previous Password Limit (Entries)	Default = 4. Range = 0 (Off) to 10 records. The number of previous password to check for duplicates against when changing the password. When set to **0**, no checking of previous passwords takes place. This setting is active for attempted password changes on both Security Manager and the system.
Password Change Period	Default = 0 (Off). Range 0 to 999 days. Sets how many days a newly changed password is valid. Selecting 0 indicates any password is valid forever. This setting is active for password changes through this form or prompted by Manager. Note that the user must be a member of a Rights Group that has the Security Administration option **Write own service user password** enabled. If this timer expires, the service user account is locked. The account may only be re-enabled using the Service User Settings. To prompt the user a number of days before the account is locked set a Expiry Reminder Time (see below). Whenever this setting is changed and the OK button is clicked, the Security Manager recalculates all existing service user password timers.

Table continues…

Field	Description
Account Idle Time	Default = 0 (Off). Range 0 to 999 days. Sets how many days a service user account may be inactive before it becomes disabled. Selecting 0 indicates an account may be idle forever. If this timer expires, the service user account is permanently disabled. The account may only be re-enabled using the Service User Settings. The idle timer is reset whenever a service user successfully logs in. Whenever this setting is changed and the OK button is clicked, the Security Manager recalculates all existing service user idle timers.
Expiry Reminder Time	Default = 10. Range 0 (Off) to 999 days. Sets the period before password or account expiry during which a reminder indication if the service user logs in. Selecting 0 prevents any reminders. Reminders are sent, for password expiry due to the Password Change Period (above) or due to the Account Expiry date (see Service User setting) – whichever is the sooner. Currently Manager displays reminders but System Status does not.
IP Office User Details These settings control IP Office user password/account policies.	
Password Enforcement	Default = On. When enabled, password settings are enforced. When disabled, password requirements are not enforced and the remaining settings are not editable
Minimum Password Length	Default = 8, Range 1 to 31 characters. This field sets the minimum password length for user passwords
Minimum Password Complexity	Default = Medium. The password complexity requirements for the Security Administrator. This setting is active for attempted password changes on both Security Manager and the system. The options are: **Low:** Any password characters may be used without constraint. **Medium:** The password characters used must include characters from at least 2 of the 'code point sets' listed below. For example a mix of lower case and upper case. In addition, 3 or more consecutive identical characters of any type is not allowed. **High:** The password characters used must include characters from at least 3 of the 'code point sets' listed below. For example a mix of lower case, upper case and numbers. In addition, 3 or more consecutive identical characters of any type is not allowed. **Code Point Sets:** • Lower case alphabetic characters. • Upper case alphabetical character.

Table continues…

Field	Description
	• Numeric characters. • Non-alphanumeric characters, for example # or *.
Password Reject Limit	Default = 5, Range 0 to 255 failures. Sets how many times an invalid name or password is allowed within a 10 minute period before the Password Reject Action is performed. Selecting 0 indicates never perform the **Password Reject Action**.
Password Reject Action	Default = Log and Temporary Disable. The action performed when a user reaches the **Password Reject Limit**. The options are: • **No Action** • **Log to Audit Trail** Log to Audit Trail creates a record indicating the user account name and time of last failure. • **Log and Disable Account** Log and Disable Account creates an audit trail record and additionally permanently disables the user account. The account can be enabled using the **Account Status** field on the **User | User** page. • **Log and Temporary Disable** Log and Temporary Disable creates an audit trail record and additionally temporarily disables the user account for 60 seconds. The account can be enabled using the **Account Status** field on the **User | User** page.

Related Links

Security Mode Field Descriptions on page 148

System

Related Links

Security Mode Field Descriptions on page 148
System Details on page 153
Unsecured Interfaces on page 155
Certificates on page 156

System Details

Field	Description
Base Configuration	
Services Base TCP Port	Default = 50804. Range = 49152 to 65526. This is the base TCP port for services provided by the system. It sets the ports on which the system listens for requests to access those services, using its LAN1 IP address. Each service uses a port offset from the base port value. If this value is changed from

Table continues…

Field	Description
	its default, the Manager application must be set to the same Base TCP Port through its Services Base TCP Port setting (File | Preferences). For information on port usage see the IP Office Avaya Port Matrix document on the Avaya support site at
Maximum Service Users	Default = 64. This is a fixed value for indication purposes only. This value is the maximum number of service users that can be stored in a system's security settings
Maximum Rights Groups	Default = 32. This is a fixed value for indication purposes only. This value is the maximum number of Rights Groups that can be stored in a system's security settings.
System Discovery System discovery is the processes used by applications to locate and list available systems. The IP Office can be disabled from responding to this process if required. If this is done, access to the IP Office requires its specific IP address to be used.	
TCP Discovery Active	Default = On. Selecting TCP Discovery Active allows the system to respond to those requests.
UDP Discovery Active	Default = On. Selecting UDP Discovery Active allows the system to respond to those requests.
Security These settings cover the per-system security aspects, primarily TLS settings.	
Session ID Cache	Default = 10 hours, Range 0 to 100 hours. This sets how long a TLS session ID is retained by the system. If retained, the session ID may be used to quickly restart TLS communications between the system and a re-connecting application. When set to **0**, no caching takes place and each TLS connection must be renegotiated.
HTTP Challenge Timeout (Seconds)	Default = 10. For HTTP/HTTPS connection attempts, this field sets the timeout for connection validation responses.
RFC2617 Session Cache (Minutes)	Default = 10. For HTTP/HTTPS sessions, this field sets the allowed duration for successful logins as per RFC2617.
HTTP Ports	
HTTP Port	Default = 80.
HTTPS Port	Default = 443.
Web Services Port	Default =8443.

Related Links

System on page 153

Unsecured Interfaces

These features relate to applications that access the system configuration settings using older security methods.

Field	Description
System Password	Default = 'password'. Range = 0 to 31 characters. The system password is used by Manager to upgrade IP Office IP500 V2 systems. Also used for Monitor when the Monitor password setting is blank.
VM Pro Password	Default = Blank. Range = 0 to 31 characters. This password is required if a matching password is also set through the Voicemail Pro client application. Typically no password is set.
Monitor Password	Default = Blank. Range = 0 to 31 characters. This password, if set, is used by the System Monitor application. If this password is not set, those applications use the system password. If changing this password with no previous password set, enter the system password as the old password.
Applications Controls	These check boxes control which actions the system will support for legacy applications. Different combinations are used by the different applications. A summary of the applications affected by changes is listed in the **Application Support** list. • **TFTP ServerIt**: Default = On. • **TFTP Directory Read**: Default = Off. • **TFTP Voicemail**: Default = On. • **Program Code**: Default = On. • **DevLink**: Default = On. • **Sys Monitor**: Default = Off. • **TAPI**: Default = On. • **HTTP Directory Read**: Default = On. Allow the system's current directory records to be accessed using HTTP. • **HTTP Directory Write**: Default = On. Allow HTTP import to be used to place temporary directory records into the directory.
Application Support	This panel is shown for information only. It indicates the effect on various applications of the Application Controls selections.

Related Links

System on page 153

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 Certificate Name	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 Domain Cert Name	Default = Blank.
SCEP Password	Default = Blank.

Related Links

System on page 153

Security Services Settings

This tab shows details of the services that the system runs to which service users can communicate.

Field	Description
Name	The name of the service. This is a fixed value for indication purposes only.
Host System	This field shows the system's name. This is a fixed value for indication purposes only.
Service Port	This is the port on which the system listens for attempts to access the service. The routing of traffic to this port may need to be enabled on firewalls and network devices between the service users and the system. The base port (TCP or HTTP) for each service is offset by a fixed amount from the ports set in System Settings. For information on port usage see the IP Office Avaya Port Matrix document on the Avaya support site at https://support.avaya.com/helpcenter/getGenericDetails?detailId=C201082074362003
Service Security Level	Default = ‘Unsecure Only’. Sets the minimum security level the service will support. See **File | Preferences | Security** for the corresponding Manager application setting, which must be changed to match the appropriate service access security settings.

Table continues…

Field	Description
	Warning: If the system does not already have an X509 security certificate, selecting a setting other than **Unsecure Only** will cause the system to stop responding for a period (less than a minute) while the system generates its own unique security certificate. The options are: • **Unsecure Only** This option allows only unsecured access to the service. The service's secure TCP port, if any, is disabled. This or disabled are the only options supported for the System Status Interface and Enhanced TSPI services. • **Unsecure + Secure** This option allows both unsecured and secure (Low) access. In addition, TLS connections are accepted without encryption, just authentication. • **Secure, Low** This option allows secure access to that service using TLS, and demands weak (for example DES_40 + MD5) encryption and authentication or higher. The service's unsecured TCP port is disabled. • **Secure, Medium** This option allows secure access to that service using TLS, and demands moderate (for example DES_56 + SHA-1) encryption and authentication or higher. The service's unsecured TCP port is disabled. • **Secure, High** This option allows secure access to that service using TLS and demands strong (for example 3DES + SHA-1) encryption and authentication, or higher. In addition, a certificate is required from the client (usually Manager). See System Details | Client Certificate Checks for tests made on the received certificate. The service's unsecured TCP port is disabled. • **Disabled** This option is available for the System Status Interface and Enhanced TSPI services. If selected, access to the service is disabled.
Service Access Source	For Server Edition systems, it is defaulted to **Business Edition Manager**. When set to **Business Edition Manager**, the system can only be configured using Manager in its Server Edition mode. When set to Unrestricted, the system can be configure using Manager in its normal Simplified View or Advanced View modes. **Warning:** Opening the configuration of a Server Edition system in Manager running in any mode other than Server Edition mode should be avoided unless absolutely necessary for system recovery. Even in that case, Manager will not allow renumbering, changes to the voicemail type and changes to H.323 lines.

Related Links

Security Mode Field Descriptions on page 148

Rights Groups

Related Links

Security Mode Field Descriptions on page 148

Group Details

This tab sets the name of the Rights Group.

Field	Description
Name	: Range = Up to 31 characters The name for the Rights Group should be unique. The maximum number of rights groups is 32.

Related Links

Rights Groups on page 161

Configuration

This tab sets the configuration settings access for service user's who are members of this Rights Group.

Field	Description		
IP Office Service Rights	This setting controls what action on the system can be performed by members of the Rights Group.		
Manager Operator Rights	This setting controls what types of configuration records Manager will allow members of the Rights Group to viewed and what actions they can perform with those types of records.		
	Operator	**View/Edit/ New/Delete**	**Configuration Record Types**
	Administrator	All	View, edit create and delete all configuration records.
	Manager	View	View all except WAN Port.
		Edit	Extension, User, Hunt Group, Short Code, Service, RAS, Incoming Call Route, Directory, Time Profile, Firewall Profile, IP Route,
		New	

Table continues…

Field	Description		
			Least Cost Route, Account Code, ARS.
		Delete	As edit except Short Code.
	Operator	View	View all except WAN Port.
		Edit	Extension, User, Hunt Group, Short Code, Service, RAS, Incoming Call Route, Time Profile, Firewall Profile, IP Route, Least Cost Route, Account Code, License, ARS.
		New	None.
		Delete	Delete Incoming Call Route and Directory.
	User & Group Edit	View	User and Hunt Group records only.
		Edit	
		New	None
		Delete	
	User & Group Admin	All	User and Hunt Group records only.
	Dir & Account Admin	All	Directory and Account Code records only.
	Time & Attendant Admin	All	Time Profile and Auto Attendant records only.
	ICR & User Rights Admin	All	Incoming Call Route and User Rights records only.
	Read Only	View	View all configuration records.
		Edit	None.
		New	
		Delete	

Related Links

Rights Groups on page 161

Security Administration

This tab sets the security settings access for Service user's who are members of this Rights Group. These settings are ignored and greyed out if a Unique Security Administrator has been enabled in General Settings.

Field	SDescription
Read all security settings	Members of the Rights Group can view the system's security settings.
Write all security settings	Members of the Rights Group can edit and return changes to the system's security settings.
Reset all security settings	If selected, members of the Rights Group can reset the security settings to default values.
Write own service user password	If selected, members of the Rights Group can change their own password when requested to do so by the system. That request may be the result of a Password Change Period, Force new password or Account Expiry. The new password change is requested automatically at login time.

Related Links

Rights Groups on page 161

System Status

This tab sets whether members of the group can access the system using the System Status Application (SSA).

Field	Description
System Status Access	If selected, members of the Rights Group can view the system's current status and resources using the System Status Application (SSA).
Read all configuration	The System Status application includes tools to take a snapshot of the system for use by Avaya for diagnostics. That snapshot can include a full copy of the system's configuration settings. This setting must be enabled for the SSA user to include a copy of the configuration in the snapshot.
System Control	If enabled, the SSA user is able to use SSA to initiate system shutdowns and memory card shutdown/restarts.
SysMonitor Access	If enabled, members of the Rights Group can use the System Monitor application to perform detailed diagnosis of system problems.

Related Links

Rights Groups on page 161

Enhanced TSPI

This tab sets whether members of the group can access the system using the Enhanced TSPI application interface.

Field	Description
Enhanced TSPI Access	If selected, applications in this rights group are able to use the system's Enhanced TSPI interface. This interface is currently used by the one-X Portal application server for its connection to the system.

Related Links

Rights Groups on page 161

HTTP

This tab sets the HTTP services supported for members of the group.

Field	Description
DECT R4 Provisioing	This service is used to allow the system to configure the DECT R4 master base station and to respond to handsets subscribing to the DECT R4 system. It requires both the system and DECT R4 master base station to be configured to enable provisioning. For full details refer to the DECT R4 Installation Manual.

Related Links

Rights Groups on page 161

Web Services

These settings are used by users in rights groups using web services to configure and manage the system. These are currently not used on Standard Mode systems

IP Office Service Rights

Field	Description
Security Read All	If selected, the rights group members can view system security settings.
Security Write All	If selected, the rights group members can change system security settings.
Security Write Own Password	If selected, members of the Rights Group can change their own password when requested to do so by the system. That request may be the result of a Password Change Period, Force new password or Account Expiry. The new password change is requested automatically at login time.
Config Read All	If selected, the rights group members can view system configuration settings
Config Write All	If selected, the rights group members can change system configuration settings.
Backup	If selected, the rights group members can initiate the system backup process.
Restore	If selected, the rights group members can initiate the system restore process.
Upgrade	If selected, the rights group members can initiate the system upgrade process.

Web Manager Rights

These rights are used with web service access to a system such as the IP Office web manager used with IP Office Basic Edition systems.

Related Links

Rights Groups on page 161

External

These settings are used by users in rights groups for external components using web services to configure and manage the system.

IP Office Service Rights

Field	Description
Voicemail Pro Basic	If selected, the rights group members can read the configuration and perform backup, restore, and upgrade.
Voicemail Pro Standard	If selected, the rights group members can update the configuration and perform backup, restore, and upgrade.
Voicemail Pro Administrator	If selected, the rights group members can update the configuration and security settings.
one-X Portal Administrator	If selected, the rights group members can update the configuration and security settings. Does not include backup and restore.
one-X Portal Super User	If selected, the rights group members can perform backup and restore.
Web Control Administrator	If selected, the rights group members can update the configuration settings.
Web Control Security	If selected, the rights group members can update the security settings.
WebRTC Gateway Administrator	If selected, the rights group members can update the configuration settings.

Related Links

Rights Groups on page 161

Service Users

These settings are displayed when **Service Users** is selected in the navigation pane and a particular service user is selected in the group pane.

The maximum number of service users is 64.

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 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**.

Table continues…

Field	Description
	• **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

Security Mode Field Descriptions on page 148

Chapter 10: Editing Configuration Settings

Before editing the system's configuration settings, it is important to understand how those settings are stored and used by the system.

The control unit holds copies of its configuration in both its internal non-volatile and RAM memory. A copy is also held on the System SD card (IP500 V2).

The copies in non-volatile memory and System SD card, are retained even if power to the control unit is removed.During power up, the system loads the configuration file stored on the System SD card into its RAM memory. Other systems load the configuration stored in non-volatile memory into RAM memory. The copy in RAM memory is then used to control the system's operation.

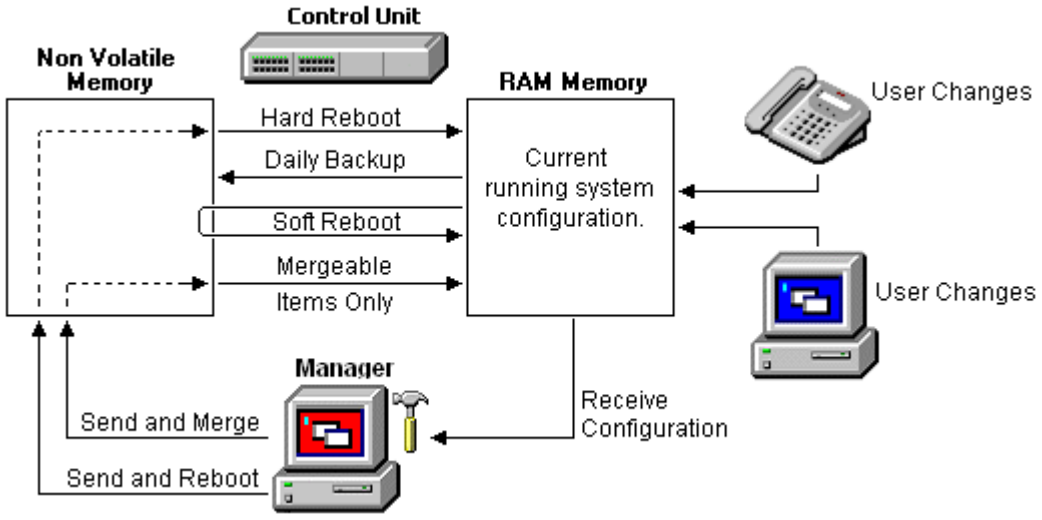
If the system encounters a problem using the configuration file in its System SD card's `/primary` folder, it attempt to use the copy in its non-volatile memory. For fully details of the IP500 V2 boot process and SD card usage refer to the IP Office Installation Manual.

Users actions such as changing their forward destinations or mailbox passcode are written to the configuration in RAM memory.

Changes made using Manager are written to the configuration in non-volatile memory and then copied into the RAM memory and System SD.

Between 00:00 and 00:30, a daily backup occurs which copies the configuration in the system's operation RAM memory back into its non-volatile memory and, on IP500 V2 system's, the System SD card.On IP500 V2 system, the contents of the system memory cards `/primary` folder can then also be automatically copied to the `/backup` folder by enabling System | System | Automatic Backup.

When the system is shutdown using the correct shutdown method, the configuration in RAM memory is copied to the non-volatile memory and System SD card.



Using Manager

When using Manager to edit the configuration settings, the following need to be remembered:

- Manager receives the current configuration settings from RAM memory. Therefore the configuration it receives includes any changes made by users up to that time. However it will not contain any subsequent changes made by users.
- When sending the configuration settings back to the system, Manager allows two choices, reboot or merge.
- Reboot sends the configuration to the system's non-volatile memory along with an instruction to reboot. Following the reboot, the new configuration in non-volatile memory is copied to the RAM memory and used.
- Merge sends the configuration to the system's non-volatile memory without rebooting. The system then copies those changes that are mergeable into the RAM memory. A key point here is that not all configuration settings are mergeable, see the Mergeable Settings list.

As a result of the above, it is important to bear the follow scenarios in mind:

- Changes made by users after a configuration is received by Manager may be lost when the configuration is sent back from Manager. Therefore it is preferable to always edit a recently received copy of the configuration rather than one that has been open for a period of time.
- If a merge is attempted with non-mergeable changes, those items will be written to the non-volatile memory but will not be copied to RAM memory. If a daily backup occurs, they will then be overwritten by the RAM. If a power loss reboot occurs, they will be written to RAM memory.

Related Links

Mergeable Settings on page 171
Configuration Size on page 173
Setting the Discovery Addresses on page 174
Opening a Configuration from a System on page 175
Opening a Configuration Stored on PC on page 178
Known System Discovery on page 178

Mergeable Settings

The table below shows the configuration records for which changes can be merged and those that require a system reboot. The **Send Configuration** menu shown when sending a configuration to the system automatically indicates when the configuration is mergeable.

Mergeable		3.2+	Pre-3.2
	System	-	-
	- System	✓*1	✗
	- LAN1/LAN2	✗	✗
	- DNS	✗	✗
	- Voicemail	✓*2	✗
	- Telephony	✓*3	✗
	- VoIP	✗	✗
	- LDAP	✗	✗
	- System Events	✗	✗
	- CDR/SMDR	✓	✗
	- Twinning	✓	-
	Line	✗	✗
	Control Unit	✗	✗
	Extension	✗	✗*4
	User	✓	✓
	Hunt Group	✓	✓
	Short Code	✓	✓

Table continues…

	Service	✓	✓
	RAS	✓	✓
	Incoming Call Route	✓	✓

Mergeable		3.2+	Pre-3.2
	WAN Port	✗	✗
	Directory	✓	✓
	Time Profile	✓	✗
	Firewall Profile	✓	✓
	IP Route	✓	✓
	Account Code	✓	✓
	License	✓	✓
	Tunnel	✗	✗
	User Rights	✓	✓
	Auto Attendant	✓	✗
	Authorization Code	✓	✗
	ARS	✓	-

***1 - 3.2+ | System | System** Changes to **Locale** and **Favor RIP Routes over Static** require a reboot.

***2 - 3.2+ | System | Voicemail** Changes to **Voicemail Type** require a reboot.

***3 - 3.2+ | System | Telephony** Changes to **Companding LAW** and **Busy Tone Detection** require a reboot.

***4 - 4.1+ | Extension Base Extension** and **Disable Speakerphone** are mergeable.

Related Links

Editing Configuration Settings on page 169

Configuration Size

The maximum size of the configuration file that can be loaded into an IP 500 V2 control unit is 2.0 MB.

When you attempt to save a configuration that is too large, you will be prompted and the save is canceled.

During normal operation, additional configuration records can be added to the configuration without using Manager (for example call log records and directory records made from phones). If, during the overnight backup to flash memory, the configuration if found to be too large, records will be removed until the configuration is sufficiently small to be backed up. The recordsremoved are call log records, system directory records and then personal directory in that order. Note that those records will still exist in the configuration running the system in its RAM memory, however if the system is restarted they will disappear as the configuration is reloaded from the Flash memory.

Figures for all individual records in the configuration cannot be given as they vary. The list below gives typical values, in bytes, for common records:

Physical Extension: 70.

IP Extension: 70.

User: 170.

User Short Code: 40.

DSS Button: 20.

Hunt Group: 100.

Hunt Group member: 10.

System Short Code: 10.

Normal Service: 220.

Intranet Service: 240.

WAN Service: 400.

RAS Service: 110.

Incoming Call Route: 30.

WAN Port (PPP): 70.

WAN Port (FR): 120.

Directory Record: 70.

Time Profile: 40.

Time Profile Record: 20.

Firewall Profile: 40.

Custom Firewall Record: 80.

IP Route (Static): 30.

License Key: 40.

Account Code: 40.

Logical LAN: 60.

Tunnel (L2TP): 200.

Tunnel (IPSec): 110.

Related Links

Editing Configuration Settings on page 169

Setting the Discovery Addresses

By default, when  or **File | Open configuration** is selected, Manager's **Select IP Office** window opens. It performs a UDP broadcast to the address 255.255.255.255. This broadcast will only locate systems that are on the same network subnet as the PC running Manager.

For systems not located on the same subnet as the Manager PC, the following options are supported.

Specific Addressing The **Unit/Broadcast Address** shown on the **Select IP Office** menu can be changed to the specific IP address of the required system. A single address is routable and so can be used to discover a system on another subnet.

TCP Discovery Address Ranges A set of TCP addresses and address ranges can be specified for use by the **Select IP Office** discovery process.

Known System Discovery Manager can write the details of systems it discovers to a file. The list of systems in that file can then be used for access to those systems. See Known System Discovery.

DNS Lookup Manager can be configured to locate systems using DNS name lookup. This requires the systems on a customer network to be added as names on the customer's DNS server and the Manager PC to be configured to use that server for DNS name resolution. The use of DNS is configured through File | Preferences | Discovery.

Changing the Initial Discovery Settings The **Discovery** tab of the **Preferences** menu can be used to set the UDP and TCP addresses used by the discovery process run by the **Select IP Office** menu.

1. Select **File | Preferences** menu.
2. Select the **Discovery** tab.

TCP Discovery: Default = On. This setting controls whether Manager uses TCP to discover systems. The addresses used for TCP discovery are set through the IP Search Criteria field below.

NIC IP/NIC Subnet This area is for information only. It shows the IP address settings of the LAN network interface cards (NIC) in the PC running Manager. Double-click on a particular NIC to add

the address range it is part of to the IP Search Criteria. Note that if the address of any of the Manager PC's NIC cards is changed, the Manager application should be closed and restarted.

IP Search Criteria This section is used to enter TCP addresses to be used for the TCP discovery process. Individual addresses can be entered separated by semi-colons, for example 135.164.180.170; 135.164.180.175. Address ranges can be specified using dashes, for example 135.64.180.170 - 135.64.180.175.

UDP Discovery: Default = On This settings controls whether Manager uses UDP to discover systems.

Enter Broadcast IP Address: Default = 255.255.255.255 The broadcast IP address range that Manager should used during UDP discovery. Since UDP broadcast is not routable, it will not locate systems that are on different subnets from the Manager PC unless a specific address is entered.

Use DNS: Selecting this option allows Manager to use DNS name (or IP address) lookup to locate a system. Note that this overrides the use of the TCP Discovery and UDP Discovery options above. This option requires the system IP address to be assigned as a name on the users DNS server. When selected, the **Unit/Discovery Address** field on the Select IP Office dialogue is replaced by a **Enter Unit DNS Name or IP Address** field.

SCN Discovery: If enabled, when discovering systems, the list of discovered systems will group systems in the same Small Community Network and allow them to be loaded as a single configuration. At least one of the systems in the Small Community Network must be running Release 6.0 or higher software. See Small Community Network Management. This does not override the need for each system in the Small Community Network to also be reachable by the **TCP Discovery** and or **UDP Discovery** settings above and accessible by the router settings at the Manager location.

Related Links

Editing Configuration Settings on page 169

Opening a Configuration from a System

The initial IP address ranges in which Manager searches for systems are set through the Manager preferences (File | Preferences | Discovery). By default it scans the local network of the Manager PC.

Start Manager. If Manager is already started and a configuration is open in it, that configuration must be closed first.

- If Manager is set to Auto Connect on start up, it will scan for systems automatically and either display the list of systems discovered or automatically start login to the only system discovered.
- Otherwise, click on  or select **File | Open Configuration**.

The Select IP Office window appears, listing those systems that responded.

- If Server Edition systems are detected, they are grouped together. By default the configuration of those systems cannot be opened using Manager in **Advanced View** mode and the configuration of a Primary Server can only be opened if the Open with Server Edition Manager option is also selected. See Server Edition Mode.
- If Manager has been set with SCN Discovery enabled, systems in a Small Community Network are grouped together. The checkbox next to the network name can be used to load the configurations of all the configurations into Small Community Network management mode.
- If the system required was not found, the **Unit/Broadcast Address** used for the search can be changed. Either enter an address or use the drop-down to select a previously used address. Then click **Refresh**to perform a new search.
- The address ranges used by Manager for searching can be configured through the **File | Preferences | Discovery** tab.
- A list of known systems can be stored and used. See Known System Discovery
- Manager can be configured to search using DNS names. See the Use DNS option.
- Systems found but not supported by the version of Manager being used will be listed as **Not Supported**.
- If the system detected is running software other than from its primary folder, a  warning icon will be shown next to it. The configuration can still be opened but only as a read-only file.

When you have located the system required, check the box next to the system and click **OK**.

If the system selected is a Server Editionsystem and Manager is not running in Server Edition mode, an **Open with Server Edition Manager** checkbox is shown and pre-selected. Clicking **OK** will switch Manager to its Server Edition mode before loading the configuration.

The system name and password request is displayed. Enter the required details and click **OK**.

The name and password used must match a service user account configured within the system's security settings.

Additional messages will inform you about the success or failure of opening the configuration from the system.

The method of connection, secure or insecure, attempted by Manager is set the applications Secure Communications preferences setting.

- When **Secure Communications** is set to **On**, a  padlock icon is displayed at all times in the lower right Manager status field.
- New installations of Manager default to having **Secure Communications** enabled. This means Manager by default attempts to use secure communications when opening a configuration.
- For Server Edition systems, Manager will always attempt to use secure communications regardless of the **Secure Communications** setting.
- If no response to the use of secure communication is received after 5 seconds, Manager will offer to fallback to using unsecured communications.

Following a successful log in, the configuration is opened in Manager. The menus and options displayed will depend on the type of system configuration loaded.

Login Messages

While attempting to login to a system, various additional messages may be displayed.

Configuration Not Loaded Messages

Access Denied This is displayed as the cause if the service user name/password were incorrect, or the service user has insufficient rights to read the configuration. The Retry option can be used to log in again but multiple rejections in a 10 minute period may trigger events, such as locking the user account, set by the Password Reject Limit and Password Reject Action options in the systems security settings.

Failed to communicate with system This is displayed as the cause if the network link fails, or the secure communication mode is incorrect (for example Manager is set to unsecured, but the system is set to secure only).

Account Locked The account of the service user name and password being used is locked. This can be caused by a number of actions, for example too many incorrect password attempts, passing a fixed expiry date, etc. The account lock may be temporary (10 minutes) or permanent until manually unlocked. An account can be enabled again through the system's security settings.

Additional Messages

Your service user account will expire in X days This message indicates that an Account Expiry date has been set on the system service user account and that date is approaching. Someone with access to the system's security settings will be required unlock the account and set a new expiry date.

Your password will expire in X days. Do you wish to change it now? This message indicates that password ageing has been configured in the system's security settings. If your password expires, someone with access to the system's security settings will be required to unlock the account.

Change password Through the system's security settings, a service user account can be required to change their password when logging in. The menu provides fields for entering the old password and new password.

Contact Information Check - This configuration is under special control This message will appear if a Manager user with administrator rights has entered their contact information into the configuration. For example to indicate that they do not want the configuration altered while a possible problem is being diagnosed. The options available are:

Cancel Select this option to close the configuration without making any changes.

Set configuration alteration flag Select this option if the configuration is being opened because some urgent maintenance action. When the configuration is next opened, the fact that it has been altered will be indicated on the System | System tab.

Delete Contact Information Select this option to take the system out of special control.

Leave contact information and flags unchanged (Administrators only) This option is only available to service users logging in with administrator rights.

Related Links

Editing Configuration Settings on page 169

Opening a Configuration Stored on PC

About this task

A configuration file previously saved on the PC can be reopened in Manager. This method of access does not require entry of a service user name and password. All parts of the configuration are visible.

Use either of the following processes to load a saved configuration file:

Procedure

1. Click the main toolbar or select **File | Offline | Open File** from the menu bar. If the files is one that has previously been opened offline, click the symbol next to in the main toolbar
2. An Open configuration file window appears.

   Use this to browse to the required configuration file.
3. Select the file and click **Open**.

Related Links

Editing Configuration Settings on page 169

Known System Discovery

The **Select IP Office** menu normally displays systems discovered by Manager using either UDP broadcast and or TCP requests (see Setting the Discovery Addresses). Manager can be configured to also record details of discovered units and then display a list of those previously discovered ('known') systems.

Related Links

Editing Configuration Settings on page 169

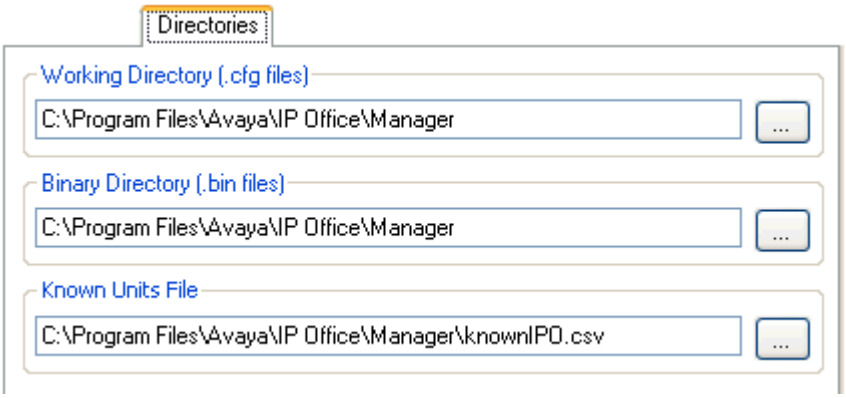
Configuring Manager for Known System Discovery

About this task

Use of known systems discovery is not enabled by default. The Manager must be configured for the feature with a file location to which it can store and retrieve known system details.

Procedure

1. Select **File | Change Working Directory**.



2. In the **Known Units File** field, enter the directory path and file name for a CSV file into which Manager can write details of the systems it discovers.

   If the file specified does not exist it will be created by Manager.

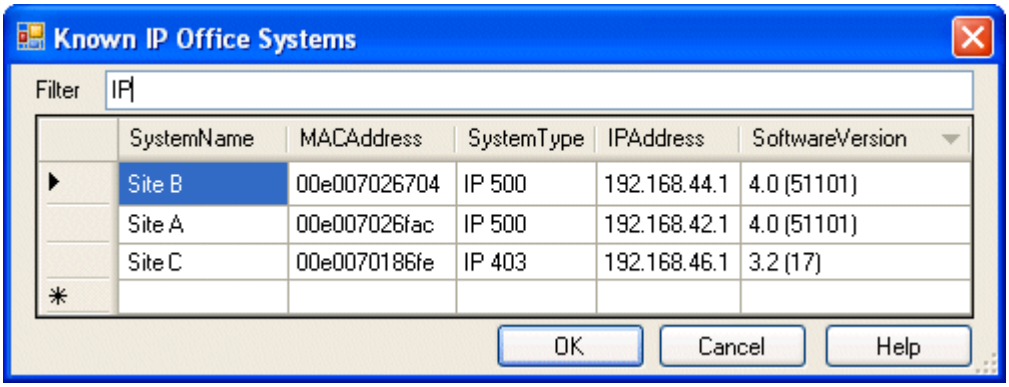
3. Click **OK**.

Using Known System Discovery

About this task

Procedure

1. When the Select IP Office screen is displayed click on **Known Units**.



2. The screen displays the list of systems previously discovered and stored in the CSV file.
3. To select an control unit, highlight the row containing unit data and click **OK**.

   The selected unit will appear in the Select IP Office window.
4. To filter displayed units, type the first few characters of the unit name in the **Filter** field.

   Any unit whose name does not match the filter will be temporarily hidden.
5. Each discovery appends data to the known unit list.

   It is possible that details of some records in the list may be out of date. Right clicking on the leftmost (grey) column of any row will bring up a floating menu offering the options of **Refresh** and **Delete**.
6. A new record may be manually added without having to access the system first through normal discovery.

   Enter the IP address of the new system in the IP Address column of the blank row shown with a * and select **Refresh** from the floating menu. This will update the Known Units file with data relating to the unit with the specified address.
7. Select **Cancel** to return to the **Select IP Office** menu.

Result

Note:

- The key used by the Known Systems CSV file is the IP address. The file cannot contain records for separate systems that use the same IP address for access.
- The file can be made read only. In that case any attempts using Manager to update the file will be ignored.

Creating New Records

There are a number of ways in which you can add new records to the configuration currently loaded in Manager.

Related Links

Editing Configuration Settings on page 169

Adding a New Record Using the Details Pane

About this task

Procedure

1. Use the navigation pane, groups pane or navigation toolbar, select an existing record of the type required.

2. Click at the top-right of the details pane.
3. Select the type of record required.

   For example, with extensions you can select from **H.323 Extension** or **SIP Extension**.
4. Complete the settings for the new record and click **OK**.

Adding a New Record Using the Group Pane

About this task

Procedure

1. Using the navigation pane or navigation toolbar, select the type of record required.
2. Right-click on the group pane and select **New**.
3. If a list is displayed, select the specific type of record required.
4. Complete the settings for the new record and click **OK**.

Adding a New Record Using the Navigation Pane

About this task

Procedure

1. In the navigation pane, right-click on the type of record required and select **New**.
2. If a list is displayed, select the specific type of record required.
3. Complete the settings for the new record and click **OK**.

Other record creation methods

About this task

Procedure

1. Import records

   New records can be created for users, hunt groups, short codes and directory entries by importing files. See Importing and Exporting Settings.
2. Automatically create records

   There are scenarios where new records are automatically added to the configuration:

   - Certain default records are added to the configuration when a new system is started or when a system configuration is erased.
   - New records for extensions and lines are automatically added to match the hardware present when a system is started or rebooted.

- For telephones connected via IP links (H.323, SIP and DECT), the system can be configured to automatically create extension and or user records to match the telephone.

3. Use templates to create records

   Manager supports a number of methods by which new records can be created from templates.

   Trunk Templates SIP trunks can be created from templates. For analog trunks, records are automatically created by the presence of the trunk hardware, however a template can then be applied to an analog trunk.

   Server Edition When being used to edit the configuration of Server Edition systems, Manager has a number of additional options to export existing records as templates and to create new records from those templates.

Creating an Offline Configuration

About this task

Manager can be used to create a new configuration without connecting to a system. This allows the creation of a configuration prior to installation of the real system and so can be used to speed up the installation process.

The configuration created must match the physical equipment in the system into which the configuration will be loaded. Doing otherwise may cause the system to reset and experience other problems.

The **Create Configuration** tool includes all control units, external expansion modules and trunk cards supported. It is your responsibility to confirm what equipment is supported in your locale.

Creating a New Configuration

Procedure

1. Close or save any configuration currently open.
2. Click  in the main toolbar or select **File | Offline | Create New Config**.
3. You should set the **Configuration**, **Locale**, **Extension Number Length** and **System Unit** first.

   Changing any of these after you start selecting other system hardware will reset the hardware selections.

4. Select the type of **Configuration** you want to create.

   The other options available will change depending on the selection. If the menu has been started from Manager running in Server Edition mode, the only option is **Server Edition Edition**.

5. Select the **Locale** for the system.

This defines a range of features such as default telephony settings.

6. The **Extension Number Length** setting value can be **None** or **3** to **15**.

   If a value is selected, all default extension, user and hunt group extension numbers created by Manager will be that length. In addition Manager will display a warning if an extension number of a different length is entered when editing the configuration.

7. Select the type of **System Unit**.

   Select the hardware components for the system. For a Server Edition system this is only necessary if a Expansion System (V2) is selected as the **System Units** option.

8. Select the additional cards to include in the control unit.

   The number and type of cards selectable will depend on the control unit type.

9. Select the external expansion modules to also include in the system.
10. Click **OK**.
11. For non-Server Edition systems, the configuration is created and loaded into Manager.

    For Server Edition systems, the Initial Configuration menu for the selected type of system unit is displayed. Complete the menu and click **Save**.

12. Once this configuration has been edited as required it can be saved on the PC or sent to a system.
13. **To Save a Configuration File on the PC** Use **File | Save Configuration**.
14. **To Send the Configuration to a System** If the system which you want to use the configuration is available, use File | Offline | Send Configuration to send the configuration to it.

    Warning:

    This action will cause the system to reboot and will disconnect all current calls and service.

    - Ensure that you have a copy of the systems existing configuration before overwriting it with the off-line configuration.
    - After sending the configuration, you should receive the configuration back from the system and note any new validation errors shown by Manager. For example, if using Embedded Voicemail, some sets of prompt languages may need to be updated to match the new configurations locale setting using the Add/Display VM Locales option.

Related Links

Editing Configuration Settings on page 169

Importing and Exporting Settings

Manager can import configuration settings created elsewhere. This can be useful when setting up a new system or sharing common settings such as a directory between systems.

The system supports LDAP (System | Directory Services | LDAP) for automatic importation of directory records (LDAP Version 2).

The system also supports HTTP (System | Directory Services HTTP) for automatic importation of directory records.

Settings are imported and exported in the following formats:

- **Binary Files (.exp)** These are non-editable files. During import and export it is possible to select what types of records should be included in the file. During import the whole file is imported.
- **Comma Separated Variable Text Files (.csv)** These are plain text files. In addition to being exported from a system these files can be created and edited using programs such as WordPad or Excel.

When opening a .csv file in Excel it will alter the way some data is displayed, automatically changing the display format of dates and long numbers such as phone numbers.

UTF-8 Character Encoding Manager imports and exports CSV files using UTF-8 character encoding which uses a multiple bytes to support characters with diacritic marks such as **ä**. Other applications, such as Excel, may, depending on the user PC settings, use different encoding which will cause such characters to be removed or corrupted. Care should be taken to ensure that any tool used to create or edit the CSV supports all the characters expected and uses UTF-8 format.

- **Importing into Manager from Excel** From Excel save the file as a .csv. This file will use ANSI character encoding. Open the file in Notepad and use the **Save As** option to rename the file and select UTF-8 encoding. Import the UTF-8 version of the file into Manager.
- **Exporting from Manager into Excel** Do not double-click on the file exported from Manager. Start Excel and use **File | Open** to select the file. Excel will recognize that the file uses UTF-8 encoding and will start its text file importation wizard. Follow the wizard instructions and select comma as the field delimiter.

CSV File Formats

The format is CSV using commas as field separator, no text delimiters and no header row. The simplest way to check the required format for a CSV file prior to import, is to export and a file from an existing system configuration.

File Name	Fields in Order
Directory	Name, Number, Speed Dial.
Hunt Group	Name, Extension, Group, Hunt, Rotary, Longest Waiting, Queuing On, Voicemail On, Broadcast, Voicemail Email.
Short Code	Code, Telephone Number, Feature.

Table continues…

File Name	Fields in Order
User	Name, Extension, User Rights, Email Address, Full Name, Password, VoiceMail Code, Login Code, UserTemplate, ExtensionTemplate.
Configuration	Proprietary format. Note that this does not contain all configuration fields.
License	License (ignored on import), License Key

Notes:

- **Hunt Group**: Apart from Name, Extension and Voicemail Email, the fields use a 1 or 0 value for on or off.
- **License**:
  - The License field is for information only and is ignored during import.
  - Following import the License name will appear as invalid with Manager. To resolve this save and then reload the configuration file.

The format of the system CSV is too complex to be described. It is a full export of all the system's configuration settings. This file format should only be used for export and import between systems and not for any offline editing.

Using the CSV Configurator spreadsheet

You can use the CSV Configurator spreadsheet to create or modify multiple user and extension configuration entries. The CSV Configurator spreadsheet is available:

- from the Avaya support site at support.avaya.com
- in the Manager install folder, for example `C:\Program Files (x86)\Avaya\IP Office \Manager`

1. Open Manager and create or load a configuration.
2. In the navigation pane on the left, right click **User** or **Extension** and select **New**.
3. In the new user or extension page, input all the desired template values.
4. In the group pane, right click the new user or extension and select **Export as Template (Binary)**.
5. In the Save As window, enter a file name.

User templates are saved with the file extension `.usr`. Extension templates are saved with file extension `.ext`.

On Windows XP systems, files must be saved to `Program Files\Avaya\IP Office\Manager \manager_files\template`.

On Windows 7 systems, the files must be saved to `Program Files (x86)\Avaya\IP Office \Manager\manager_files\template`

You can now use the exported file with the CSV Configurator spreadsheet. Follow the instructions in the spreadsheet.

Caution:

If you are working with an offline configuration, templates are stored on the local machine. If you close the Manager

application, the templates are deleted.

Related Links

Editing Configuration Settings on page 169

Exporting Settings

About this task

Procedure

1. Select **File | Import/Export...** from the menu bar.
2. Select **Export**.
3. Select the type of file.

   The list of exportable record types will change to match the file type.
4. Select the types of items that should be exported.
5. Use the Save In path to select the location for the exported files.

   The default location used is sub-directory of the Manager application directory based on system name of the currently loaded system.
6. Click **OK**.

Importing Settings will overwrite any existing records that match a record being imported

About this task

Procedure

1. Select **File | Import/Export...** from the menu bar.
2. Select **Import**.
3. Select the type of file.

   The list of items will change to match the type of file selected and whether a matching file or files is found in the current file path.
4. Use **Look In** to adjust the file path.

   The default location used is sub-directory of the Manager application directory based on system name of the currently loaded system.
5. Select the types of items that should be imported.

6. Click **OK**.

Copying and Pasting

Manager supports the normal Windows methods of cutting, copying, pasting and deleting records and settings. These can be accessed through the **Edit** menu in the menu bar or using the standard Windows keyboard shortcuts for those actions. They can also be accessed by selecting a record or text field and then right-clicking.

Copy and paste can be used with the navigation and group panes to create a new record with the same settings as the original. The copy will be renamed as **Copy of ...** to avoid conflicting with the original.

When using copy and paste between individual settings fields, whether on the same record or a different record, care should be taken to ensure that the fields use the same type of data. Similarly copying a record in the navigation or group pane and then pasting it into the details pane will prompt Manager to paste the copied records data into the first field of the current record in the details pane. As a general rule, cut and paste actions should be used with the same pane and within similar record types.

For users and user rights, a number of controls have been provided to copy settings between a user and a user right or vice versa. See User Rights Overview in the Configuration Settings section.

Related Links

Editing Configuration Settings on page 169

Saving a Configuration onto PC

The system configuration settings shown within Manager can be saved as a .cfg file on the Manager PC. These files can be used as backups or sent to other persons to aid problem diagnostics. Note however that an offline configuration file does not include the Audit Trail records for the system.

Automatically Saving Sent Configurations

By default, Manager creates a file copy of the configuration before it is sent to the system. This copy is stored in Manager's Working Directory using the system name and .cfg. This behavior is controlled by the Backup File on Send (File | Preferences | Security) option.

The number of backups of each systems configuration can be limited to a set number of the most recent copies.

Saving a Configuration Received from a System

Select **File | Save Configuration as** from the menu bar.

Saving a Configuration opened on the PC

Click in the main toolbar or select **File | Save Configuration** from the menu bar.

Related Links

Editing Configuration Settings on page 169

Sending a Configuration

The current configuration settings open within Manager can be sent to the system. The method depends on whether Manager is being used to edit the configuration of a single system or a network of systems.

Sending an Individual System Configuration

The first steps of this process depend on whether you are sending a configuration received from the system or sending one opened offline/created new.

- **A Configuration Opened from a System** Click in the main toolbar or select **File | Save Configuration** from the menu bar.
- **A Configuration Created Offline or Opened from a PC File** Select **File | Offline | Send Config** from the menu bar.

The **Send Configuration** menu is displayed.

Configuration Reboot Mode If Manager thinks the changes made to the configuration settings are mergeable, it will select **Merge** by default, otherwise it will select **Immediate**.

- **Merge** Send the configuration settings without rebooting the system. This mode should only be used with settings that are mergeable. Refer to Mergeable Settings.
- **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. This mode can be combined with the **Call Barring** options.
- **Timed** The same as **When Free** but waits for a specific time after which it then wait for there to be no calls in progress. The time is specified by the **Reboot Time**. This mode can be combined with the **Call Barring** options.
- **Reboot Time** This setting is used when the reboot mode **Timed** is selected. It sets the time for the system reboot. If the time is after midnight, the system's normal daily backup is canceled.
- **Call Barring** These settings can be used when the reboot mode **When Free** or **Timed** is selected. They bar the sending or receiving of any new calls.

Click **OK**. A service user name and password may be requested.

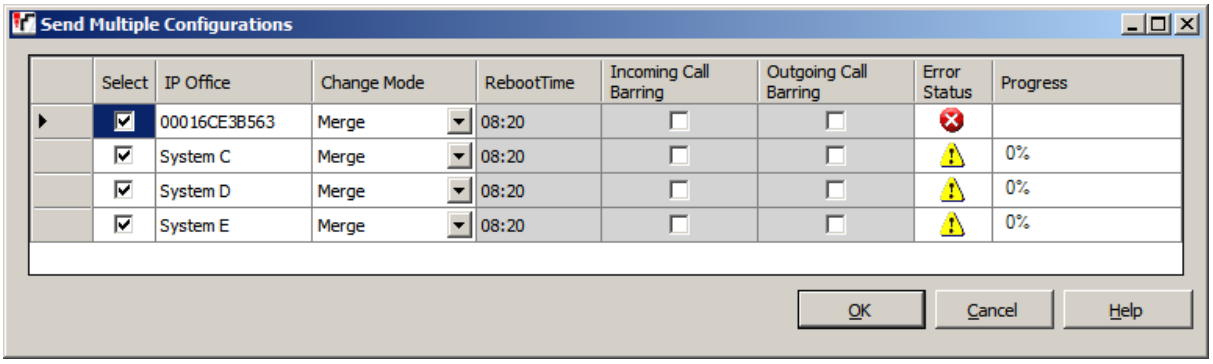
- If the service user name or password used do not valid, **"Access Denied"** is displayed.
- If the service user name used does not have rights to send a configuration or to request a reboot or merge, "Insufficient service user rights" is displayed.

- If the service user name used does not have operator rights to make the changes that have been made to the configuration, **"Insufficient operator rights. Operator cannot modify xxxx records"** is displayed.
- The warning will appear if the configuration being sent contain any errors indicated by a icon in the error pane. The configuration can still be sent by selected **Yes**.
- The message **Failed to save the configuration data. (Internal error)** may indicate that the IP500 V2 system has booted using software other than that in its System SD card's primary folder.

Sending Multiple Configurations

When Manager is running in Server Edition mode or SCN Management mode, it loads multiple configurations at the same time.

1. Click in the main toolbar or select **File | Save Configuration** from the menu bar.
2. The menu displayed only shows details for those systems where the system configuration has been changed and needs to be sent back to the system.



- **Select** By default all systems with configuration changes are selected. If you want to exclude a system from having its configuration updated, either deselect it or cancel the whole process.
- **Change Mode** If Manager thinks the changes made to the configuration settings are mergeable, it will select **Merge** by default, otherwise it will select **Immediate**.
- **Merge** Send the configuration settings without rebooting the system. This mode should only be used with settings that are mergeable. Refer to Mergeable Settings.
- **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. This mode can be combined with the **Incoming Call Barring** and **Outgoing Call Barring** options.
- **Store Offline** It is possible to add a reference for a Server Edition Secondary or for a Server Edition Expansion System to create a configuration file for that system even though it is not physically present. Store Offline saves that configuration on the Server Edition Primary in its file store. The same file is retrieved from there until such time as the physical server is present at which time you are prompted whether to use the stored file or the actual servers current configuration.

- **Timed** The same as **When Free** but waits for a specific time after which it then wait for there to be no calls in progress. The time is specified by the **Reboot Time**. This mode can be combined with the **Incoming Call Barring** and **Outgoing Call Barring** options.
- **Reboot Time** This setting is used when the reboot mode **Timed** is selected. It sets the time for the system reboot. If the time is after midnight, the system's normal daily backup is canceled.
- **Incoming Call Barring** This setting can be used when the reboot mode **When Free** or **Timed** is selected. It bars the receiving of any new calls.
- **Outgoing Call Barring** This setting can be used when the reboot mode **When Free** or **Timed** is selected. It bars the making of any new calls.

Click **OK**. The progress of the sending of each configuration is displayed.

Related Links

Editing Configuration Settings on page 169

Erasing the Configuration

About this task

The system configuration settings can be erased. During this process, the system is rebooted and starts with a set of default settings. This process does not erase the security settings of the system.

Erasing the Configuration

Procedure

1. Select **File | Advanced | Erase Configuration (Default)**.
2. Enter a valid user name and password.
3. The system will be rebooted.

Related Links

Editing Configuration Settings on page 169

Default Settings

The following applies to new systems and those defaulted using the Erase Configuration command. They also apply to IP500 V2 control units defaulted using the reset button on the rear of the unit (refer to the Installation manual for details of using the reset button).

Mode

IP500 V2 control units can operate in a number of modes. The initial mode is determined by the type of System SD card fitted and the level of software.

IP Office A-Law: A system fitted with this type of card will default to A-Law telephony. The system will default to IP Office Basic Edition - Quick Mode **PBX System** operation.

IP Office U-Law: A system fitted with this type of card will default to ULAW telephony. The system will default to IP Office Basic Edition - Quick Mode **Key System** operation.

IP Office Partner Edition: A system fitted with this type of card will default to A-Law telephony and IP Office Basic Edition - PARTNER® Mode operation.

IP Office Norstar Edition: A system fitted with this type of card will default to U-Law telephony and IP Office Basic Edition - Norstar® Mode operation.

Enterprise Branch: Use this option for an SD card intended to be used with an IP Office system running in Enterprise Branch Mode. There is a separate SD card for Enterprise Branch. The Enterprise Branch SD card can only be used for Enterprise Branch operation and cannot be used to change modes to IP Office. You also cannot use or change an IP Office SD card for use with an Enterprise Branch system.

⚠ Warning:

Do not re-purpose a Enerprise Branch card for use with any other IP Office mode. Doing so may damage the SD card and make it unusable for your Enterprise Branch system.

Default Short Codes

For IP500 V2 control units, A-Law or U-Law operation is determined by the Feature Key dongle installed in the system. Depending on the variant, a default system will use different sets of default short codes. See the Default System Short Code List.

Default Data Settings

When a new or defaulted control unit is switched on, it requests IP address information from a DHCP Server on the network. This operation will occur whether the LAN cable is plugged in or not.

If a DHCP server responds within approximately 10 seconds, the control unit defaults to being a DHCP client and uses the IP address information supplied by the DHCP server.

If no DHCP Server responds, the control unit still defaults to being the DHCP client but assumes the following default LAN addresses:

- For its LAN1 it allocates the IP address 192.168.42.1 and IP Mask 255.255.255.0.
- For its LAN2 if supported, it allocates the IP address 192.168.43.1 and IP Mask 255.255.255.0.

Once a control unit has obtained IP address and DHCP mode settings, it will retain those settings even if rebooted without a configuration file present on the System SD card. To fully remove the existing IP address and DHCP mode setting, the system must be defaulted using Manager.

Default Security Settings

Security settings are held separately from the configuration settings and so are not defaulted by actions that default the configuration. To return the security settings to their default values the separate Erase Security Settings command should be used.

Default Standard Mode Telephony Configuration Settings

A hunt group **Main** is created with extension number 200. The first 16 extensions on the systems are added to the group.

All physical extensions ports are numbered from extension number 201 upwards. A matching user record for each extension is also created.

A default incoming call route for all voice calls is created, with the default hunt group Main as its destination.

A default incoming call route for data calls is created with the default RAS record DialIn as its destination.

All lines are defaulted to Incoming Group ID and Outgoing Group ID of 0.

Default short codes are created based on whether the system's locale is A-Law or U-Law. See Default Short Codes.

Default Server Edition Telephony Configuration Settings

No users except **NoUser**.

All extensions are unnumbered.

No default hunt group or incoming calls routes are created.

All auto-create options are off by default.

Related Links

Editing Configuration Settings on page 169

Chapter 11: Configuration Mode Field Descriptions

This following sections detail the configuration settings for the different record types within the system. Depending on the type and locale of the system some settings and tabs may be hidden as they are not applicable. Other settings may be grayed out. This indicates that the setting is either for information only or that another setting needs to be enabled first.

Related Links

Configuration field display

The way that the system configuration settings are grouped and displayed in the navigation pane depends on whether Manager is running in its normal Standard mode or in Server Edition mode.

Related Links

[Configuration Mode Field Descriptions](#) on page 193
[Configuration field display in Standard mode](#) on page 194
[Configuration field display in Server Edition mode](#) on page 195

Configuration field display in Standard mode

This order of display of different types of configuration record is used for Standard mode systems.

 System Overall settings for the data and telephony operation of the system.

 Line Settings for trunks and trunk channels within the system.

 Control Unit Information summary of the system.

 Extension Settings for extension ports.

 User Settings for each system user. They may or may not be associated with an extension.

 Hunt Group Collections of users to which calls can be directed for answer by any one of those users.

 Short Code These are numbers which when dialed trigger specific features or are translated for external dialing. Short codes can be set at both the system wide level and locally for a particular system.

 Service Configuration settings such as user names and passwords needed for connections to data services such as the Internet.

 RAS Remote Access Service settings for connecting incoming data calls.

 Incoming Call Route Records here are used to match incoming call details on external trunks to destinations on the system.

 WAN Port Configuration settings for the WAN ports provided on some units.

 Directory External names and numbers. Used for matching names to incoming calls and for dialing from user applications.

 Time Profile Used to control when various functions are active.

 Firewall Profile Use to control the types of data traffic that can cross into or out of the system.

 IP Route These records are used to determine where data traffic on the system should be routed.

 Account Code Used for call logging and to control the dialing of certain numbers.

 License License keys are used to enable system features and applications.

 Tunnel Used to created IPSec and L2TP data tunnels.

 User Rights Provide templates to control the settings applied to associated users.

 Auto Attendant Used when an Avaya memory card is installed in the control unit.

 ARS Automatic Route Selection is used by to control outgoing external calls.

 Authorization Codes Authorization codes are similar to account codes. However, unlike account codes which are usable by any user, each authorization code is only usable by a specific user or users associated with a specific set of user rights.

Related Links

Configuration field display on page 194

Configuration field display in Server Edition mode

When Manager is being used in Server Edition mode, the navigation pane works in the same way as normal. However, the different types of configuration records are ordered and grouped differently. This reflects the fact that some types of record are automatically shared across all systems in the network.

Solution settings

The first 8 types are records have special behaviors that are different from normal records stored in the configurations of individual systems in the network.

 User These records show settings for system users. Each user may or may not be associated with an extension. All the users configured on all systems are grouped here to allow easy configuration access. The individual user records are still stored in the configuration of the particular

system on which the user was created and can also be accessed through that system's configuration settings. New users are created through the **User** settings of the system that hosts the user.

 Hunt Group These records are groups of users to which calls can be directed for answering by any one of those users. Hunt group records are stored in the configuration of the Primary Server but those hunt groups are advertised for use by all systems in the network.

 Directory External names and numbers. These records are used to match names to incoming calls and for making calls by name selection from the directory on phones or in applications. These directory records are stored in the configuration of the Primary Server. By default all other systems in the network automatically import a copy of the Primary Server system directory at regular intervals.

By default, the following types of records are all shared and replicated by each system in the network and cannot be set at an individual system level. That operation can be changed using the consolidation settings.

 Short Code These are numbers which when dialed trigger specific features or are translated for external dialing. These short codes are common to all systems in the network.

 Incoming Call Route Records set here are used to match incoming call details on external trunks to destinations. These incoming call routes are shared by all systems in the network.

 Time Profile Used to control when various functions are active. The time profiles set here are shared by all systems in the network.

 Account Code Used for call logging and to control the dialing of certain numbers. The account codes set here are shared by all systems in the network.

 User Rights Provide templates to control the settings applied to users associated with a particular set of user rights. These user rights are shared and replicated on all systems in the network.

Individual system settings

In addition to the settings above, a range of other types of record can be configured for each individual system in the network. Visibility and configuration of **Short Code**, **Incoming Call Route**, **Time Profile**, **Account Code** and **User Rights** records is dependent on the consolidation settings of Manager.

 System A system icon is shown for each system in the network. That is, one for the Primary Server, one for the the Secondary Server if installed and one for each Expansion System (L) and Expansion System (V2) systems. Each can be expanded to allow configuration of records that are particular to that system.

-  Line Settings for trunks and trunk channels within the system.
-  Control Unit Information summary of the system.

-  Extension Settings for extension ports.
-  User Settings for each system user. They may or may not be associated with an extension.
-  Short Code These are numbers which when dialed trigger specific features or are translated for external dialing.
-  Service Configuration settings such as user names and passwords needed for connections to data services such as the Internet.
-  RAS Remote Access Service settings for connecting incoming data calls.
-  WAN Port Configuration settings for the WAN ports provided on some units.
-  Firewall Profile Use to control the types of data traffic that can cross into or out of the system.
-  IP Route These records are used to determine where data traffic on the system should be routed.
-  License License keys are used to enable system features and applications.
-  Tunnel Used to created IPSec and L2TP data tunnels.
-  ARS Automatic Route Selection is used by to control outgoing external calls.
-  Authorization Codes Authorization codes are similar to account codes. However, unlike account codes which are usable by any user, each authorization code is only usable by a specific user or users associated with a specific set of user rights.

Related Links

Configuration field display on page 194

BOOTP | BOOTP Record

The BOOTP settings are used by the Manager application itself. They are not system configuration settings.

BOOTP is protocol used by devices to request software when restarting. It is used when upgrading the control unit within a system or when the core software within the control unit has been erased.

When running, Manager can respond to BOOTP requests and, if it finds a matching BOOTP record for the system, provide the software file indicated by that record.

BOOTP records are not part of a system's configuration settings, they are items saved on the Manager PC. Normally Manager automatically creates a BOOTP record for each system with which it has communicated, up to a maximum of 50 records. However BOOTP records can be added and edited manually when necessary.

Field	Description
File Location	The location from which Manager provides files in response to BOOTP is its binaries directory. This can be changed using **File** > **Change Working Directory** or **File** > **Preferences** > **Directories**. This directory is also the directory used by Manager when providing files by TFTP.
Disabling BOOTP	Manager can be disabled from providing BOOTP support for any systems. Select**File** > **Preferences** > **Preferences** > **Enable BOOTP and TFTP Server**.
Enabled	Default = Enabled If unchecked, BOOTP support for the matching system from this Manager PC is disabled.
System Name	This field is not changeable. It shows the system name.
MAC Address	The MAC address of the system. The address can be obtained and or verified in a number of ways: • When a system's configuration settings are loaded into Manager, it is shown as the Serial Number on the Unit form. On defaulted systems, it is also used as the system name. • If the system is requesting software, the MAC address is shown as part of the request in the status bar at the base of the Manager screen. • If the system can be pinged, it may be possible to obtain its MAC address using the command **arp -a <ip address>**.
IP Address	The IP address of the system's LAN1.
Filename	The name of the .bin software file used by that type of control unit. To be transferred to the system, this file must exist in the Manager applications **Working Directory**.
Time Offset	**:** Default = 0. In addition to performing BOOTP support for systems, the Manager application can also act as a time server (RFC868). This field sets the offset between the time on the PC running Manager and the time sent to the system in response to its time requests. The field is not used if a specific Time Server IP Address is set through the **System** form in the system's configuration settings. Manager can be disabled from acting as an Internet Time (RFC868) server. Select**File** > **Preferences** > **Preferences** and uncheck **Enable time server**.

Related Links

Configuration Mode Field Descriptions on page 193

System

Configuration overview

There is one System record for each system being managed. When using Manager in Server Edition or Small Community Network Management modes, clicking on the **System** icon for a particular system displays a system inventory page for that system.

The following tabs are part of the **System** configuration.

Tab	Description
System	General settings for the system.
LAN1	Network settings for the RJ45 Ethernet LAN port on the control unit.
LAN2	Network settings for the RJ45 Ethernet WAN port on the control unit.
DNS	Specify the Domain Name Server addresses to use for address resolution.
Voicemail	Details the type and location of the voicemail server.
Telephony	System-wide telephony settings.
Directory Services	Settings to allow the system to import directory numbers from other sources.
System Events	Simple Network Management Protocol (SNMP), email (SMTP), and Syslog settings for the sending of system events.
SMTP	Settings for SMTP email sending from the system.
Twinning	System wide controls for the use of Mobile Twinning.
SMDR	Settings for the sending of call records to a specified IP address.
CCR	This tab is used for settings specific to the Customer Call Reporter (CCR) application. Not supported in multi-site networks.

Related Links

Configuration Mode Field Descriptions on page 193
System | System on page 200
System | LAN1 on page 205
System | LAN2 on page 215
System | DNS on page 216
System | Voicemail on page 217
System | Telephony on page 224
System | Directory Services on page 249
System | System Events on page 253
System | SMTP on page 260
System | SMDR on page 261
System | Twinning on page 262

System | System

These settings are mergeable. However, changes to **Locale** or **Favor RIP Routes over Static Routes** require a reboot.

Field	Description
Name	Default: = System MAC Address. A name to identify this system. This is typically used to identify the configuration by the location or customer's company name. Some features such as Gatekeeper require the system to have a name. This field is case sensitive and within any network of systems must be unique. Do not use <, >, |, \0, :, *, ?, . or /.
Contact Information	Default = Blank. This field is only be edited by service user with administrator rights. If Contact Information is entered, it will set the system under 'special control'. If the contact information is set using a standalone version of Manager, warnings that "This configuration is under special control" are given when the configuration is opened again. This can be used to warn other users of Manager that the system is being monitored for some specific reason and provide them with contact details of the person doing that monitoring. See Loading a Configuration.
Locale	Sets default telephony and language settings based on the selection. It also sets various external line settings and so must be set correctly to ensure correct operation of the system. See Supported Country and Locale Settings. For individual users, the system settings can be overridden through their own locale setting Select **User** > **User** > **Locale**.
Location	Default = None. Specify a location to associate the system with a physical location. Associating a system with a location allows emergency services to identify the source of an emergency call. The drop down list contains all locations that have been defined in the Location page.
Customize Locale Settings The **Customize** locale matches the Saudi Arabia locale but with the following additional controls shown below. For other locales, these are set on the **System** > **Telephony** > **Tones and Music** tab.	
Tone Plan	Default = Tone Plan 1 The tone plan control tones and ringing patterns. The options are: • **Tone Plan 1**: United States. • **Tone Plan 2**: United Kingdom.

Table continues…

Field	Description
	• **Tone Plan 3**: France. • **Tone Plan 4**: Germany. • **Tone Plan 5**: Spain.
CLI Type	Used to set the CLI detection used for incoming analogue trunks. The options are: • **DTMF** • **FSK V23** • **FSK BELL202**
Device ID	Server Edition Only. Displays the value set for **Device ID** on the System | System Events | Configuration tab. If an SSL VPN is configured, Avaya recommends that the Device ID match an SSL VPN service Account Name. Each SSL VPN service account name has an associated SSL VPN tunnel IP address. Having the displayed Device ID match an SSL VPN service account name helps identify a particular SSL VPN tunnel IP address to use for remotely managing IP Office.
TFTP Server IP Address	Default = 0.0.0.0 (Disabled). While running, Manager can act as a TFTP server and provides files from its configured binaries directory. To set the address to broadcast, use the value 255.255.255.255. TFTP can also be disabled through the Enable BootP and TFTP Servers command. On Server Edition Systems, the default setting on the Primary Server is 0.0.0.0 (disabled). The default setting on Secondary and Expansion servers is the address of the Primary Server. For Avaya IP phones using the system for DHCP, the address set here is used when they make TFTP requests for software and settings files. On systems with an Avaya memory card, the LAN1 IP Address can be entered to specify that memory card as the TFTP file source. The files required for download must be transferred onto the card using either TFTP from the PC command line (see **File Writer IP Address** below) or through Embedded File Management. 1100, 1200, 1600 and 9600 Series IP phones do not support TFTP and require an HTTP Server IP Address (see below) to be specified. This address is only used in DHCP responses if the **Phone File Server Type** is set to **Custom**.
HTTP Server IP Address	Default = 0.0.0.0 (Disabled). For Avaya IP phones using the system for DHCP, the address set here is used when they make HTTP requests for software and settings files. The files for download should be placed in the HTTP server's root directory. Using the system's own memory card is supported as the source for HTTP files. This is supported for up to 50 IP phones total. This is done by setting the **TFTP Server IP Address** and **HTTP Server IP Address** to match the system IP address. HTTP-TFTP Relay is support using Manager as the TFTP server (not supported by Linux based systems). This is done by setting the **TFTP Server IP Address** to the address of

Table continues…

Field	Description
	the Manager PC and the **HTTP Server IP Address** to the control unit IP address. This method is supported for up to 5 IP phones total. This address is only used in DHCP responses if the **Phone File Server Type** (see below) is set to **Custom**.
Phone File Server Type	Default = Memory Card (Disk on a Linux system). For IP (H.323 and SIP) phones using the system as their DHCP server, the DHCP response can include the address of a file server from which the phone should request files. The setting of this field controls which address is used in the DHCP response. The options are: • **Custom**: The DHCP response provided to phones it is supporting contains the TFTP Address from the **TFTP Server IP Address** above and the HTTP Address from the **HTTP Server IP Address** above. • **Memory Card** (**Disk** on a Linux system): The system will respond to file requests from phones using files on its own memory card. The DHCP response provided to phones it is supporting contains the LAN address of the system for both TFTP and HTTP address. • **Manager**: The system will forward any H.323 phone file request to the configured **Manager PC IP Address** set below. HTTP-TFTP relay is used for HTTP requests. The DHCP response provided to phones the system is supporting contains the LAN address of the system for the HTTP Address. This option is not supported for Linux based systems.
HTTP Redirection	Default = Off. Allows for the use of an alternate HTTP file server for the download of large binary files. This field is available when the **Phone File Server Type** is set to **Memory Card** (or **Disk** on a Linux system). When this field is set to **Phone Binaries**, 96x1 H.323 phones requesting their binary files are redirected to the HTTP server defined in the **HTTP Server IP Address** field.
Manager PC IP Address	Default = 0.0.0.0 (Broadcast). This address is used when the **Phone File Server Type** is set to **Manager**.
Avaya HTTP Clients Only	Default = Off. When selected, the system only responds to HTTP requests from sources it identifies as another system, an Avaya phone or application.
Enable SoftPhone HTTP Provisioning	Default = Off. This option must be enabled if the IP Office Video Softphone is being supported.
Favour RIP Routes over Static Routes	Default = Off RIP can be enabled on the system LAN1 and LAN2 interfaces, and on specific Services. When this setting is on, the RIP route to a destination overrides any static route to the same destination in the system's IP Routes, regardless of the RIP route's metric. The only exception is RIP routes with a metric of 16 which are always ignored.

Table continues…

Field	Description
	Note: If a previously learnt RIP route fails, the system applies a metric of 16 five minutes after the failure. When off, any RIP route to a destination for which a static route has been configured is ignored. This option is not supported on Linux based systems.
Automatic Backup	Default = On. This command is available with IP500 V2 systems. When selected, as part of its daily backup process, the system automatically copies the folders and files from the **System SD** card's `/primary` folder to its `/backup` folder. Any matching files and folders already present in the **/backup** folder are overwritten.
Provider	Default = Not visible. This field is visible only if the system has been branded by addition of a special license for a specific equipment provider. The branding is fixed, that is it remains even if the license is subsequently removed. The number shown is a unique reference to the particular equipment provider for whom the system has been branded. When branded, the equipment provider's name is displayed on idle phone displays and other provider related features are enabled.
Time Setting Config Source	The time is either set manually (see Date and Time), obtained using Time protocol (RFC868) requests or obtained using Network Time Protocol (RFC958) request. This field is used to select which method is used and to apply ancillary settings based on the selected method. For Server Edition networks, the Primary Server is defaulted to use **SNTP** to **0.pool.ntp.org** to obtain its time and date. The Secondary Server and expansion servers are defaulted to use **SNTP** to obtain their time from the Primary Server. For other IP Office systems the default is **Voicemail Pro/Manager**. This option should not be used with Server Edition systems and systems with a Unified Communication Module as in those scenarios, the voicemail server is being hosted by and getting its time from the same server as the IP Office. • **None**, the system to not make any time requests. The system time and date needs to be set using a phone with **System Phone Rights** (User | User). The system can then automatically apply daylight saving settings to the manually set time. • **Voicemail Pro/Manager** Both the Voicemail Pro service and the Manager program can act as RFC868 Time servers for the system. Use of other RFC868 server sources is not supported. They provide both the UTC time value and the local time as set on the PC. The system makes a request to the specified address following a reboot and every 8 hours afterwards. This option should not be used with Server Edition systems and systems with a Unified Communication Module as in those scenarios the voicemail server is being hosted by and getting its time from the same server as the IP Office. - **IP Address**: Default = 0.0.0.0 (Broadcast) The address to which the RFC868 request is sent. 0.0.0.0 means default operation. In this mode, following a reboot the control unit will send out a time request on its LAN interfaces. It first makes the request to the Voicemail Server IP address in its configuration if set and, if it receives no reply, it then makes a broadcast request.

Table continues…

Field	Description
	- **Time Offset**: Default = 00:00 This value is not normally set as any time changes, including daylight saving changes, that occur on the PC will be matched by the system. If you are running Manager when the voicemail server starts, voicemail does not start as a time server. It is therefore recommended that you have no copy of Manager running when you start or restart the voicemail server. Manager can be disabled from acting as a RFC868 time server by deselecting the **Enable Time Server** option (File | Preferences | Edit | Preferences). • **SNTP**: Use a list of SNTP servers to obtain the UTC time. The records in the list are used one at a time in order until there is a response. The system makes a request to the specified addresses following a reboot and every hour afterwards.
Time Settings	
Time Server Address	Default = Blank Enter a list of IP addresses, host names, or fully qualified domain names (FQDN) for the SNTP servers. Separate each record with a space. The use of broadcast addresses is not supported. The list is used in order of the records until a response is received.
Time Offset	Default = 00:00 This setting is used to set the local time difference from the UTC time value provided by an SNTP server. For example, if the system is 5 hours behind UTC, this field should be configured with **-05:00** to make the adjustment. The time offset can be adjusted in 15 minute increments. If also using the daylight time saving settings below, use this offset to set the non-DST local time.
File Writer IP Address	Default = 0.0.0.0 (Disabled) This field set the address of the PC allowed to send files to the System SD card installed in the system using HTTP or TFTP methods other than embedded file management.On systems with an Avaya memory card, this field sets the address of the PC allowed to send files to the memory card using HTTP or TFTP methods other than embedded file management. For Linux based systems it is applied to non-embedded file management access to the /opt/ipoffice folder on the server. An address of 255.255.255.255 allows access from any address. If embedded file management is used, this address is overwritten by the address of the PC using embedded file management (unless set to 255.255.255.255).
Dongle Serial Number	This field is for information only. It shows the serial number of the feature key dongle against which the system last validated its licenses. **Local** is shown for a serial port, Smart Card or System SD feature key plugged directly into the control unit. **Remote** is shown for a parallel or USB feature key connected to a feature Key Server PC. For IP500 V2 systems, the serial number is printed on the System SD card and prefixed with **FK**. For Linux based telephone systems this field is replaced by the **System Identification** field below.
AVPP IP Address	Default = 0.0.0.0 (Disabled) Where Avaya 3600 Series SpectraLink wireless handsets are being used with the system, this field is used to specify the IP address of the Avaya Voice Priority Processor (AVPP)

Related Links

System on page 199

System | LAN1

This tab is used to configure the behavior of the services provided by the system's first LAN interface.

Up to 2 LAN's (LAN1 and LAN2) can be configured. The control unit has 2 RJ45 Ethernet ports, marked as LAN and WAN. These form a full-duplex managed layer-3 switch. Within the system configuration, the physical LAN port is LAN1, the physical WAN port is LAN2.

Related Links

System on page 199
LAN Settings on page 205
VoIP on page 206
Network Topology on page 211
DHCP Pools on page 214

LAN Settings

This form is used to set the general LAN settings for the LAN interface such as the IP address mode.

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

Field	Description
IP Address	Default = 192.168.42.1 or DHCP client. This is the IP address of the Control Unit on LAN1. If the control unit is also acting as a DHCP server on the LAN, this address is the starting address for the DHCP address range.
IP Mask	Default = 255.255.255.0 or DHCP client. This is the IP subnet mask used with the IP address.
Primary Trans. IP Address	Default = 0.0.0.0 (Disabled) This setting is only available on control units that support a LAN2. Any incoming IP packets without a service or session are translated to this address if set.
RIP Mode	Default = None. Routing Information Protocol (RIP) is a method by which network routers can exchange information about device locations and routes. Routes learnt using RIP are known as 'dynamic routes'. The system also supports 'static routes' though its IP Route records. For Server Edition systems this setting is only available on Expansion System (V2) systems. The options are: • **None**: The LAN does not listen to or send RIP messages

Table continues…

Field	Description
	• **Listen Only (Passive)**: Listen to RIP-1 and RIP-2 messages in order to learn RIP routes on the network. • **RIP1**: Listen to RIP-1 and RIP-2 messages and send RIP-1 responses as a sub-network broadcast. • **RIP2 Broadcast (RIP1 Compatibility)**: Listen to RIP-1 and RIP-2 messages and send RIP-2 responses as a sub-network broadcast. • **RIP2 Multicast**: Listen to RIP-1 and RIP-2 messages and send RIP-2 responses to the RIP-2 multicast address.
Enable NAT	Default = Off This setting controls whether NAT should be used for IP traffic from LAN1 to LAN2. This setting should not be used on the same LAN interface as a connected WAN3 expansion module.
Number of DHCP IP Addresses	Default = 200 or DHCP client. See Default Settings. Range = 1 to 999. This defines the number of sequential IP addresses available for DHCP clients.
DHCP Mode	Default = DHCP Client. This controls the control unit's DHCP mode for the LAN. When doing DHCP: • LAN devices are allocated addresses from the bottom of the available address range upwards. • Dial In users are allocated addresses from the top of the available range downwards. • If the control unit is acting as a DHCP server on LAN1 and LAN2, Dial in users are allocated their address from the LAN1 pool of addresses first. The options are: • **Server**: When this option is selected, the system will act as a DHCP Server on this LAN, allocating address to other devices on the network and to PPP Dial in users. • **Disabled** When this option is selected, the system will not use DHCP. It will not act as a DHCP server and it will not request an IP address from a DHCP server on this LAN. • **Dial In** When this option is selected, the system will allocate DHCP addresses to PPP Dial In users only. On systems using DHCP pools, only addresses from a pool on the same subnet as the system's own LAN address will be used. • **Client** When this option is selected, the system will request its IP Address and IP Mask from a DHCP server on the LAN. • **Advanced**: (IP500 V2 only). The system can be configured with a number of DHCP Pools from which it can issue IP addresses.

Related Links

System | LAN1 on page 205

VoIP

This form is used to set the system defaults for VoIP operation on the LAN interface.

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

Note:

Under **SIP Registrar Enable**, the **Auto-create Extn/User** setting is mergeable. Changing this setting does not require a reboot.

Field	Description
H.323 Gatekeeper Enable	Default = On This settings enables gatekeeper operation.
H.323 Auto-create Extn	Default = Off When this option is on, an extension record is automatically created for H.323 phones registering themselves with the system as their gatekeeper. SIP Extensions use a separate setting. If using resilience backup to support Avaya IP phones, **Auto-create Extn** and **Auto-create User** should not be left enabled after initial configuration or any subsequent addition of new extensions and users. Leaving auto-create options enabled on a system that is a failover target may cause duplicate extension/user records on the multi-site network under multiple failure scenarios.
H.323 Auto-create User	Default = Off When this option is on and **H.323 Auto-create Extn** is also on, when a new H.323 extension is created a matching user record is also created.
H.323 Remote Extn Enable	Default = Off. The system can be configured to support remote H.323 extensions in the case where NAT is used in the connection path. This could be the case where the IP Office is located behind a corporate NAT/Firewall router and/or the H.323 phone is located behind residential NAT enable router. The use of this option and the interaction and configuration of external third party elements is beyond the scope this help file. In the case where the public IP address of the corporate router is unknown, the LAN's Network Topology settings should be used to configure a STUN Server. Enabling the Allow Remote Extn option also makes visible the configuration of the RTP Port number Range (NAT) settings below. This option is not supported if the **Firewall/NAT Type** (System | LAN1 | Network Topology) is set to **Symmetric Firewall** or **Open Internet**. Currently, only 9600 Series phones are supported as H.323 remote extensions.
SIP Trunks Enable	Default = On This settings enables support of SIP trunks. It also requires entry of **SIP Trunk Channels** licenses.
SIP Registrar Enable	Default = Off. Used to set the system parameters for the system acting as a SIP Registrar to which SIP endpoint devices can register. Separate SIP registrars can be configured on LAN1 and

Table continues…

Field	Description
	LAN2. Registration of a SIP endpoint requires an available **IP Endpoints** license. SIP endpoints are also still subject to the extension capacity limits of the system.
Auto-create Extn/User	Default = Off. If on, a new extension and user records are created by the registration of a new SIP endpoint. If off, SIP endpoint can only register against existing configuration records. If a password is requested by a SIP device during registration to create a new user and extension records in the system configuration, **0000** should be used. If registering against an existing user record, the user **Login Code** should be used if set or **0000** if the user does not have a **Login Code** set. **Note:** This setting is not applicable to the Avaya A175 Desktop Video Device with the Avaya Communicator.
SIP Remote Extn Enable	Default = Off. The system can be configured to support remote SIP extensions in the case where NAT is used in the connection path. This could be the case where the IP Office is located behind a corporate NAT/Firewall router and/or the SIP phone is located behind residential NAT enable router. This option cannot be enabled on both LAN1 and LAN2. The use of this option and the interaction and configuration of external third party elements is beyond the scope this help file. In the case where the public IP address of the corporate router is unknown, the LAN's Network Topology settings should be used to configure a STUN Server. Enabling the SIP Remote Extn Enable option also makes visible the configuration of the Remote UDP Port, Remote TCP Port, Remote TLS Port settings below. Currently, only Avaya Communicator for Windows, Avaya Communicator for iPad, one-X Mobile iOS and one-X Mobile Android SIP clients are supported as SIP remote extensions.
Domain Name	Default = Blank This is the local SIP registrar domain name that will be needed by SIP endpoints in order to register with the system. If this field is left blank, registration is against the LAN IP address.
Layer 4 Protocol	Default = TCP and UDP. This field is used to select which protocosl are supported for SIP connections: TCP, UDP, or TLS. • **UDP Port**: Default = 5060. The port to use for SIP UDP support if UDP is selected as the **Layer 4 Protocol** above. • **TCP Port**: Default = 5060. The port to use for SIP TCP support if TCP is selected as the **Layer 4 Protocol** above. • **TLS Port**: Default = 5061. The port to use for SIP TLS support. • **Remote UDP Port**: Default = 5060. The port to use for SIP UDP support if UDP is selected as the Layer 4 Protocol for remote SIP extension. • **Remote TCP Port**: Default = 5060. The port to use for SIP TCP support if TCP is selected as the Layer 4 Protocol for remote SIP extension.

Table continues…

Field	Description
	• **Remote TLS Port**: Default = 5061. The port to use for SIP TLS support if TLS is selected as the Layer 4 Protocol for remote SIP extension.
Challenge Expiry Time (secs)	Default = 10. The challenge expiry time is used during SIP extension registration. When a device registers, the system SIP Registrar will send a challenge back to the device and waits for an appropriate response. If the response is not received within this timeout the registration is failed.
RTP	
Port Number Range	For each VoIP call, a receive port for incoming Real Time Protocol (RTP) traffic is selected from a defined range of possible ports, using the even numbers in that range. The Real Time Control Protocol (RTCP) traffic for the same call uses the RTP port number plus 1, that is the odd numbers. For control units and Avaya H.323 IP phones, the default port range used is 49152 to 53246. On some installations, it may be a requirement to change or restrict the port range used. It is recommended that only port numbers between 49152 and 65535 are used, that being the range defined by the Internet Assigned Numbers Authority (IANA) for dynamic usage. **Important:** The minimum and maximum settings of the port range should only be adjusted after careful consideration of the customer network configuration and existing port usage. For pre-Release 8.1 systems, the gap between the minimum and maximum port values must be at least 1024. For Release 8.1 and higher, the gap between the minimum and maximum port values must be at least 254.
Port Range (minimum)	IP 500 v2 default = 4000. Range = 46750 to 50750. Linux default = 10000. Range = 40750 to 50750 This sets the lower limit for the RTP port numbers used by the system.
Port Range (maximum)	IP 500 v2 default = 4000. Range = 46750 to 50750. Linux default = 10000. Range = 40750 to 50750 This sets the upper limit for the RTP port numbers used by the system.
Port Number Range (NAT)	
Port Range (minimum)	Default = 49152. Range = 1024 to 65280.
Port Range (maximum)	Default = 53246. Range = 1278 to 65534.
Enable RTCP Monitor On Port 5005	Default = On. For 1600, 4600, 5600 and 9600 Series H.323 phones, the system can collect VoIP QoS (Quality of Service) data from the phones. For other phones, including non-IP phones, it can collect QoS data for calls if they use a VCM channel. The QoS data collected by the system is displayed by the System Status Application. This setting is mergeable. However it only affects H.323 phones when the register with the system. therefore any change to this setting requires H.323 phones that have already been

Table continues…

Field	Description
	registered to be rebooted. Avaya H.323 phones can be remotely rebooted using the System Status Application. The QoS data collected includes: RTP IP Address, Codec, Connection Type, Round Trip Delay, Receive Jitter, Receive Packet Loss. This setting is not the same as the RTCPMON option within Avaya H.323 phone settings. The system does not support the RTCPMON option.
RTCP Collector IP address for phones	Default = Blank. This setting defines an alternate destination for the RTCP Monitor data described in the **Enable RTCP Monitor On Port 5005** field above. This enables you to send the data collected to a third party QoS monitoring application. The **Enable RTCP Monitor On Port 5005** must be turned Off to enable this field. Changes to this setting requires a reboot of the phones.
Keepalives These settings can be used with SIP trunks associated with the LAN through their **Use Network Topology Info** setting (Line | Transport). For some scenarios, with frequent call forwarding on the same SIP trunk, speech path may be lost during the connection. The use of periodic keepalive packets may prevent the issue.	
Scope	Default = Disabled Select whether the sending of keepalive packets should be disabled or sent for RTP or for both RTP and RTCP.
Periodic timeout	Default = 0 (Off). Range = 0 to 180 seconds. Sets how long the system will wait before sending a keepalive if no other packets of the select **SCOPE** are seen.
Initial keepalives	Default = Disabled. If enabled, keepalives can also been sent during the initial connection setup.
DiffServ Settings When transporting voice over low speed links it is possible for normal data packets (1500 byte packets) to prevent or delay voice packets (typically 67 or 31 bytes) from getting across the link. This can cause unacceptable speech quality. Therefore it is important that all traffic routers and switches in a network to have some form of Quality of Service mechanism (QoS). QoS routers are essential to ensure low speech latency and to maintain sufficient audible quality. The system applies the DiffServ settings to outgoing traffic on any SIP lines which have their **User Network Topology Info** setting (Line | Transport) set to match the LAN interface. DiffServ settings are not applied to any other traffic on the systems LAN interface. The system does not use DiffServ markings used to prioritize traffic on its LAN interface. The system supports the DiffServ (RFC2474) QoS mechanism. This uses a Type of Service (ToS) field in the IP packet header. The system uses this field to prioritize voice and voice signaling packets on its WAN interfaces. Note that the system does not perform QoS for its Ethernet ports. The hex and decimal entry fields for the following values are linked, the hex value being equal to the decimal multiplied by 4.	

Table continues…

Field	Description
DSCP (Hex)	Default = B8 (Hex)/46 (decimal). Range = 00 to FC (Hex)/0 to 63 (decimal) The DiffServ Code Point (DSCP) setting applied to VoIP calls. By default, the same setting is used for audio and video. If desired, you can configure separate values for audio and video. For correct operation, especially over WAN links, the same value should be set at both ends.
Video DSCP (Hex)	Default = B8 (Hex)/46 (decimal). Range = 00 to FC (Hex)/0 to 63 (decimal) The DiffServ Code Point (DSCP) setting applied to video VoIP calls. For correct operation, especially over WAN links, the same value should be set at both ends.
DSCP Mask (Hex)	Default = FC (Hex)/63 (decimal). Range = 00 to FC (Hex)/0 to 63 (decimal) Allows a mask to be applied to packets for the DSCP value.
SIG DSCP (Hex)	Default = 88 (Hex)/34 (decimal). Range = 00 to FC (Hex)/0 to 63 (decimal) This setting is used to prioritize VoIP call signaling.
DHCP Settings	
Primary Site Specific Option Number (SSON)	Default = 176. Range = 128 to 254. A site specific option number (SSON) is used as part of DHCP to request additional information. 176 is the default SSON used by 4600 Series and 5600 Series IP phones.
Secondary Site Specific Option Number (SSON)	Default = 242. Range = 128 to 254. Similar to the primary SSON. 242 is the default SSON used by 1600 and 9600 Series IP phones requesting installation settings via DHCP.
VLAN	Default = Not present. This option is applied to H.323 phones using the system for DHCP support. If set to **Disabled**, the L2Q value indicated to phones in the DHCP response is 2 (disabled). If set to **Not Present**, no L2Q value is included in the DHCP response.
1100 Voice VLAN Site Specific Option Number (SSON)	Default = 232. This is the SSON used for responses to 1100/1200 Series phones using the system for DHCP.
1100 Voice VLAN IDs	Default = Blank. For 1100/1200 phone being supported by DHCP, this field sets the VLAN ID that should be provided if necessary. Multiple IDs (up to 10) can be added, each separated by a + sign.

Related Links

System | LAN1 on page 205

Network Topology

STUN (Simple Traversal of UDP through NAT) is a mechanism used with overcome the effect of NAT firewalls. The network address translation (NAT) action performed by this type of firewall can have negative effects on VoIP calls.

Test packets are sent by the system to the address of the external STUN server, those packets crossing the firewall in the process. The STUN server replies and includes copies of the packets it received in the reply. By comparing the packet sent and received, it is possible for the system to

determine the type of NAT firewall and to modify future packets to overcome the effects of the firewall.

These settings are used for SIP trunk connections from the LAN. For further details of system SIP operation refer to the SIP Line section. The use of STUN is unnecessary if the SIP ITSP uses a Session Border Controller (SBC). Use of SIP requires entry of SIP Trunk Channels licenses.

The network topology settings are also used for H.323 remote extensions supported on the LAN.

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

The following fields can be completed either manually or the system can attempt to automatically discover the appropriate values. To complete the fields automatically, only the STUN Server IP Address is required. STUN operation is then tested by clicking Run STUN. If successful the remaining fields are filled with the results.

Field	Description
STUN Server IP Address	Default = Blank Enter the IP address or fully qualified domain name (FQDN) of the SIP ITSP's STUN server. The system will send basic SIP messages to this destination and from data inserted into the replies can try to determine the type NAT changes being applied by any firewall between it and the ITSP.
STUN Port	Default = 3478. Defines the port to which STUN requests are sent if STUN is used.
Firewall/NAT Type	Default = Unknown The settings here reflect different types of network firewalls. The options are: • **Blocking Firewall** • **Symmetric Firewall**: SIP packets are unchanged but ports need to be opened and kept open with keep-alives. If this type of NAT is detected or manually selected, a warning 'Communication is not possible unless the STUN server is supported on same IP address as the ITSP' will be displayed as part of the manager validation. • **Open Internet**: No action required. If this mode is selected, settings obtained by STUN lookups are ignored. The IP address used is that of the system LAN interface. • **Symmetric NAT**: A symmetric NAT is one where all requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host. SIP Packets need to be mapped but STUN will not provide the correct information unless the IP address on the STUN server is the same as the ITSP Host. If this type of NAT/Firewall is detected or manually selected, a warning 'Communication is not possible unless the STUN server is supported on same IP address as the ITSP' will be displayed as part of the manager validation.

Table continues…

Field	Description
	• **Full Cone NAT**: A full cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address. SIP packets need to be mapped to NAT address and Port; any Host in the internet can call in on the open port, that is the local info in the SDP will apply to multiple ITSP Hosts. No warning will be displayed for this type of NAT because the system has sufficient information to make the connection). • **Restricted Cone NAT**: A restricted cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Unlike a full cone NAT, an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X. SIP packets needs to be mapped. Responses from hosts are restricted to those that a packet has been sent to. So if multiple ITSP hosts are to be supported, a keep alive will need to be sent to each host. If this type of NAT/ Firewall is detected or manually selected, no warning will be displayed for this type of NAT. • **Port Restricted Cone NAT**: A port restricted cone NAT is like a restricted cone NAT, but the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P. SIP packets needs to be mapped. Keep-alives must be sent to all ports that will be the source of a packet for each ITSP host IP address. If this type of NAT/Firewall is detected or manually selected, no warning will be displayed for this type of NAT. However, some Port Restricted NAT's have been found to be more symmetric in behavior, creating a separate binding for each opened Port, if this is the case the manager will display a warning 'Communication is not possible unless the STUN server is supported on same IP address as the ITSP' as part of the manager validation. • **Static Port Block**: Use the RTP Port Number Range specified on the VoIP tab without STUN translation. Those ports must be fixed as open on any NAT firewall involved • **One-To-One NAT**: This setting supports IP Office cloud deployments where the Primary server is behind a NAT that performs IP address translation but not port mappings. All required ports must be open on the NAT. When set to **One-To-One NAT**, the following configuration settings are applied and cannot be edited. - The **LAN | Network Topology | Public Port** values are set to 0. - **LAN | VoIP | SIP Registrar Enable** remote protocol port values are set to equal their corresponding local protocol port values. - The **LAN | VoIP | RTP | Port Number Range (NAT) Minimum** and **Maximum** values are set to equal the corresponding **Port Number Range** values. • **Unknown**

Table continues…

Field	Description
Binding Refresh Time (seconds)	Default = 0 (Never). Range = 0 to 3600 seconds. Having established which TCP/UDP port number to use, through either automatic or manual configuration, the system can send recurring 'SIP OPTIONS requests' to the remote proxy terminating the trunk. Those requests will keep the port open through the firewall. Requests are sent every x seconds as configured by this field. **Note:** If a binding refresh time has not been set you may experience problems receiving inbound SIP calls as they are unable to get through the Firewall. In these circumstances make sure that this value has been configured.
Public IP Address	Default = 0.0.0.0 This value is either entered manually or discovered by the Run STUN process. If no address is set, the system LAN1 address is used.
Public Port	Default = 0 The public port value for **UDP**, **TCP**, and **TLS**. For each protocol, this value is either entered manually or discovered by the Run STUN process.
Run STUN	This button tests STUN operation between the system LAN and the STUN Server IP Address set above. If successful the results are used to automatically fill the remaining fields with appropriate values discovered by the system. Before using Run STUN the SIP trunk must be configured. When this option is used, a information icon is shown against the fields to indicate that the values were automatically discovered rather than manually entered.
Run STUN on startup	Default = Off This option is used in conjunction with values automatically discovered using Run STUN. When selected, the system will rerun STUN discovery whenever the system is rebooted or connection failure to the SIP server occurs.

Related Links

System | LAN1 on page 205

DHCP Pools

DHCP pools allows for the configuration of of IP address pools for allocation by the system when acting as a DHCP server. On an IP500 V2 system, you can configure up to 8 pools. On Server Edition Linux systems, you can configure up to 64 pools.

By default the DHCP settings (IP Address, IP Mask and Number of DHCP IP Addresses) set on the LAN Settings tab are reflected by the first pool here. For support of PPP Dial In address requests, at least one of the pools must be on the same subnet as the system's LAN. Only addresses from a pool on the same subnet as the system's own LAN address will be used for PPP Dial In.

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

Field	Description
Apply to Avaya IP Phones Only	Default = Off. If this option is selected, the DHCP addresses are only used for requests from Avaya IP phones. Other devices connected to the system LAN will have to use static addresses or obtain their address from another DHCP server. In addition to the above control, Avaya IP phones will only complete DHCP against a DHCP server configured to supports a Site Specific Option Number (SSON) that matches that set on the phone. The SSON numbers supported by the system DHCP are set on the VoIP sub-tab.
DHCP Pool	Up to 8 pools can be added. The first pool matches the IP Address, IP Mask and Number of DHCP IP Addresses on the LAN Settings sub-tab. When adding or editing pools, Manager will attempt to warn about overlaps and conflicts between pools. The options are: • **Start Address** Sets the first address in the pool. • **Subnet Mask**: Default = 255.255.255.0 Sets the subnet mask for addresses issued from the pool. • **Default Router**: Default = 0.0.0.0 For pools issuing IP addresses on the same subnet as the system LAN's, **0.0.0.0** instructs the system to determined the actual default router address to issue by matching the IP address/subnet mask being issued in the IP Routing table. This matches the default behaviour used by systems without multiple pools. For pools issuing addresses not on the same subnet as the system LAN's, the default router should be set to the correct value for devices on that subnet. • **Pool Size**: Default = 0 Set the number of DHCP client addresses available in the pool.

Related Links

System | LAN1 on page 205

System | LAN2

This set of tabs is used to configure the system's second LAN interface.

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

The fields available for LAN2 are the same as for LAN1 except for the following additional field:

Field	Description
Firewall	Default = <None> (No firewall) Allows the selection of a system firewall to be applied to traffic routed from LAN2 to LAN1.

Related Links

System on page 199

System | DNS

DNS is a mechanism through which the URL's requested by users, such as www.avaya.com, are resolved into IP addresses. These requests are sent to a Domain Name Server (DNS) server, which converts the URL to an IP address. Typically the internet service provider (ISP) will specify the address of the DNS server their customers should use.

WINS (Windows Internet Name Service) is a similar mechanism used within a Windows network to convert PC and server names to IP addresses via a WINS server.

If the system is acting as a DHCP server, in addition to providing clients with their own IP address settings it can also provide them with their DNS and WINS settings if requested by the client.

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

Field	Description
DNS Service IP Address	Default = 0.0.0.0 (Do not provide DNS/Use DNS forwarding) This is the IP address of a DNS Server. Your Internet service provider or network administrator provides this information. If this field is left blank, the system uses its own address as the DNS server for DHCP client and forward DNS requests to the service provider when **Request DNS** is selected in the service being used (Service | IP).
Backup DNS Server IP Address	Default = 0.0.0.0 (No backup)
DNS Domain	Default = Blank (No domain) This is the domain name for your IP address. Your Internet service provider or network administrator provides this. Typically this field is left blank.
WINS Server IP Address	Default = 0.0.0.0 (Do not provide WINS) This is the IP address of your local WINS server. This is only used by Windows PCs, and normally points to an NT server nominated by your network administrator as your WINS server. Setting a value will result in also sending a mode of "hybrid". For Server Edition this field is only available on Expansion System (V2) servers.
Backup WINS Server IP Address	Default = 0.0.0.0 (No backup)
WINS Scope	Default = Blank (no scope) This is provided by your network administrator or left blank. For Server Edition this field is only available on Expansion System (V2) servers.

Related Links

System on page 199

System | Voicemail

The following settings are used to set the system's voicemail server type and location. Fields are enabled or grayed out as appropriate to the selected voicemail type. Refer to the appropriate voicemail installation manual for full details.

Changes to **Voicemail Type** require a reboot.

Field	Description
Voicemail Type	Defaults: Non-Server Edition = Embedded Voicemail, Primary Server = Voicemail Pro, Server Edition Secondary Server with independent voicemail or for Outbound Contact Express = Voicemail Pro, Server Edition Others: Centralized Voicemail. Sets the type of voicemail system being used. The options are: • **None**: No voicemail operation. • **Analogue Trunk MWI** (Release 9.0.3+): Select this option to support receiving a message waiting indicator (MWI) signal from analog trunks terminating on the ATM4U-V2 card. MWI is a telephone feature that turns on a visual indicator on a telephone when there are recorded messages. • **Avaya Aura Messaging**: Select this option if you want to configure the system to use Avaya Aura Messaging as the central voicemail system. If you choose this option, you are still able to use Embedded Voicemail or Voicemail Pro at each branch to provide auto-attendant operation and announcements for waiting calls. When selected, access to voicemail is routed via an SM line to the numbers specified in the **AAM Number** field. The optional **AAM PSTN Number** can be configured for use when the SM Line is not in service. For a setup where the voicemail box numbers configured on Avaya Aura Messaging or Modular Messaging are same as the caller's DID, the short code to route the PSTN call should be such that the caller-id is withheld ("W" in the telephone-number of the shortcode). This is to make sure that, during rainy day - the voicemail system does not automatically go to the voicemail box of the caller based on the caller id. • **CallPilot**: Select this option if you want to configure the system to use CallPilot over SIP as the central voicemail system. If you choose this option, you are still able to use **Embedded Voicemail** or Voicemail Pro at each branch to provide auto-attendant operation and announcements for waiting calls. When selected, access to voicemail is routed via SM line to the numbers specified in the **CallPilot Number** field. The optional **CallPilot PSTN Number** can be configured for use when the SM Line is not in service. **Note:** The **CallPilot PSTN Number** field and associated **Enable Voicemail Instructions Using DTMF** check box are not supported. IP Office cannot access the CallPilot system over the PSTN when the Session Manager line is down. • **Centralized Voicemail** Select this option when using a Voicemail Pro system installed and licensed on another system in a multi-site network. The outgoing line

Table continues…

Field	Description
	group of the H.323 IP line connection to the system with the Voicemail Pro should be entered as the **Voicemail Destination**. In a Server Edition network this option is used on the Secondary Server and expansion systems to indicate that they use the Primary Server for as their voicemail server. • **Distributed Voicemail**: This option can be used when additional Voicemail Pro voicemail servers are installed in a multi-site network and configured to exchange messages with the central voicemail server using email. This option is used if this system should use one of the additional servers for its voicemail services rather than the central sever. When selected, the **Voicemail Destination** field is used for the outgoing H.323 IP line to the central system and the **Voicemail IP Address** is used for the IP address of the distributed voicemail server the system should use. This option is not supported by Server Edition systems. • **Embedded Voicemail** On systems with an Avaya memory card, select this option to run Embedded Voicemail which stores messages and prompts on the memory card. It also supports internal Auto Attendant configuration through the system configuration. The IP500 V2 supports 2 simultaneous Embedded Voicemail calls by default but can be licensed for up to 6. The licensed limit applies to total number of callers leaving messages, collecting messages and or using an auto attendant. This option is not supported by Server Edition systems. • **Group Voicemail** This option is used to support third-party voicemail systems attached by extension ports in the group specified as the **Voicemail Destination**. This option is not supported by Server Edition systems. • **Modular Messaging over SIP** Select this option if you want to configure the system to use Modular Messaging over SIP as the central voicemail system. If you choose this option, you are still able to use Embedded Voicemail or Voicemail Pro at each branch to provide auto-attendant operation and announcements for waiting calls. When selected, access to voicemail is routed via an SM line to the numbers specified in the **MM Number** field. The optional **MM PSTN Number** can be configured for use when the SM Line is not in service. **Note:** Embedded Voicemail and Voicemail Pro are available only in Distributed branch deployments. They are not available when there are centralized users configured for a IP Officee system that is deployed as either a Centralized branch or a mixed branch. The Embedded Voicemail option uses the Essential Edition and the Additional Voicemail Ports licenses to control the number of ports that can be used. These licenses are also used to control the number of ports on systems where Embedded Voicemail is configured to provide local Auto Attendant and announcements while the selected option for voicemail is one of the central voicemail options through the Session Manager (i.e. Avaya Aura Messaging, Modular Messaging, or CallPilot). Similarly, the Voicemail Pro option uses the Preferred Edition and the Incremental Voicemail Ports licenses to control the number of ports that can be used. These licenses are also used to control the number of ports on systems where Voicemail

Table continues…

Field	Description
	Pro is configured to provide local Call Flow processing while the selected option for voicemail is Avaya Aura Messaging, Modular Messaging or CallPilot. - When the system routes a call to the voicemail server it indicates the locale for which matching prompts should be provided if available. The locale sent to the voicemail server by the system is determined as show below. If the required set of prompts is not available, the voicemail will fallback to another appropriate language and finally to English (refer to the appropriate voicemail installation manual for details). - **Short Code Locale**: The short code locale, if set, is used if the call is routed to voicemail using the short code. - **Incoming Call Route Locale**: The incoming call route locale, if set, is used if caller is external. - **User Locale**: The user locale, if set, is used if the caller is internal. - **System Locale**: If no user or incoming call route locale is set, the system locale is used unless overridden by a short code locale. - Systems using Embedded Voicemail, if the required set of upgraded language prompts to match the locale is not present on the system SD card, Manager will display an error. The required prompt set can be uploaded from Manager using the Add/Display VM Locales option. • **Remote Audix Voicemail**: Select this option if using a remote Avaya Intuity Audix or MultiMessage voicemail system. Requires entry of an **Audix Voicemail** license in Licenses. This option is not supported by Server Edition systems. • **Voicemail Pro** Select this option when using Voicemail Pro. The IP address of the PC being used should be set as the **Voicemail IP Address**. In a Server Edition network this option is used on the Primary Server. It can also be used on the Secondary Server if the Secondary server is connected to its own voice mail server or if the Secondary Server is part of an Outbound Contact Express deployment. Use of Voicemail Pro requires licenses for the number of simultaneous calls to be supported. Licenses are not required for an Outbound Contact Express deployment. • **Voicemail Mode**: Default = IP Office Mode. Embedded Voicemail on IP500 V2 systems can use either **IP Office Mode** or **Intuity Mode** key presses for mailbox functions. End users should be provided with the appropriate mailbox user guide for the mode selected. IP500 V2 systems use **IP Office Mode** only. You can switch between modes without losing user data, such as passwords, greetings, or messages. The following user guides are available from the Avaya support web site: • IP Office Basic Edition - Embedded Voicemail User Guide (Intuity Mode) • IP Office Basic Edition - Embedded Voicemail User Guide (IP Office Mode) • IP Office Basic Edition Norstar Mode - Embedded Voicemail User Guide (Intuity Mode)

Table continues…

Field	Description
	• IP Office Basic Edition Norstar Mode - Embedded Voicemail User Guide (IP Office Mode) • IP Office Basic Edition Partner Mode - Embedded Voicemail User Guide (Intuity Mode) • IP Office Basic Edition Partner Mode - Embedded Voicemail User Guide (IP Office Mode) • IP Office Essential Edition - Embedded Voicemail User Guide (Intuity Mode) • IP Office Essential Edition - Embedded Voicemail User Guide (IP Office Mode) • IP Office Voicemail Pro Mailbox User Guide (Intuity Mode) • IP Office Voicemail Pro Mailbox User Guide (IP Office Mode)
Add/Display VM Locales	For new IP500 V2 SD cards and cards recreated using Manager, the following Embedded Voicemail languages set are placed onto cards by default. Using this option displays the list of languages that can be uploaded from Manager. Those languages already present or not supported are greyed out. If a locale is selected for the system, a user, a short code or an incoming call route which is not present on the SD card, Manager will display an error. This command can be used to upload the required language prompts to correct the error.
Voicemail Destination	Defaults: Non-Server Edition = Blank, Server Edition = IP trunk connection to the Primary Server. • When the **Voicemail Type** is set to **Remote Audix Voicemail**, **Centralized Voicemail** or **Distributed Voicemail**, this setting is used to enter the outgoing line group of the line configured for connection to the phone system hosting the central voicemail server. • When the **Voicemail Type** is set to **Group Voicemail**, this setting is used to specify the group whose user extensions are connected to the 3rd party voicemail system. • When the **Voicemail Type** is set to **Analogue Trunk MWI**, this setting is used to specify the phone number of the message center. All analogue trunks configured for **Analogue Trunk MWI** must have the same destination.
Voicemail IP Address	Defaults: Non-Server Edition = 255.255.255.255, Primary Server = Primary Server IP Address. This setting is used when the **Voicemail Type** is set to **Voicemail Pro** or **Distributed Voicemail**. It is the IP address of the PC running the voicemail server that the system should use for its voicemail services. If set as 255.255.255.255, the control unit broadcasts on the LAN for a response from a voicemail server. If set to a specific IP address, the system connects only to the voicemail server running at that address. If the system is fitted with an Unified Communication Module hosting Voicemail Pro, the field should be set to 169.254.0.2.
Backup Voicemail IP Address	Defaults: Primary Server = Secondary Server IP Address, All others = 0.0.0.0 (Off). This option is supported with Voicemail Pro.

Table continues…

Field	Description
	An additional voicemail server can be setup but left unused. If contact to the voicemail server specified by the **Voicemail IP Address** is lost, responsibility for voicemail services is temporarily transferred to this backup server address.
Audix UDP	Available if the voicemail type Remote Audix Voicemail is selected. Needs to be completed with a four digit number from the Universal Dial Plan of the Avaya Communication Manager system.
Voicemail Channel Reservation	These settings allow the channels between the system and Voicemail Pro to be reserved for particular functions. Unreserved channels can be used for any function but reserved channels cannot be used for any function other than that indicated. These settings are not available unless the configuration includes validated licenses for the total number of voicemail channels. Note that the voicemail server also restricts the maximum number of channels that can be used for some services that would be taken from the **Unreserved Channels** pool. Alarms and callbacks are each limited to up to 2 channels at any time. Outcalling and conference invites are each limited to up to 5 channels at any time. • **Unreserved Channels**: This setting cannot be changed and by default will show the total number of licensed voicemail channels. This number will decrease as channels are reserved for the following functions. • **Mailbox Access**: Default = 0 This setting sets the number of channels reserved for users accessing mailboxes to collect messages. • **Auto-Attendant:**: Default = 0 This setting sets the number of channels reserved for users directed to Voicemail Pro short code and module start points. • **Voice Recording**: Default = 0 This setting sets the number of channels reserved for voice recording other than mandatory voice recording (see below). If no channels are available recording does not occur though recording progress may be indicated. • **Mandatory Voice Recording**: Default = 0 This setting sets the number of channels reserved for mandatory voice recording. When no channels are available for a call set to mandatory recording, the call is barred and the caller hears busy tone. • **Announcements:** Default = 0 This setting sets the number of channels reserved for announcements. When no channels are available calls continue without announcements. - **Call Recording**: These setting relate to call recording. Call recording is only supported when using a Voicemail Pro voicemail server. - **Auto Restart Paused Recording (secs)**: Default = 15 seconds. Range = Never or 5 to 999 seconds. If recording, manual or automatic, of a call is halted using a Pause Recording button, this timer determines when recording is restarted if the button is not pressed again. - **Hide Auto Recording**: Default = On (USA)/Off (Rest of World) During call recording by Voicemail Pro, some Avaya phones display REC or similar to show that the call is being recorded. When on, hide auto recording suppresses this recording indication.

Table continues…

Field	Description
Maximum Record Time	Default = 120 seconds. Range = 30 to 180 seconds. This field is only available when **Embedded Voicemail** is selected as the **Voicemail Type**. The value sets the maximum record time for messages and prompts.
Messages Button Goes to Visual Voice	Default = On. Visual Voice allows phone users to check their voicemail mailboxes and perform action such as play, delete and forward messages through menus displayed on their phone. By default, on phones with a **MESSAGES** button, the navigation is via spoken prompts. This option allows that to be replaced by Visual Voice on phones that support Visual Voice menus. For further details see Visual Voice.
Outcalling Control	Default = Off. This setting is used to enable or disable system wide outcalling on VMPro.
DTMF Breakout Allows system defaults to be set. These are then applied to all user mailboxes unless the users own settings differ. The Park & Page feature is supported when the system voicemail type is configured as **Embedded Voicemail** or **Voicemail Pro**. Park & Page is also supported on systems where Avaya Aura Messaging, Modular Messaging over SIP, or CallPilot (for IP Office Aura Edition with CS 1000 deployments) is configured as the central voice mail system and the local Embedded Voicemail or Voicemail Pro provides auto attendant operation. The Park & Page feature allows a call to be parked while a page is made to a hunt group or extension. This feature can be configured for Breakout DTMF 0, Breakout DTMF 2, or Breakout DTMF 3.	
Reception/Breakout (DTMF 0)	The number to which a caller is transferred if they press 0while listening to the mailbox greeting rather than leaving a message (***0** on Embedded Voicemail in IP Office Mode). For voicemail systems set to Intuity emulation mode, the mailbox owner can also access this option when collecting their messages by dialing ***0**. If the mailbox has been reached through a Voicemail Pro call flow containing a **Leave Mail** action, the option provided when **0** is pressed are: • For IP Office mode, the call follows the **Leave Mail** action's **Failure** or **Success** results connections depending on whether the caller pressed **0** before or after the record tone. • For Intuity mode, pressing **0** always follows the **Reception/Breakout (DTMF 0)** setting. • When Park & Page is selected for a DTFM breakout, the following drop-down boxes appear: - **Paging Number**: Displays a list of hunt groups and users (extensions). Select a hunt group or extension to configure this option. - **Retries**: The range is 0 to 5. The default setting is 0. - **Retry Timeout**Provided in the format M:SS (minute:seconds). The range can be set in 15-second increments. The minimum setting is 15 seconds and the maximum setting is 5 minutes. The default setting is 15 seconds

Table continues…

Field	Description
Breakout (DTMF 2)	The number to which a caller is transferred if they press 2while listening to the mailbox greeting rather than leaving a message (***2** on Embedded Voicemail in IP Office Mode).
Breakout (DTMF 3)	The number to which a caller is transferred if they press 3while listening to the mailbox greeting rather than leaving a message (***3** on Embedded Voicemail in IP Office Mode).
Voicemail Code Complexity Defines the requirements for the voicemail code. For IP Office systems that have **Voicemail Type** set to **Centralized**, the **Voicemail Code Complexity** settings must be the same as the IP Office system that is connected to Voicemail Pro.	
Enforcement	Default = On. When on, a user PIN is required.
Minimum Length	Default = 4. Maximum 15 digits.
Complexity	Default = On. When on, the following complexity rules are enforced. • The user extension number cannot be used. • A PIN consisting of repeated digits is not allowed (1111). • A PIN consisting of a sequence, forward or reverse, is not allowed (1234).
SIP Settings	For Enterprise Branch deployments, these settings are used for calls made or received on a SIP line where any of the line's SIP URI fields are set to use internal data. For Voicemail Pro, for calls made or received on a SIP line where any of the line's SIP URI fields are set to **Use Internal Data**, that data is taken from these settings. These options are shown if the system has SIP trunks or is set to use **Voicemail Lite/Pro**, **Centralized Voicemail** or **Distributed Voicemail**.
SIP Name	Default = Blank on Voicemail tab/Extension number on other tabs. The value from this field is used when the From field of the SIP URI being used for a SIP call is set to **Use Internal Data**.
SIP Display Name (Alias)	Default = Blank on Voicemail tab/Name on other tabs. The value from this field is used when the Display Name field of the SIP URI being used for a SIP call is set to **Use Internal Data**
Contact	Default = Blank on Voicemail tab/Extension number on other tabs. The value from this field is used when the Contact field of the SIP URI being used for a SIP call is set to **Use Internal Data**.
Anonymous	Default = On on Voicemail tab/Off on other tabs. If the From field in the SIP URI is set to **Use Internal Data**, selecting this option inserts **Anonymous** into that field rather than the SIP Name set above.

Voicemail Language Prompts

When the system routes a call to the voicemail server it indicates the locale for which matching prompts should be provided if available. The locale sent to the voicemail server by the system is

determined as show below. If the required set of prompts is not available, the voicemail will fallback to another appropriate language and finally to English (refer to the appropriate voicemail installation manual for details).

- **Short Code Locale**: The short code locale, if set, is used if the call is routed to voicemail using the short code.
- **Incoming Call Route Locale**: The incoming call route locale, if set, is used if caller is external.
- **User Locale**: The user locale, if set, is used if the caller is internal.
- **System Locale**: If no user or incoming call route locale is set, the system locale is used unless overridden by a short code locale.

Systems using Embedded Voicemail, if the required set of upgraded language prompts to match the locale is not present on the system SD card, Manager will display an error. The required prompt set can be uploaded from Manager using the Add/Display VM Locales option.

Related Links

System on page 199

System | Telephony

This tab is used to set the default telephony operation of the system. Some settings shown here can be overridden for individual users through their User | Telephony tab. The settings are split into a number of sub-tabs.

Related Links

System on page 199
Telephony on page 224
Park and Page on page 235
Tones and Music on page 236
Ring Tones on page 242
SM on page 243
Call Log on page 246
TUI on page 247

Telephony

These settings have changed in release 9.1. View the 9.0 settings on page 230.

This page is used to configure a wide range of general purpose telephony settings for the whole system.

These settings are mergeable. However, changes to **Companding LAW** and **Automatic Codec Preference** require a reboot.

Field	Description
Analog Extensions	

Table continues…

Field	Description
These settings apply only to analog extension ports provided by the system. For Server Edition this field is only available on Expansion System (V2) systems	
Default Outside Call Sequence	Default = Normal This setting is only used with analog extensions. It sets the ringing pattern used for incoming external calls. For details of the ring types see Ring Tones. This setting can be overridden by a user's **User | Telephony | Call Settings | Outside Call Sequence** setting. Note that changing the pattern may cause fax and modem device extensions to not recognize and answer calls.
Default Inside Call Sequence	Default = Ring Type 1 This setting is only used with analog extensions. It sets the ringing pattern used for incoming internal calls. For details of the ring types see Ring Tones. This setting can be overridden by a user's **User | Telephony | Call Settings | Inside Call Sequence** setting.
Default Ring Back Sequence	Default = Ring Type 2 This setting is only used with analog extensions. It sets the ringing pattern used for ringback calls such as hold return, park return, voicemail ringback, and Ring Back when Free. For details of the ring types see Ring Tones. This setting can be overridden by a user's **User | Telephony | Call Settings | Ringback Call Sequence** setting.
Restrict Analog Extension Ringer Voltage	Default = Off. Supported on IP500 V2 systems only. If selected, the ring voltage on analogue extension ports on the system is limited to a maximum of 40V Peak-Peak. Also when selected, the message waiting indication (MWI) settings for analog extension are limited to **Line Reversal A**, **Line Reversal B** or **None**. Any analog extension already set to another MWI setting is forced to **Line Reversal A**.
Dial Delay Time (secs)	Default = 4 (USA/Japan) or 1 (ROW). Range = 1 to 30 seconds. This setting sets the time the system waits following a dialed digit before it starts looking for a short code match. In situations where there are potential short codes matches but not exact match, it also sets the delay following the dialing of a digit before dialing complete is assumed. See the Short Codes section.
Dial Delay Count	Default = 0 digits (USA/Japan) or 4 digits (ROW). Range = 0 to 30 digits. This setting sets the number of digits dialed after which the system starts looking for a short code match regardless of the **Dial Delay Time**.
Default No Answer Time (secs)	Default = 15 seconds. Range = 6 to 99999 seconds. This setting controls the amount of time before an alerting call is considered as unanswered. How the call is treated when this time expires depends on the call type. For calls to a user, the call follows the user's Forward on No Answer settings if enabled. If no forward is set, the call will go to voicemail if available or else continues to ring. This timer is also used to control the duration of call forwarding if the forward destination does not answer. It also controls the duration of ringback call

Table continues…

Field	Description
	alerting. This setting is overridden by the **User | Telephony | Call Settings | No Answer Time** setting for a particular user if different. For calls to hunt groups, this setting controls the time before the call is presented to the next available hunt group member. This setting is overridden by the **Hunt Group | Hunt Group | No Answer Time** setting for a particular hunt group if different.
Hold Timeout (secs)	Default = Locale specific. Range = 0 (Off) to 99999 seconds. This setting controls how long calls remain on hold before recalling to the user who held the call. Note that the recall only occurs if the user has no other connected call. Recalled calls will continue ringing and do not follow forwards or go to voicemail.
Park Timeout (secs)	Default = Locale specific. Range 0 (Off) to 99999 seconds. This setting controls how long calls remain parked before recalling to the user who parked the call. Note that the recall only occurs if the user has no other connected call. Recalled calls will continue ringing and do not follow forwards or go to voicemail.
Ring Delay	Default = 5 seconds. Range = 0 to 98 seconds. This setting is used when any of the user's programmed appearance buttons is set to Delayed ringing. Calls received on that button will initially only alert visually. Audible alerting will only occur after the ring delay has expired. This setting can be overridden by a ring delay set for an individual user (**User | Telephony | Multi-line Options | Ring Delay**).
Call Priority Promotion Time (secs)	Default = Disabled. Range = Disabled, 10 to 999 seconds. When calls are queued for a hunt group, higher priority calls are placed ahead of lower priority calls, with calls of the same priority sort by time in queue. External calls are assigned a priority (**1-Low**, **2-Medium** or **3-High**) by the Incoming Call Route that routed the call. Internal calls are assigned a priority of **1-Low**. This option can be used to increase the priority of a call each time it has remained queued for longer than this value. The calls priority is increased by 1 each time until it reaches 3-High. In situations where calls are queued, high priority calls are placed before calls of a lower priority. This has a number of effects: • Mixing calls of different priority is not recommended for destinations where Voicemail Pro is being used to provided queue ETA and queue position messages to callers since those values will no longer be accurate when a higher priority call is placed into the queue. Note also that Voicemail Pro will not allow a value already announced to an existing caller to increase. • If the addition of a higher priority call causes the queue length to exceed the hunt group's Queue Length Limit, the limit is temporarily raised by 1. This means that calls already queued are not rerouted by the addition of a higher priority call into the queue.
Default Currency	Default = Locale specific. This setting is used with ISDN Advice of Charge (AOC) services. Note that changing the currency clears all call costs stored by the system except those already logged through SMDR. The currency is displayed in the system SMDR output.
Maximum SIP Sessions	Default = 0.

Table continues…

Field	Description
	This field is shown for Server Edition systems. On Server Edition systems, the Maximum SIP Sessions value must match the total number of SIP set and trunk calls that can occur at the same time. The **Maximum SIP Sessions** setting determines the number of SIP Trunk Channel licenses reserved for concurrent sessions on any SIP trunks provided by the server. Those licenses are reserved from the pool of SIP Trunk Channel licenses in the configuration of the Primary Server.
Default Name Priority	Default = Favour Trunk. For SIP trunks, the caller name displayed on an extension can either be that supplied by the trunk or one obtained by checking for a number match in the extension user's personal directory and the system directory. This setting determines which method is used by default. For each SIP line, this setting can be overridden by the line's own **Name Priority** setting if required. Select one of the following options: • **Favour Trunk**: Display the name provided by the trunk. For example, the trunk may be configured to provide the calling number or the name of the caller. The system should display the caller information as it is provided by the trunk. If the trunk does not provide a name, the system uses the **Favour Directory** method. • **Favour Directory**: Search for a number match in the extension user's personal directory and then in the system directory. The first match is used and overrides the name provided by the SIP line. If no match is found, the name provided by the line, if any, is used.
Media Connection Preservation	Default = Enabled. When enabled, attempts to maintain established calls despite brief network failures. Call handling features are no longer available when a call is in a preserved state. When enabled, Media Connection Preservation applies to SCN links and Avaya H.323 phones that support connection preservation.
Phone Failback	Default = Automatic. Applies to H.323 phones that support resiliency. The options are: • **Automatic** • **Manual** Phones are permitted to failover to the secondary gatekeeper when the IP Office Line link to the primary gatekeeper is down. When set to **Automatic**, if a phone's primary gatekeeper has been up for more than 10 minutes, the system causes the phone to failback if the phone is not in use. If the phone is in use, the system will reattempt failback 10 seconds after the phone ceases to be in use. When set to **Manual**, phones remain in failover until manually restarted or re-registered, after which the phone attempts to fail back.
Login Code Complexity	

Table continues…

Field	Description
Defines the requirements for the login code.	
Enforcement	Default = On. When on, a user PIN is required.
Minimum Length	Default = 4. Maximum 15 digits.
Complexity	Default = On. When on, the following complexity rules are enforced. • The user extension number cannot be used. • A PIN consisting of repeated digits is not allowed (1111). • A PIN consisting of a sequence is not allowed (1234).
Companding Law	These settings should not normally be changed from their defaults. They should only be used where 4400 Series phones (ULAW) are installed on systems which have A-Law digital trunks. **A-Law or U-Law>** PCM (Pulse Code Modulation) is a method for encoding voice as data. In telephony, two methods of PCM encoding are widely used, A-Law and U-Law (also called Mu-Law or μ-Law). Typically U-Law is used in North America and a few other locations while A-Law is used elsewhere. As well as setting the correct PCM encoding for the region, the A-Law or U-Law setting of a system when it is first started affects a wide range of regional defaults relating to line settings and other values. For IP500 V2 systems, the encoding default is set by the type of Feature Key installed when the system is first started. The cards are either specifically A-Law or U-Law>. PARTNER Mode cards are U-Law. Norstar Mode cards are A-Law.
DSS Status	Default = Off This setting affects Avaya display phones with programmable buttons. It controls whether pressing a DSS key set to another user who has a call ringing will display details of the caller. When off, no caller information is displayed.
Auto Hold	Default = On (Off for the United States locale). Used for users with multiple appearance buttons. When on, if a user presses another appearance button during a call, their current call is placed on hold. When off, if a users presses another appearance button during a call, their current call is disconnected.
Dial By Name	Default = On When on, allows the directory features on various phones to match the dialing of full names. This option is fixed as **On** and is not adjustable.
Show Account Code	Default = On This setting controls the display and listing of system account codes. • **When on:** When entering account codes through a phone, the account code digits are shown while being dialed. • **When off**: When entering account codes through a phone, the account code digits are replaced by s characters on the display.

Table continues…

Field	Description
Inhibit Off-Switch Forward/Transfer	Default = On When enabled, this setting stops any user from transferring or forwarding calls externally. See Off-Switch Transfer Restrictions.
Restrict Network Interconnect	Default = Off. When this option is enabled, each trunk is provided with a **Network Type** option that can be configured as either **Public** or **Private**. The system will not allow calls on a public trunk to be connected to a private trunk and vice versa, returning number unobtainable indication instead. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Include location specific information	Default = Off. When set to On, this setting is available in the trunk configuration settings when **Network Type** is set to **Private**. Set to **On** if the PBX on the other end of the trunk is toll compliant.
Drop External Only Impromptu Conference	Default = On. If selected, when the last remaining internal user in a conference exits the conference, the conference is ended, regardless of whether it contains any external callers. If not selected, the conference is automatically ended when the last internal party or trunk that supports reliable disconnect exits the conference. The Inhibit Off-Switch Forward/Transfer option above is no longer applied to conference calls.
Visually Differentiate External Call	Default = Off. This setting is applied to the lamp flashing rate used for bridged appearance and call coverage appearance buttons on 1400, 1600 and 9600 Series phones and on their button modules. When selected, external calls alerting on those buttons will use a slow flash (200ms on/50ms off). If not selected or if the call is internal, normal flashing (500ms on/500ms off) is used.
Unsupervised Analog Trunk Disconnect Handling	Default = Off. When using analog trunks, various methods are used for trunk supervision, ie. to detect when the far end of the trunk has disconnected and so disconnect the local end of the call. Depending on the locale, the system uses Disconnect Clear signalling and or Busy Tone Detection. This setting should only be enabled if it is know that the analog trunks do not provide disconnect clear signalling or reliable busy tone. For Server Edition this field is only available on Expansion System (V2) systems. When enabled: • Disconnect Clear signalling detection is disabled. Busy tone detection remains on. • Unsupervised transfers and trunk-to-trunk transfers of analog trunk calls are not allowed. The **Allow Analog Trunk to Trunk Connect** setting on analog trunks (Line | Analog Options) is disabled. • If Voicemail Pro is being used for external call transfers, **Supervised Transfer** actions should be used in call flows rather than **Transfer** actions.

Table continues…

Field	Description
	• All systems in the network must have this setting set to match each other.
High Quality Conferencing	Default = On. Supports the use of the G.722 codec. IP lines and extensions using G.722 are provided with wide band audio. If **High Quality Conferencing** is enabled, when several wide band audio devices are in the same conference, the system will ensure that the audio between them remains wide band, even if the conference also contains other lines and devices using narrow band audio (analog devices, digital devices and IP devices using codecs other than G.722).
Digital/Analogue Auto Create User	Default = On. (Not supported on Server Edition Linux systems) When enabled, an associated user is created for each digital/analogue extension created. Digital/analogue extension creation occurs on initial start up, reset of configuration, or addition of new digital/analogue expansion units or plug-in modules.
Directory Overrides Barring	Default = On. When enabled, barred numbers are not barred if the dialed number is in the External Directory.

Related Links

System | Telephony on page 224
Telephony (9.0) on page 230

Telephony (9.0)

This page is used to configure a wide range of general purpose telephony settings for the whole system.

These settings are mergeable. However, changes to **Companding LAW** and **Automatic Codec Preference** require a reboot.

Field	Description
Analog Extensions These settings apply only to analog extension ports provided by the system. For Server Edition this field is only available on Expansion System (V2) systems	
Default Outside Call Sequence	Default = Normal This setting is only used with analog extensions. It sets the ringing pattern used for incoming external calls. For details of the ring types see Ring Tones. This setting can be overridden by a user's **User | Telephony | Call Settings | Outside Call Sequence** setting. Note that changing the pattern may cause fax and modem device extensions to not recognize and answer calls.
Default Inside Call Sequence	Default = Ring Type 1 This setting is only used with analog extensions. It sets the ringing pattern used for incoming internal calls. For details of the ring types see Ring Tones. This setting can

Table continues…

Field	Description
	be overridden by a user's **User | Telephony | Call Settings | Inside Call Sequence** setting.
Default Ring Back Sequence	Default = Ring Type 2 This setting is only used with analog extensions. It sets the ringing pattern used for ringback calls such as hold return, park return, voicemail ringback, and Ring Back when Free. For details of the ring types see Ring Tones. This setting can be overridden by a user's **User | Telephony | Call Settings | Ringback Call Sequence** setting.
Restrict Analog Extension Ringer Voltage	Default = Off. Supported on IP500 V2 systems only. If selected, the ring voltage on analogue extension ports on the system is limited to a maximum of 40V Peak-Peak. Also when selected, the message waiting indication (MWI) settings for analog extension are limited to **Line Reversal A**, **Line Reversal B** or **None**. Any analog extension already set to another MWI setting is forced to **Line Reversal A**.
Dial Delay Time (secs)	Default = 4 (USA/Japan) or 1 (ROW). Range = 1 to 30 seconds. This setting sets the time the system waits following a dialed digit before it starts looking for a short code match. In situations where there are potential short codes matches but not exact match, it also sets the delay following the dialing of a digit before dialing complete is assumed. See the Short Codes section.
Dial Delay Count	Default = 0 digits (USA/Japan) or 4 digits (ROW). Range = 0 to 30 digits. This setting sets the number of digits dialed after which the system starts looking for a short code match regardless of the **Dial Delay Time**.
Default No Answer Time (secs)	Default = 15 seconds. Range = 6 to 99999 seconds. This setting controls the amount of time before an alerting call is considered as unanswered. How the call is treated when this time expires depends on the call type. For calls to a user, the call follows the user's Forward on No Answer settings if enabled. If no forward is set, the call will go to voicemail if available or else continues to ring. This timer is also used to control the duration of call forwarding if the forward destination does not answer. It also controls the duration of ringback call alerting. This setting is overridden by the **User | Telephony | Call Settings | No Answer Time** setting for a particular user if different. For calls to hunt groups, this setting controls the time before the call is presented to the next available hunt group member. This setting is overridden by the **Hunt Group | Hunt Group | No Answer Time** setting for a particular hunt group if different.
Hold Timeout (secs)	Default = Locale specific. Range = 0 (Off) to 99999 seconds. This setting controls how long calls remain on hold before recalling to the user who held the call. Note that the recall only occurs if the user has no other connected call. Recalled calls will continue ringing and do not follow forwards or go to voicemail.
Park Timeout (secs)	Default = Locale specific. Range 0 (Off) to 99999 seconds. This setting controls how long calls remain parked before recalling to the user who parked the call. Note that the recall only occurs if the user has no other connected

Table continues…

Field	Description
	call. Recalled calls will continue ringing and do not follow forwards or go to voicemail.
Ring Delay	Default = 5 seconds. Range = 0 to 98 seconds. This setting is used when any of the user's programmed appearance buttons is set to Delayed ringing. Calls received on that button will initially only alert visually. Audible alerting will only occur after the ring delay has expired. This setting can be overridden by a ring delay set for an individual user (**User | Telephony | Multi-line Options | Ring Delay**).
Call Priority Promotion Time (secs)	Default = Disabled. Range = Disabled, 10 to 999 seconds. When calls are queued for a hunt group, higher priority calls are placed ahead of lower priority calls, with calls of the same priority sort by time in queue. External calls are assigned a priority (**1-Low**, **2-Medium** or **3-High**) by the Incoming Call Route that routed the call. Internal calls are assigned a priority of **1-Low**. This option can be used to increase the priority of a call each time it has remained queued for longer than this value. The calls priority is increased by 1 each time until it reaches 3-High. In situations where calls are queued, high priority calls are placed before calls of a lower priority. This has a number of effects: • Mixing calls of different priority is not recommended for destinations where Voicemail Pro is being used to provided queue ETA and queue position messages to callers since those values will no longer be accurate when a higher priority call is placed into the queue. Note also that Voicemail Pro will not allow a value already announced to an existing caller to increase. • If the addition of a higher priority call causes the queue length to exceed the hunt group's Queue Length Limit, the limit is temporarily raised by 1. This means that calls already queued are not rerouted by the addition of a higher priority call into the queue.
Default Currency	Default = Locale specific. This setting is used with ISDN Advice of Charge (AOC) services. Note that changing the currency clears all call costs stored by the system except those already logged through SMDR. The currency is displayed in the system SMDR output.
Maximum SIP Sessions	Default = 0. This field is shown for Server Edition systems. On Server Edition systems, the Maximum SIP Sessions value must match the total number of SIP set and trunk calls that can occur at the same time. The **Maximum SIP Sessions** setting determines the number of SIP Trunk Channel licenses reserved for concurrent sessions on any SIP trunks provided by the server. Those licenses are reserved from the pool of SIP Trunk Channel licenses in the configuration of the Primary Server.
Default Name Priority	Default = Favour Trunk. For SIP trunks, the caller name displayed on an extension can either be that supplied by the trunk or one obtained by checking for a number match in the extension user's personal directory and the system directory. This setting determines which method is used by default. For each SIP line, this setting can be

Table continues…

Field	Description
	overridden by the line's own **Name Priority** setting if required. Select one of the following options: • **Favour Trunk**: Display the name provided by the trunk. For example, the trunk may be configured to provide the calling number or the name of the caller. The system should display the caller information as it is provided by the trunk. If the trunk does not provide a name, the system uses the **Favour Directory** method. • **Favour Directory**: Search for a number match in the extension user's personal directory and then in the system directory. The first match is used and overrides the name provided by the SIP line. If no match is found, the name provided by the line, if any, is used.
Media Connection Preservation	Default = Enabled. When enabled, attempts to maintain established calls despite brief network failures. Call handling features are no longer available when a call is in a preserved state. When enabled, Media Connection Preservation applies to SCN links and Avaya H.323 phones that support connection preservation.
Companding Law	These settings should not normally be changed from their defaults. They should only be used where 4400 Series phones ULAW are installed on systems which have A-Law digital trunks. **A-Law or U-Law>** PCM (Pulse Code Modulation) is a method for encoding voice as data. In telephony, two methods of PCM encoding are widely used, A-Law and U-Law (also called Mu-Law or μ-Law). Typically U-Law is used in North America and a few other locations while A-Law is used elsewhere. As well as setting the correct PCM encoding for the region, the A-Law or U-Law setting of a system when it is first started affects a wide range of regional defaults relating to line settings and other values. For IP500 V2 systems, the encoding default is set by the type of Feature Key installed when the system is first started. The cards are either specifically A-Law or U-Law>. PARTNER Mode cards are U-Law. Norstar Mode cards are A-Law.
DSS Status	Default = Off This setting affects Avaya display phones with programmable buttons. It controls whether pressing a DSS key set to another user who has a call ringing will display details of the caller. When off, no caller information is displayed.
Auto Hold	Default = On. Used for users with multiple appearance buttons. When on, if a user presses another appearance button during a call, their current call is placed on hold. When off, if a users presses another appearance button during a call, their current call is disconnected.
Dial By Name	Default = On When on, allows the directory features on various phones to match the dialing of full names. This option is fixed as **On** and is not adjustable.

Table continues…

Field	Description
Show Account Code	Default = On This setting controls the display and listing of system account codes. • **When on:** When entering account codes through a phone, the account code digits are shown while being dialed. • **When off**: When entering account codes through a phone, the account code digits are replaced by s characters on the display.
Inhibit Off-Switch Forward/Transfer	Default = On When enabled, this setting stops any user from transferring or forwarding calls externally. See Off-Switch Transfer Restrictions.
Restrict Network Interconnect	Default = Off. When this option is enabled, each trunk is provided with a **Network Type** option that can be configured as either **Public** or **Private**. The system will not allow calls on a public trunk to be connected to a private trunk and vice versa, returning number unobtainable indication instead. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Include location specific information	Default = Off.
Drop External Only Impromptu Conference	Default = On. If selected, when the last remaining internal user in a conference exits the conference, the conference is ended, regardless of whether it contains any external callers. If not selected, the conference is automatically ended when the last internal party or trunk that supports reliable disconnect exits the conference. The Inhibit Off-Switch Forward/Transfer option above is no longer applied to conference calls.
Visually Differentiate External Call	Default = Off. This setting is applied to the lamp flashing rate used for bridged appearance and call coverage appearance buttons on 1400, 1600 and 9600 Series phones and on their button modules. When selected, external calls alerting on those buttons will use a slow flash (200ms on/50ms off). If not selected or if the call is internal, normal flashing (500ms on/500ms off) is used.
Unsupervised Analog Trunk Disconnect Handling	Default = Off. When using analog trunks, various methods are used for trunk supervision, ie. to detect when the far end of the trunk has disconnected and so disconnect the local end of the call. Depending on the locale, the system uses Disconnect Clear signalling and or Busy Tone Detection. This setting should only be enabled if it is know that the analog trunks do not provide disconnect clear signalling or reliable busy tone. For Server Edition this field is only available on Expansion System (V2) systems. When enabled: • Disconnect Clear signalling detection is disabled. Busy tone detection remains on.

Table continues…

Field	Description
	• Unsupervised transfers and trunk-to-trunk transfers of analog trunk calls are not allowed. The **Allow Analog Trunk to Trunk Connect** setting on analog trunks (Line | Analog Options) is disabled. • If Voicemail Pro is being used for external call transfers, **Supervised Transfer** actions should be used in call flows rather than **Transfer** actions. • All systems in the network must have this setting set to match each other.
High Quality Conferencing	Default = On. Supports the use of the G.722 codec. IP lines and extensions using G.722 are provided with wide band audio. If **High Quality Conferencing** is enabled, when several wide band audio devices are in the same conference, the system will ensure that the audio between them remains wide band, even if the conference also contains other lines and devices using narrow band audio (analog devices, digital devices and IP devices using codecs other than G.722).
Strict SIPS	(Enterprise Branch deployments) Default = Off. This option provides a system-wide configuration for call restrictions based on SIPS URI. When this option is off, calls are not rejected due to SIPS. A call is sent according to the configuration of the outgoing trunk or line that it is routed to, regardless of the way the call came in, even if the call came in as a SIP invite with SIPS URI and is being sent with a SIP URI onto a non-secure SIP trunk. When this option is on, an incoming SIP invite with SIPS URI if targeted to a SIP trunk (SM line or SIP line) is rejected if the target trunk is not configured with SIPS in the URI Type field.
Digital/Analogue Auto Create User	Default = On. (Off for Server Edition) When enabled, an associated user is created for each digital/analogue extension created. Digital/analogue extension creation occurs on initial start up, reset of configuration, or addition of new digital/analogue expansion units or plug-in modules.
Directory Overrides Barring	Default = On. When enabled, barred numbers are not barred if the dialed number is in the External Directory.

Related Links

Telephony on page 224

Park and Page

The Park and Page tab allows for simple configuration of the of the short code and the programmable button for the park and page function.

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

Field	Description
Central Park Range	Default = Blank. Range = nX to nnnnnnnXX The park slot ID range definition, where n is a digit sequence from 1 to 9999999 and X represents a park slot value from 0 to 99. The Central Park Range cannot exceed 9 characters total length. Examples: • 1X defines range 10-19 • 3XX defines range 300-399 • 9876543XX defines range 987654300-987654399
Page Target Group List	Default = Blank. The list of paging group targets that are presented on supported phones if the Page action is requested after the Call Park. On some phones, only the first three groups can be presented as Page options (via the Softkeys on the phone). On phones that support scrolling lists, a larger list of possible Page targets can be presented.

Related Links

System | Telephony on page 224

Tones and Music

These settings have changed in release 9.1. View the release 9.0 settings on page 240.

This page is used to configure the various tones and music on hold sources used by the system.

The settings are mergable with the following exceptions.

- Changes to **Disconnect Tone** requires a reboot.
- Changes to **Busy Tone Detection** requires a reboot.
- For **Hold Music**, changes to the **System Source** requires a reboot. Deleting any of the hold music **Alternate Sources** also requires a reboot.

For additional information on configuring hold music, see Music On Hold on page 568.

Field	Description
Conferencing Tone	Default = Entry & Exit Tones. This settings controls how conference tones are used. The options are: • **Entry & Exit Tones**: Asingle tone is heard when a new party joins a conference and double-tone is heard when a party leaves the conference. • **Repeating Tone**A conference tone is heard every 10 seconds by all conference parties. Note that no conference tones are played in an a conference initiated by an Outbound Contact Express agent.
Disconnect Tone	Default = Default (Use locale setting).

Table continues…

Field	Description
	For digital and IP phones, when the system detects that the far end of a call has disconnected, it can make the near end either go idle or play disconnect tone. By default, the chosen behavior depends on the system locale. This field can be used to override the locale's default action and force either disconnect tone or go idle. The options are: • **Default**: Use the system locale specific action for disconnected calls. • **On**: Play disconnect tone when far end disconnection is detected. • **Off**: Go idle when far end disconnection is detected.
Busy Tone Detection	Default = Off. Enables or disables the use of busy tone detection for call clearing. This is a system wide setting.
CLI Type	This field is used to set the CLI detection used for incoming analogue trunks. Note that the CLI Type field is shown for locales other than **Customize**. For the **Customize** locale it is set through the System | System form.The options are: • **DTMF** • **FSK V23** • **FSK BELL202**
Local Dial Tone	Default = On For all normal operation this setting should be left enabled as it allows the system to provide dial tone to users (essential for MSN working).
Local Busy Tone	Default = Off This setting should only be used when the local exchange gives a busy signal via Q.931 but does not provide busy tone.
Beep on Listen	Default = On This setting controls whether call parties hear a repeating tone when their call is monitored by another party using the Call Listen feature. **Warning:** The use of features to listen to a call without the other call parties being aware of that monitoring may be subject to local laws and regulations. Before enabling the feature you must ensure that you have complied with all applicable local laws and regulations. Failure to do so may result in severe penalties.
GSM Silence Suppression	Default = Off. This setting should only be selected if voice quality problems are experienced with calls to voicemail or while recording calls. When on, the system signals silence by generating silence data packets in periods when the voicemail system is not playing prompts. Note that use of this option may cause some timeout routing options in voicemail to no longer work.
Analogue Trunk VAD	Default = Off.

Table continues…

Field	Description
	Select this option to enable Voice Activity Detection (VAD) for analog trunks terminating on the ATM4U-V2 card. VAD functionality provides a Call Answer signal triggered by voice activity. This signal can be used for: • Mobile Twinning • SMDR • Call Forwarding • Call Display • Mobile Call Control • Transfer Ringing Call • TAPI • Trunk to Trunk Call
Busy Tone Detection	Default = System Frequency (Tone defined by system locale) Allows configuration of the system's busy tone detection settings on lines that do not provide reliable disconnect signalling. In that case, the system will use tone disconnect clearing to disconnect such lines after 6 seconds of continuous tone. The default tone (frequency and on/off cadence) detection used is defined by the system locale. The settings should not be adjusted unless advised by Avaya Technical Support. Changes to this setting require a reboot rather than a merge when the new configuration is sent to the system. .For Server Edition this field is only available on Expansion System (V2) systems.
Hold Music This section is used to define the source for the system's music on hold source. You must ensure that any MOH source you use complies with copyright, performing rights and other local and national legal requirements. Server Edition deployments support centralized music on hold, where the Primary Server streams music to the Secondary Server and all expansion servers.	
System Source	Default = WAV File. Selects the default hold music source for most uses of music on hold. Note that changes to the **System Source** requires a reboot. The options are: • **WAV**: Use the WAV file **HoldMusic.wav**. This file is loaded via TFTP. Note that on Linux systems, the file name is case sensitive. • **WAV (restart)**: Identical to WAV except that for each new listener, the file plays from the beginning. Not supported on IP500 V2 systems. Cannot be used as a centralized source. • **External**: Applicable to IP 500 v2 systems. Use the audio source connected to the back of the control unit. • **Tone**: The use of a double beep tone (425Hz, 02./0.2/0.2/3.4 seconds on/off) can be selected as the system source. The hold music tone is automatically used if the

Table continues…

Field	Description
	system source is set to **WAV File** but the `holdmusic.wav` file has not yet been successfully downloaded.
Alternate Sources	Up to three additional hold music source can be specified. Note that adding and changing a source can be done using a merge but deleting a source requires a reboot. • **Number**: Assigned automatically by the system. The alternate sources are numbered 2, 3 and 4. • **Name**: Up to 31 characters This field is used to associate a name with the alternate source. That name is then used in the Hold Music Source field on Incoming Call Routes and Hunt Groups. • **Source**: Up to 31 characters. Defines the source for the music on hold. The options are listed below with a brief description. For more information, see Alternate Source on page 569. - **WAV**: To specify a wav file, enter **WAV:** followed by the file name. Playback resumes from where it left off the last time. - **XTN**: Any analog extension. Not applicable to Linux systems. - **WAVRST**: To specify a wav file, enter **WAVRST:** followed by the file name. Playback is started every time from the beginning. - **WAVDIR**: Multiple WAV file source. The WAV files must be stored in the `/opt/ipoffice/tones/mohwavdir/` directory. Playback resumes from where it left off the last time. Not applicable to IP500 V2 systems. - **WAVDIRRST**: Multiple WAV file source. The WAV files must be stored in the `/opt/ipoffice/tones/mohwavdir/` directory. Playback is started every time from the beginning. Not applicable to IP500 V2 systems. - **USB**: Supports multiple USB inputs. Enter `USB:<number>`. Not applicable to IP500 V2 systems. - **LINE**: In Server Edition networks, setting the Secondary Server and Expansion Server **Alternate Source** to **Line** allows the server to receive streamed audio from a source on the Primary Server. On the Secondary Server and Expansion Server, enter `Line:x,`ywhere **x** is the line number to the Primary Server and **y** is the MOH source number on the Primary Server.

Related Links

System | Telephony on page 224
Tones and Music (9.0) on page 240

Tones and Music (9.0)

This page is used to configure the various tones and music on hold sources used by the system.

Changes to **Busy Tone Detection** requires a reboot.

For **Hold Music**, changes to the **System Source** requires a reboot. Deleting any of the hold music **Alternate Sources** also requires a reboot.

Field	Description
Conferencing Tone	Default = Entry & Exit Tones. This settings controls how conference tones are used. The options are: • **Entry & Exit Tones**: Asingle tone is heard when a new party joins a conference and double-tone is heard when a party leaves the conference. • **Repeating Tone**A conference tone is heard every 10 seconds by all conference parties. Note that no conference tones are played in an a conference initiated by an Outbound Contact Express agent.
Disconnect Tone	Default = Default (Use locale setting). For digital and IP phones, when the system detects that the far end of a call has disconnected, it can make the near end either go idle or play disconnect tone. By default, the chosen behavior depends on the system locale. This field can be used to override the locale's default action and force either disconnect tone or go idle. The options are: • **Default**: Use the system locale specific action for disconnected calls. • **On**: Play disconnect tone when far end disconnection is detected. • **Off**: Go idle when far end disconnection is detected.
Busy Tone Detection	Default = Off. Enables or disables the use of busy tone detection for call clearing. This is a system wide setting.
CLI Type	This field is used to set the CLI detection used for incoming analogue trunks. Note that the CLI Type field is shown for locales other than **Customize**. For the **Customize** locale it is set through the System | System form.The options are: • **DTMF** • **FSK V23** • **FSK BELL202**
Local Dial Tone	Default = On For all normal operation this setting should be left enabled as it allows the system to provide dial tone to users (essential for MSN working).
Local Busy Tone	Default = Off This setting should only be used when the local exchange gives a busy signal via Q.931 but does not provide busy tone.

Table continues…

Field	Description
Beep on Listen	Default = On This setting controls whether call parties hear a repeating tone when their call is monitored by another party using the Call Listen feature. **Warning:** The use of features to listen to a call without the other call parties being aware of that monitoring may be subject to local laws and regulations. Before enabling the feature you must ensure that you have complied with all applicable local laws and regulations. Failure to do so may result in severe penalties.
GSM Silence Suppression	Default = Off. This setting should only be selected if voice quality problems are experienced with calls to voicemail or while recording calls. When on, the system signals silence by generating silence data packets in periods when the voicemail system is not playing prompts. Note that use of this option may cause some timeout routing options in voicemail to no longer work.
Busy Tone Detection	Default = System Frequency (Tone defined by system locale) Allows configuration of the system's busy tone detection settings on lines that do not provide reliable disconnect signalling. In that case, the system will use tone disconnect clearing to disconnect such lines after 6 seconds of continuous tone. The default tone (frequency and on/off cadence) detection used is defined by the system locale. The settings should not be adjusted unless advised by Avaya Technical Support. Changes to this setting require a reboot rather than a merge when the new configuration is sent to the system. .For Server Edition this field is only available on Expansion System (V2) systems.
Hold Music This section is used to define the source for the system's music on hold source. You must ensure that any MOH source you use complies with copyright, performing rights and other local and national legal requirements. Server Edition deployments support centralized music on hold, where the Primary Server streams music to the Secondary Server and all expansion servers.	
System Source	Default = WAV File. Selects the default hold music source for most uses of music on hold. Note that changes to the **System Source** requires a reboot. The options are: • **WAV**: Use the WAV file **HoldMusic.wav**. This file is loaded via TFTP. Note that on Linux systems, the file name is case sensitive. • **WAV (restart)**: Identical to WAV except that for each new listener, the file plays from the beginning. Not supported on IP500 V2 systems. Cannot be used as a centralized source. • **External**: For IP 500 v2 systems, use the audio source connected to the back of the control unit. For Linux servers, use the first available USB audio source.

Table continues…

Field	Description
	• **Tone**: The use of a double beep tone (425Hz, 02./0.2/0.2/3.4 seconds on/off) can be selected as the system source. The hold music tone is automatically used if the system source is set to **WAV File** but the `holdmusic.wav` file has not yet been successfully downloaded.
Alternate Sources	Up to three additional hold music source can be specified. Note that adding and changing a source can be done using a merge but deleting a source requires a reboot. • **Number:** : Assigned automatically by the system. The alternate sources are numbered 2, 3 and 4. • **Name:**: Up to 31 characters This field is used to associate a name with the alternate source. That name is then used in the Hold Music Source field on Incoming Call Routes and Hunt Groups. • **Source:**: Up to 31 characters Defines the source for the music on hold. - **WAV**: For a wav file, enter WAV: followed by the file name. For example, for the file **holdmusic2.wav**, enter `WAV:holdmusic2.wav`. The system will automatically attempt to load that file via TFTP following a reboot. - **XTN**: Any analog extension with its Equipment Classification set as **MOH Source** can be entered as the alternate source. Enter **XTN:** followed by the extension's Base Extension number. For example **XTN:224**. - **WAVDIR**: Multiple WAV file source. The WAV files must be stored in the /opt/ipoffice/tones/mohwavdir/ directory. The directory can contain up to 255 files and each file can be up to 10 minutes in length. Not applicable to Server Edition IP500 V2 expansion systems. - **USB**: Supports multiple USB inputs. Enter `USB:<number>`. **USB:1** is the first source found and is treated as **External** when the **System Source** is set to **External**. Additional devices are numbered sequentially. For example USB:2, USB:3. - **LINE**: In Server Edition networks, setting the Secondary Server and Expansion Server **Alternate Source** to **Line** allows the server to receive streamed audio from a source on the Primary Server. On the Secondary Server and Expansion Server, enter `Line:x,` ywhere **x** is the line number to the Primary Server and **y** is the MOH source number on the Primary Server.

Related Links

Tones and Music on page 236

Ring Tones

This page is used to configure ring tones. You can configure distinct ring tones for different hunt groups and for internal calls. Ring Tone configuration is only supported on 1400 series and 9500 series phones.

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

Field	Description
Available Ring Tones	In this table, the **Number**, **Name**, and **Source** values are system supplied. The **Name** value is used to create a ring tone plan.
Ring Tone Plan	Use this table to specify available ring tones. Ring tones in this table can be applied to hunt groups and incoming call routes. • **Number**: System supplied. • **Name**: A descriptive name for where this ring tone is used. For example, the name of a hunt group. Each name in the table must be unique. Once configured in this table, ring tone names can be selected from the **Ring Tone Override** field on the **Hunt Group | Hunt Group** tab and on the **Incoming Call Route | Standard** tab. • **Ring Tone**: The list of ring tone names from the **Available Ring Tones** table.

Related Links

System | Telephony on page 224

SM

These settings have changed in release 9.1. View the 9.0 settings on page 244.

This page is used to configure settings that apply to both SM lines.

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

Field	Description
Short Form Dialing Length	Default = 0. Range = 0 to 14. This number specifies the short-form dialing length for all Centralized users and Groups. Configuration of this field allows IP Office to treat the last N digits (where N is the number entered in this field) of each Centralized user's extension number as an alias to that user's extension number. For example, if a Centralized user's extension number is 5381111 and the Short Form Dialing Length is 4, the system will match calls to 1111 with this extension. When 1111 is dialed by another user on the system, entered from the autoattendant, or comes from the ICR, then in sunny-day that call will be sent to Session Manager with the number converted to 5381111 and in rainy-day it will target the extension 5381111 locally.
Branch Prefix	Default = Blank. Maximum range = 15 digits. This number is used to identify the IP Office system within the Avaya Aura® network. The branch prefix of each IP Office system must be unique and must not overlap. For example 85, 861 and 862 are okay, but 86 and 861 overlap. On calls routed via an SM Line, the branch prefix is added to the caller's extension number. You have the option to leave the Branch Prefix field blank. If you do not configure the branch prefix, the IP Officeuser extensions must be defined with the full enterprise number.
Local Number Length	Default = Blank (Off). Range = Blank (Off) or 3 to 9.

Table continues…

Field	Description
	This field sets the default length for extension numbers for extensions, users, andhunt groups added to the IP Office configuration. Entry of an extension number of a different length will cause an error warning by Manager. The number entered in the **Branch Prefix** field plus the number entered in the **Local Number Length** field must not exceed 15 digits. You have the option to leave the **Local Number Length** field blank.
Proactive Monitoring	Default = 60 seconds. Range = 60 seconds to 100000 seconds. The Enterprise Branch system sends regular SIP OPTIONS messages to the SM line in order to check the status of line. This setting controls the frequency of the messages when the SM line is currently in service. Centralized SIP phones use their own settings.
Monitoring Retries	Default = 1. Range = 0 to 5. The number of times the Enterprise Branch system retrys sending an OPTIONS request to Session Manager before the SM Line is marked out-of-service.
Reactive Monitoring	Default 60 seconds. Range = 10 to 3600 seconds. The Enterprise Branch system sends regular SIP OPTIONS messages to the SM line in order to check the status of line. This setting controls the frequency of the messages when the SM line is currently out of service. Centralized SIP phones use their own settings.
Failback Policy	Default = Auto. This field allows the administrator to choose between an automatic or manual failback policy on the IP Office. In deployments with Centralized phones, this field must be set consistently with the Failback Policy of the phones, which is configured via the Session Manager global settings in System Manager. The options are: • **Auto**: IP Office automatically brings the SM Line to ‘In Service’ status as soon as it detects via the Reactive Monitoring that the Session Manager is reachable • **Manual**: When an SM line is in "Out of Service" state, IP Office does not bring it back to "In Service" status based on automatic detection. IP Office keeps the SM Line in "Out of Service" state until the administrator manually initiates Failback of IP Office from Session Manager.

Related Links

System | Telephony on page 224
SM (9.0) on page 244

SM (9.0)

This page is used to configure settings that apply to both SM lines.

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

Field	Description
Short Form Dialing Length	Default = 0. Range = 0 to 14. This number specifies the short-form dialing length for all Centralized users and Groups. Configuration of this field allows IP Office to treat the last N digits (where N is the number entered in this field) of each Centralized user's extension number as an alias to that user's extension number. For example, if a Centralized user's extension number is 5381111 and the Short Form Dialing Length is 4, the system will match calls to 1111 with this extension. When 1111 is dialed by another user on the system, entered from the autoattendant, or comes from the ICR, then in sunny-day that call will be sent to Session Manager with the number converted to 5381111 and in rainy-day it will target the extension 5381111 locally.
Branch Prefix	Default = Blank. Maximum range = 15 digits. This number is used to identify the IP Office system within the Avaya Aura® network. The branch prefix of each IP Office system must be unique and must not overlap. For example 85, 861 and 862 are okay, but 86 and 861 overlap. On calls routed via an SM Line, the branch prefix is added to the caller's extension number. You have the option to leave the Branch Prefix field blank. If you do not configure the branch prefix, the IP Officeuser extensions must be defined with the full enterprise number.
Local Number Length	Default = Blank (Off). Range = Blank (Off) or 3 to 9. This field sets the default length for extension numbers for extensions, users, andhunt groups added to the IP Office configuration. Entry of an extension number of a different length will cause an error warning by Manager. The number entered in the **Branch Prefix** field plus the number entered in the **Local Number Length** field must not exceed 15 digits. You have the option to leave the **Local Number Length** field blank.
Proactive Monitoring	Default = 60 seconds. Range = 60 seconds to 100000 seconds. The Enterprise Branch system sends regular SIP OPTIONS messages to the SM line in order to check the status of line. This setting controls the frequency of the messages when the SM line is currently in service. Centralized SIP phones use their own settings.
Monitoring Retries	Default = 1. Range = 0 to 5. The number of times the Enterprise Branch system retrys sending an OPTIONS request to Session Manager before the SM Line is marked out-of-service.
Reactive Monitoring	Default 60 seconds. Range = 10 to 3600 seconds. The Enterprise Branch system sends regular SIP OPTIONS messages to the SM line in order to check the status of line. This setting controls the frequency of the messages when the SM line is currently out of service. Centralized SIP phones use their own settings.
Failback Policy	Default = Auto. This field allows the administrator to choose between an automatic or manual failback policy on the IP Office. In deployments with Centralized phones, this field

Table continues…

Field	Description
	must be set consistently with the Failback Policy of the phones, which is configured via the Session Manager global settings in System Manager. The options are: • **Auto**: IP Office automatically brings the SM Line to 'In Service' status as soon as it detects via the Reactive Monitoring that the Session Manager is reachable • **Manual**: When an SM line is in "Out of Service" state, IP Office does not bring it back to "In Service" status based on automatic detection. IP Office keeps the SM Line in "Out of Service" state until the administrator manually initiates Failback of IP Office from Session Manager.
Media Security	Default = Disable. Secure RTP (SRTP) can be used between IP devices to add additional security. These setting control whether SRTP is used for this device and the setting used for the SRTP. For further details of SRTP refer to Secure VoIP (SRTP). These settings apply only to centralized phones. 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.
Media Security Options	Not displayed if **Media Security** is disabled. The options are: • **Encryptions**: Default = RTP This setting allows selection of which parts of a media session should be protected using encryption. The default is to encrypt just the RTP stream (the speech). • **Authentication**: Default = RTP and RTCP This setting allows selection of which parts of the media session should be protected using authentication. The default is authenticate just the RTCP stream (call control signals). • **Replay Protection SRTP Window Size**: Default = 64. Currently not adjustable. • **Crypto Suites**: Default = SRTP_AES_CM_128_SHA1_80 and SRTP_AES_CM_128_SHA1_32.

Related Links

SM on page 243

Call Log

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

On Avaya phones with a fixed **Call Log** or **History** button (1400, 1600, 9500 and 9600 Series), that button can be used to display the user's centralized call log. The centralized call log is also used for M-Series and T-Series phone. The user can use the call log to make calls or to store as a personal

speed dial. They can also edit the call log to remove records. The same call log is also used if the user logs into one-X Portal for IP Office.

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

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

<table>
<tr><th>Field</th><th colspan="3">Description</th></tr>
<tr><td>Default Centralized Call Log On</td><td colspan="3">Default = On.

When selected, each user is defaulted to have the system store a call log of their calls. This call log is accessible on the phone when the user is using a phone with a Call Log or History button. The use of centralized call logging can be enabled/disabled on a per user basis using the Centralized Call Log user setting (User | Telephony | Call Log).</td></tr>
<tr><td rowspan="4">Log Missed Calls Answered at Coverage</td><td colspan="3">Default = Off.

This setting controls how calls to a user, that are answered by a covering user should be logged in the centralized call log. This option applies for calls answered elsewhere (covered) by pickup, call coverage (call coverage buttons or coverage group), bridged appearance button, user BLF, voicemail, etc.</td></tr>
<tr><td>Setting</td><td>Targeted User</td><td>Covering User</td></tr>
<tr><td>Off</td><td>Nothing</td><td>Answered Call</td></tr>
<tr><td>On</td><td>Missed Call</td><td>Answered Call</td></tr>
<tr><td>Log Missed Hunt Group Calls</td><td colspan="3">Default = Off. By default, hunt group calls are not included in any user's centralized call log unless answered by the user. If this option is selected, a separate call log is kept for each hunt group of calls that are not answered by anyone. It includes hunt group calls that go to voicemail.

If missed hunt group calls are also being logged, the system stores up to 10 call records for each hunt group. When this limit is reached, new call records replace the oldest record.

Within the user call log setting (User | Telephony | Call Log), the list of hunt groups allows selection of which hunt groups' missed call records should be displayed as part of the user's centralized call log.</td></tr>
</table>

Related Links

System | Telephony on page 224

TUI

This page is used to configure system wide telephony user interface (TUI) options.

These settings are mergeable.

Default Phone Display Options:

Use these settings to define the default phone display when feature menus are disabled. Note that for new users, the default phone display options are set to the system default values.

Feature menus can be disabled in one of two ways.

On **System | Telephony | TUI**, set the **Features Menu** to off. On **User | Telephony | TUI**, set the **User Setting** to **Same as System**.

On **User | Telephony | TUI**, set the **User Setting** to **Custom** and set the **Features Menu** to off.

Phone Type	Variable	Description
1400 1600	Display Name Preference	Defines the default value of the User's Features > Phone User > Phone Screen Settings > Display Name setting. Default = Off When enabled, displays the user name.
9500 9608 9611	Column View Preference	Defines the default value of the User's Features > Phone User > Phone Screen Settings > Display Mode setting. Default = Dual Column view can be Single or Dual.
9621 9641	Quick Touch Panel Lines	Defines the default value of the User's Features > Phone User > Phone Screen Settings > Quick Touch Lines setting. Default = Optimize Sets the Quick Touch Panel number. The options are 1, 2, and Optimize. When set to Optimize: • 9621 = 1 • 9641 = 2

Field	Description
Time Format	Default = Locale Defined. Set the system time format display. The default time format is defined by the **Locale** setting. You can override the default and set the time format to a 12- hour or 24-hour clock.
Features Menu Controls	
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) Forwarding Hot Desk Functions

Table continues…

Field	Description
	Passcode Change Phone Lock Self Administration Voicemail Controls For information on telephony features, see the IP Office Product Description.

Related Links

System | Telephony on page 224

System | Directory Services

Related Links

System on page 199
System | Directory Services | LDAP on page 249
System | Directory Services | HTTP on page 252

System | Directory Services | LDAP

The system supports LDAP Version 2. LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network. LDAP is lighter because in its initial version, it did not include security features.

The system supports the import of directory records from one system to another using HTTP. That includes using HTTP to import records that another system has learnt using LDAP. HTTP import, which is simpler to configure, can be used to relay LDAP records with LDAP configured on just one system.

LDAP records can contain several telephone numbers. Each will be treated as a separate directory record when imported into the system directory.

In a network, a directory tells you where in the network something is located. On TCP/IP networks, including the Internet, the Domain Name System (DNS) is the directory system used to relate the domain name to a specific network address. However, you may not know the domain name. LDAP allows you to search for an individual without knowing where they're located (although additional information will help with the search).

An LDAP directory is organized in a simple "tree" hierarchy consisting of the following levels:

- The "root" directory (the starting place or the source of the tree), which branches out to
- Countries, each of which branches out to
- Organizations, which branch out to

- Organizational units (divisions, departments, and so forth), which branches out to (includes an entry for)
- Individuals (which includes people, files, and shared resources such as printers)

An LDAP directory can be distributed among many servers. Each server can have a replicated version of the total directory that is synchronized periodically. An LDAP server is called a Directory System Agent (DSA). An LDAP server that receives a request from a user takes responsibility for the request, passing it to other DSA's as necessary, but ensuring a single coordinated response for the user.

LDAP Directory Synchronization allows the telephone number Directory held in the Control Unit to be synchronized with the information on an LDAP server. The feature can be configured to interoperate with any server that supports LDAP Version 2.

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

Field	Description
LDAP Enabled	Default = Off This option turns LDAP support on or off. The system uses LDAP Version 2. If the server being queried is an LDAP Version 3 server, support for LDAP Version 2 requests may need to be enabled on that server (all LDAP Version 3 servers support LDAP Version 2 but do not necessarily have it enabled by default).
User Name	Default = Blank Enter the user name to authenticate connection with the LDAP database. To determine the domain-name of a particular Windows 2000 user look on the "Account" tab of the user's properties under "Active Directory Users and Computers". Note that this means that the user name required is not necessarily the same as the name of the Active Directory record. There should be a built-in account in Active Directory for anonymous Internet access, with prefix "IUSR_" and suffix server_name (whatever was chosen at the Windows 2000 installation). Thus, for example, the user name entered is this field might be: IUSR_CORPSERV@example.com
Password	Default = Blank Enter the password to be used to authenticate connection with the LDAP database. Enter the password that has been configured under Active Directory for the above user. Alternatively an Active Directory object may be made available for anonymous read access. This is configured on the server as follows. In "Active Directory Users and Computers" enable "Advanced Features" under the "View" menu. Open the properties of the object to be published and select the "Security" tab. Click "Add" and select "ANONYMOUS LOGON", click "Add", click "OK", click "Advanced" and select "ANONYMOUS LOGON", click "View/Edit", change "Apply onto" to "This object and all child objects", click "OK", "OK", "OK". Once this has been done on the server, any record can be made in the User Name field in the System configuration form (however this field cannot be left blank) and the Password field left blank. Other non-Active Directory LDAP servers may allow

Table continues…

Field	Description
	totally anonymous access, in which case neither User Name nor Password need be configured.
Server IP Address	Default = Blank Enter the IP address of the server storing the database.
Server Port	Default = 389 This setting is used to indicate the listening port on the LDAP server.
Authentication Method	Default = Simple Select the authentication method to be used. The options are: • **Simple**: clear text authentication • **Kerberos**: Kerberos 4 LDAP and Kerberos 4 DSA encrypted authentication (for future use).
Resync Interval (secs)	Default = 3600 seconds. Range = 1 to 99999 seconds. The frequency at which the system should resynchronize the directory with the server. This value also affects some aspects of the internal operation. The LDAP search inquiry contains a field specifying a time limit for the search operation and this is set to 1/16th of the resync interval. So by default a server should terminate a search request if it has not completed within 225 seconds (3600/16). The client end will terminate the LDAP operation if the TCP connection has been up for more than 1/8th of the resync interval (default 450 seconds). This time is also the interval at which a change in state of the "LDAP Enabled" configuration item is checked.

Search Base/Search Filter	Default = Blank These 2 fields are used together to refine the extraction of directory records. Basically the Base specifies the point in the tree to start searching and the Filter specifies which objects under the base are of interest. The search base is a distinguished name in string form (as defined in RFC1779).
	The Filter deals with the attributes of the objects found under the Base and has its format defined in RFC2254 (except that extensible matching is not supported). If the Search Filter field is left blank the filter defaults to "(objectClass=*)", this will match all objects under the Search Base. The following are some examples applicable to an Active Directory database.
	• To get all the user phone numbers in a domain:
	`Search Base: cn=users,dc=acme,dc=com`
	`Search Filter: (telephonenumber=*)`
	• To restrict the search to a particular Organizational Unit (eg office) and get cell phone numbers also:
	`Search Base: ou=holmdel,ou=nj,DC=acme,DC=com`
	`Search Filter: (|(telephonenumber=*)(mobile=*))`
	• To get the members of distribution list "group1":

Table continues…

Field	Description
	Search Base: cn=users,dc=acme,dc=com Search Filter: (&(memberof=cn=group1,cn=users,dc=acme,dc=com)(telephonenumber=*))
Number Attributes	: Default = see below Enter the number attributes the server should return for each record that matches the Search Base and Search Filter. Other records could be ipPhone, otherIpPhone, facsimileTelephoneNumber, otherfacsimileTelephone Number, pager or otherPager. The attribute names are not case sensitive. Other LDAP servers may use different attributes. By default the record is "telephoneNumber,otherTelephone,homePhone=H,otherHomePhone=H,mobile=M, otherMobile=M", as used by Windows 2000 Server Active Directory for Contacts. The optional "=string" sub-fields define how that type of number is tagged in the directory. Thus, for example, a cell phone number would appear in the directory as: John Birbeck M 7325551234

Related Links

System | Directory Services on page 249

System | Directory Services | HTTP

The system can use HTTP to import the directory records held by another system. Note that support for HTTP can be disabled. The Avaya HTTP Clients Only setting (System | System) can restrict a system from responding to HTTP requests. The system's Unsecured Interface security settings also included controls for HTTP access (**HTTP Directory Read** and **HTTP Directory Write**).

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

For Server Edition, on Secondary Server, Expansion System (L) and Expansion System (V2) systems, the HTTP settings are automatically defaulted to obtain the system directory from the Primary Server.

Field	Description
Directory Type	Default = None (No HTTP import)/IP Office SCN on Server Edition. Set whether HTTP import should be used and the method of importation. The options are: • **None**: Do not use HTTP import. • **IP Office**: Import from the system at the IP address set in the **Source** field. • **IP Office SCN**: Import from a system in a multi-site network. The **Source** field is used to select the **Outgoing Line** ID that matches the H.323 line to the remote system.
Source	Default = Blank/9999 on Server Edition.

Table continues…

Field	Description
	The form of this field changes according to the **Directory Type** selection above. For IP Office this field requires the IP address of the other system. For IP Office SCN, the outgoing group ID of the line to the remote system is used. • **List**: Default = All This field sets what types of directory record should be imported. • **All**: Import the full set of directory records from the remote system. • **Config Only**: Import just directory records that are part of the remote system's configuration. Note that these will be treated as imported records and will not be added to the local systems own configuration records. • **LDAP Only**: Import just directory records that the remote system has obtained as the result of its own LDAP import. This allows LDAP directory records to be relayed from one system to another. • **HTTP Only**: Import just directory records that the remote system has obtained as the result of its own HTTP import. This allows HTTP directory records to be relayed from one system to another.
URI	Default = /system/dir/complete_dir_list?sdial=true This field is for information only and cannot be adjusted. The path shown changes to match the **List** setting above.
Resync Interval (secs)	Default = 3600 seconds. Set how often the system should request an updated import. When a new import is received, all previously imported records are discarded and the newly imported records are processed.

Related Links

System | Directory Services on page 249

System | System Events

The system supports a number of methods by which events occurring on the system can be reported. These are in addition to the real-time and historical reports available through the System Status Application (SSA).

Related Links

System on page 199
System Events | Configuration on page 253
System Events | Alarms on page 255

System Events | Configuration

This form is used for general configuration related to system alarms. For email alarms the SMTP tab is also used.

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

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. • 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 | System Events on page 253

System Events | Alarms

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 2 alarm destinations can be configured for SNMP, 2 for Syslog and 3 for SMTP email. For Server Edition, 5 SNMP alarms can be configured.	
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.
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 = 516. Range = 0 to 65535. The Syslog destination port. • **Protocol**: Default = UDP. Select UDP or TCP. • **Format**: Default = 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.

Table continues…

Field	Description
	• **Minor**: Minor, major, and critical events are sent. Warnings are not sent. • **Major**: Major and critical events are sent. Warnings and minor events will not be sent. • **Critical**: Only critical events are sent. •
Events	Default = None Sets which types of system events should be collected and sent. The table below lists the alarms associated with each type of event. Text in italics in the messages is replaced with the appropriate data. Items in [] brackets are included in the message if appropriate. The subject line of SMTP email alarms takes the form "System name: IP address - System Alarm".

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.

Table continues…

Type	Events	Event State	Message
			• 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.
		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
	Compact Flash Card	Change	The PC card in name has changed.
	Expansion Module	Operational	Expansion module name link is up.
		Failure	Expansion module name link is down.
		Error	Expansion module name link has a link error.
		Change	Expansion module name link has changed.
	Trunk	Operational	Trunk number (name) [on expansion module number] is now operational.

Table continues…

Type	Events	Event State	Message
		Failure	Trunk number (name) [on expansion module number] is down.
	Trunk	Trunk seize failure	Seize failure: Channel [number] or Port [number].
		Incoming call outgoing trunk failure	Incoming call outgoing trunk: Channel [number] or Port [number].
		CLI not delivered	CLI not delivered: Channel [number] or Port [number].
		DDI incomplete	DDI incomplete. Expected Number of digits: <number>.
		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.

Table continues…

Type	Events	Event State	Message
		Network link failure	Network Interface name (ip address) has been disconnected.
		Network link operational	Network Interface name (ip address) has been connected.
		System warm start	System has been restarted (warm start).
		System cold start	System has restarted from power fail (cold start).
		SNMP Invalid community	Invalid community specified in SNMP request.
License	**License Server**	Server operational	The license server is now operational.
		Server failure	The license server is no longer operational.
	License Key Failure	License Key Failure	
Loopback	**Loopback**	Near end line loopback	Trunk number (name) [on expansion module number] is in near end loopback.
		Near end payload loopback	Trunk number (name) [on expansion module number] is in near end loopback with payload.
		Loopback off	Trunk number (name) [on expansion module number] has no loopback.
Phone Change	**Phone Change**	Phone has been unplugged	The phone with id n has been removed from extension extension (unit, port number).
		Phone has been plugged in	The phone with type type (id number) has been plugged in for extension extension (unit, port number).
Quality of Service	**QoS Monitoring**	If Enable RTCP Monitor on Port 5005 is selected, any monitored calls that exceeds the set QoS Parameters 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

Table continues…

Type	Events	Event State	Message
		No incoming call route for call	The following line had no Incoming Call Route for a call. Line: <number> or Line Group ID: <number>.
		Installed hardware failure	Installed hardware failure details will be provided.
	System Shutdown		
	Running Backup		
	Emergency Calls	Emergency call successful	Successful Emergency Call | Emergency call! Location:location Dialled:dialled number Called:number sent on the line CallerID:ID Usr:user Extn:extension
		Emergency call failure	Failed Emergency Call | Emergency call! Location:location Dialled:dialled number FailCause:cause Usr:user Extn:extension

Related Links

System | System Events on page 253

System | SMTP

SMTP can be used as the method of sending system alarms. The email destination is set as part of the email alarms configured in System | System Events | Alarms.

SMTP can be used with Embedded Voicemail for Voicemail Email. The voicemail destination is set by the user's Voicemail Email address.

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 This field sets the IP address of the SMTP server being used to forward SNMP alarms sent by email.
Port	Default = 25. Range = 0 to 65534. This field set the destination port on the SMTP server.
Email From Address	Default = Blank This field set the sender address to be used with mailed alarms. Depending of the authentication requirements of the SMTP server this may need to be a valid

Table continues…

Field	Description
	email address hosted by that server. Otherwise the SMTP email server may need to be configured to support SMTP relay.
Use STARTTLS	Default = Off. (Release 9.0.3). Select this field to enable TLS/SSL encryption. Encryption allows voicemail-to-email integration with hosted email providers that only permit SMTP over a secure transport.
Server Requires Authentication	Default = On This field should be selected if the SMTP server being used requires authentication to allow the sending of emails. When selected, the User Name and Password fields become available
User Name	Default = Blank This field sets the user name to be used for SMTP server authentication.
Password	Default = Blank This field sets the password to be used for SMTP server authentication.
Use Challenge Response Authentication (CRAM-MD5)	Default = Off. This field should be selected if the SMTP uses CRAM-MD5.

Related Links

System on page 199

System | SMDR

Using a specified IP address, the system can send a call record for each completed call.

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

Note:

Outbound Contact Express does not generate SMDR records.

Field	Description
Output	Default = No Output. Select the type of call record that the system should output via IP. The options are: • **No Output** • **SMDR Only** : Send call records using the SMDR settings below.
SMDR: Station Message Detail Recorder Communications This fields are available when SMDR is selected as the output. For information on SMDR record details, see the appendix.	
IP Address	Default = 0.0.0.0 (Listen).

Table continues…

Field	Description
	The destination IP address for SMDR records. The address 0.0.0.0 puts the control unit in listen mode on the specified TCP port. When a connection is made on that port, all SMDR records in the buffer are provided.
TCP Port	Default = 0. The destination IP port for SMDR records.
Records to Buffer	Default = 500. Range = 10 to 3000. The system can cache up to 3000 SMDR records if it detects a communications failure with destination address. If the cache is full, the system will begin discarding the oldest records for each new record.
Call Splitting for Diverts	Default = Off. When enabled, for calls forwarded off-switch using an external trunk, the SMDR produces separate initial call and forwarded call records. This applies for calls forwarded by forward unconditional, forward on no answer, forward on busy, DND or mobile twinning. It also applies to calls forwarded off-switch by an incoming call route. The two sets of records will have the same Call ID. The call time fields of the forward call record are reset from the moment of forwarding on the external trunk.

Related Links

System on page 199

System | Twinning

These settings are used with Mobile Twinning, see the **User | Mobility** tab for further details.

On mobile twinned calls, if the original party information is used or a specific calling party information CLI is set, that number overrides setting the outgoing CLI using short codes.

Warning:

Outgoing CLI

Changing the outgoing CLI for calls requires the line provider to support that function. You must consult with your line provider before attempting to change the outgoing CLI, failure to do so may result in loss of service. If changing the outgoing CLI is allowed, most line providers required that the outgoing CLI used matches a number valid for return calls on the same trunks. Use of any other number may cause calls to be dropped or the outgoing CLI to be replaced with a valid number.

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

Field	Description
Send Original Party Information for Mobile Twinning	Default = Off

Table continues…

Field	Description
	When on, the system will attempt to send the ICLID information provided with the incoming call to the twinning destination. • The SIP line **Send Caller ID** setting takes priority. • The values on the System | Twinning tab override the SIP lines **Send Caller ID** setting.
Calling Party Information for Mobile Twinning	Default = Blank (Disabled). Range = Up to 32 digits. This field is usable when **Send Original Party Information for Mobile Twinning** is off. Note that the number entered here for use as the CLI must be a valid number for return calls to the same site. Some line providers may reject calls that use a number that is not valid for return calls to the same site. In addition depending on the line type and line provider settings the maximum number of digits may be limited.

Related Links

System on page 199

System | VCM

This form allows adjustment of the operation of any Voice Compression Modules (VCM's) installed in a control unit.

Calls to and from IP devices can require conversion to the audio codec format being used by the IP device. For systems this conversion is done by voice compression channels. These support the common IP audio codecs G.711, G.723 and G.729a. For details of how to add voice compression resources to a system, refer to the IP Office Installation Manual.

These settings should only be adjusted under the guidance of Avaya support.

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

When are Voice Compression Channels Used

IP Device to Non-IP Device: These calls require a voice compression channel for the duration of the call. If no channel is available, busy indication is returned to the caller.

IP Device to IP Device: Call progress tones (for example dial tone, secondary dial tone, etc) do not require voice compression channels with the following exceptions:

- Short code confirmation, ARS camp on and account code entry tones require a voice compression channel.
- Devices using G.723 require a voice compression channel for all tones except call waiting.

When a call is connected:

- If the IP devices use the same audio codec no voice compression channel is used.
- If the devices use differing audio codecs, a voice compression channel is required for each.

Non-IP Device to Non-IP Device: No voice compression channels are required.

Music on Hold: This is provided from the system's TDM bus and therefore requires a voice compression channel when played to an IP device.

Conference Resources and IP Devices: Conferencing resources are managed by the conference chip which is on the system's TDM bus. Therefore, a voice compression channel is required for each IP device involved in a conference. This includes services that use conference resources such as call listen, intrusion and silent monitoring. They also apply to call recording.

Page Calls to IP Device: Page calls require 1 voice compression channel per audio codec being used by any IP devices involved. The system only uses G.729a for page calls, therefore only requiring one channel but also only supporting pages to G.729a capable devices.

Voicemail Services and IP Devices: Calls to the system voicemail servers are treated as data calls from the TDM bus. Therefore calls from an IP device to voicemail require a voice compression channel.

Fax Calls: These are voice calls but with a slightly wider frequency range than spoken voice calls. The system only supports fax across IP between systems with the Fax Transport option selected.

SIP Calls:

- **SIP Line Call to/from Non-IP Devices**: Voice compression channel required.
- **Outgoing SIP Line Call from IP Device**: No voice compression channel required.
- **Incoming SIP Line Call to IP Device**: Voice compression channel reserved until call connected.

T38 Fax Calls: The system supports T38 fax on SIP trunks and SIP extensions. Each T38 fax call uses a VCM channel.

- Within a multi-site network, an T38 fax call can be converted to a call across across an H.323 line between systems using the **Fax Transport Support** protocol. This conversion uses 2 VCM channels.
- In order use T38 Fax connection, the **Equipment Classification** of an analog extension connected to a fax machine can be set **Fax Machine**. Additionally, the short code feature **Dial Fax** is available.

Note:

T3 IP devices must be configured to 20ms packet size for the above conditions to apply. If left configured for 10ms packet size, a voice compression channel is needed for all tones and for non-direct media calls.

Measuring Channel Usability

The System Status Application can be used to display voice compression channel usage. Within the Resources section it displays the number of channel in use. It also displays how often there have been insufficient channels available and the last time such an event occurred.

Field	Description
Echo Return Loss (dB)	Default = 6dB. IP500 VCM, IP500 VCM V2 and IP500 Combination Cards. This control allows adjustment of expected echo loss that should be used for the echo cancellation process.

Table continues…

Field	Description
	Echoes are typically generated by impedance mismatches when a signal is converted from one circuit type to another, most notably from analog to IP. To resolve this issue, an estimated echo signal can be created from one output and then subtracted from the input to hopefully remove any echo of the output. The options are: • **0dB** • **3dB** • **6dB** • **9dB**
Nonlinear Processor Mode	Default = Adaptive. I A low level of comfort noise is required on digital lines during periods where there would normally be just silence. This is necessary to reassure users that the call is still connected. These controls allow adjustment of the comfort noise generated by the nonlinear processor (NLP) component of the VCM. The options are: • **Adaptive**: Adaptive means the comfort noise generated by the NLP will try to match background noise. • **Silence**: Silence means the NLP will not generate comfort noise at all • **Disabled**: Nonlinear processing is not applied, in which case some residual echo may be heard.
NLP Comfort Noise Attenuation	Default = -9dB. The options are: • **-3dB** • **-6dB** • **-9dB**
NLP Comfort Noise Ceiling	Default =-30dB. The options are: • **-30dB** • **-55dB**
Modem For Fax relay, these settings allow adjustment of the TDM side operation applied to fax calls using VCM channels.	
Tx Level (dB)	Default = -9dB. Range = 0 to -13dB.
CD Threshold	Default = -43dB, Options = -26dB, -31dB or -43dB.
No Activity Timeout (secs)	Default = 30 seconds. Range = 10 to 600 seconds.

Related Links

System on page 199

System | CCR

Customer Call Reporter (CCR) is an application that collects and displays information on the current status of hunt groups and users that have been configured for Customer Call Reporter operation. CCR is not supported by Server Edition.

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

Field	Description
Busy Not Available Reason Codes Agents who indicate that they are in a 'busy not available' state can be prompt to also indicate the reason for being in that state. This menu allows descriptions for the possible reasons to be entered. The descriptions are then used in menus from which the Agent's make selections when setting themselves into busy not available state and in reports on Agent status.	
Code/Reason	Rows 1 to 8 can be used to contain descriptions of up to 31 characters each. Rows **0** and **9** are fixed as **Unsupported** and **Busy Not Available**. For Customer Call Reporter 6.1, the reason codes are used to categorize calls in the Agent Time Card report. Reason 1 is used to define lunch. All other reason codes are reported as breaks.
Default After Call Work Time (seconds)	Default = 10. Range = 10 to 999 seconds. If an agent goes into the After Call Work (ACW) state, either automatically or manually, this field sets the duration of that state after which it is automatically cleared. This duration can be overridden by the Agent's own setting (User | Telephony | Supervisor Settings | After Call Work Time). During ACW state, hunt group calls are not presented to the user.

Related Links

System on page 199

System | Codecs

This tab is used to set the codecs available for use with all IP (H.323 and SIP) lines and extensions and the default order of codec preference.

- Avaya H.323 telephones do not support G.723 and will ignore it if selected.
- For systems with H.323 lines and extensions, one of the G.711 codecs must be selected and used.
- G.723 is not supported by Linux based systems.
- The number of channels provided by an IP500 VCM 32 or IP500 VCM 64 card, up to a maximum of 32 or 64 respectively, depends on the actual codecs being used. This also applies to IP500 VCM 32 V2 and IP500 VCM 64 V2 cards. The following table assumes that all calls using the VCM use the same codec.

Codec	IP500 VCM 32 IP500 VCM 32 V2	IP500 VCM 64 IP500 VCM 64 V2
G.711	32	64
G.729a	30	60
G.723	22	44
G.722	30	60

When paging, always use only one codec (the preferred). It is the system administrator's responsibility to ensure all the phones in the paging group support the codec.

Usability

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

Field	Description
RFC2833 Default Payload	Default = 101. Range = 96 - 127. This field specifies the default value for RFC2833 dynamic payload negotiation. Service providers that do not support dynamic payload negotiation may require a fixed value.
Available Codecs	This list shows the codecs supported by the system and those selected as usable. Those codecs selected in this list are then available for use in other codec lists shown in the configuration settings. For example the adjacent **Default Selection** list and the individual custom selection list on IP lines and extensions. **Warning:** Removing a codec from this list automatically removes it from the codec lists of any individual lines and extensions that are using it. The 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 system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition it is supported on Primary Server, Secondary Server and Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo.
Default Codec Selection	By default, all IP (H.323 and SIP) lines and extensions added to the system have their **Codec Selection** setting set to **System Default**. That setting matches the codec selections made in this list. The buttons between the two lists can be used to move codecs between the **Unused** and the **Selected** parts of the list and to change the order of the codecs in the selected codecs list.

Related Links

System on page 199

System | VoIP Security

Use this tab to set system level media security settings. These settings apply to all lines and extensions on which SRTP is supported and which have their **Media Security** settings configured to be **Same as System**. Individual lines and extensions have media security settings that can override system level settings.

Simultaneous SIP extensions that do not have physical extensions in the configuration use the system security settings.

SM lines and all centralized user extensions must have uniform media security settings.

Field	Description
Media Security	Default = Disabled. Secure RTP (SRTP) can be used between IP devices to add additional security. These settings control whether SRTP is used for this system and the settings used for the SRTP. The options are: • **Disabled**: 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.
Media Security Options	Not displayed if **Media Security** is set to **Disabled**. The options are: • **Encryptions**: Default = RTP This setting allows selection of which parts of a media session should be protected using encryption. The default is to encrypt just the RTP stream (the speech). • **Authentication**: Default = RTP and RTCP This setting allows selection of which parts of the media session should be protected using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Currently not adjustable. • **Crypto Suites**: Default = SRTP_AES_CM_128_SHA1_80. There is also the option to select SRTP_AES_CM_128_SHA1_32.
Strict SIPS	(Enterprise Branch deployments) Default = Off. This option provides a system-wide configuration for call restrictions based on SIPS URI. When this option is off, calls are not rejected due to SIPS. A call is sent according to the configuration of the outgoing trunk or line that it is routed to, regardless of the way the call came in, even if the call came in as a SIP invite with SIPS URI and is being sent with a SIP URI onto a non-secure SIP trunk.

Table continues…

Field	Description
	When this option is on, an incoming SIP invite with SIPS URI if targeted to a SIP trunk (SM line or SIP line) is rejected if the target trunk is not configured with SIPS in the URI Type field.

Related Links

System on page 199

Dialer

Use this tab to configure the functions required for an Outbound Contact Express deployment.

These settings are mergeable. However, changes to the **Operation** field or to the **Trunk Range / IP Office** table require a reboot.

It is recommended that you do not change the mergeable settings while the system is in use.

<table>
<tr><th>Field</th><th colspan="3">Description</th></tr>
<tr><td>Operation</td><td colspan="3">Default = Off.

On the primary IP Office Server Edition server, set this field to Primary. For all other IP Office servers, set this field to Child. When set to Off or Child, no other fields are displayed.</td></tr>
<tr><td>Record Mode</td><td colspan="3">Default = Off

Defines the automatic call recording function on VMPro. The options are:

• Whole Call: The entire call is recorded.

• Agent Connected: Recording starts once the conversation begins.

• Off</td></tr>
<tr><td>Record Controls</td><td colspan="3">: Default = Full Defines what functions an agent can perform from WebAgent or from the handset. The options are:

• Full

• Pause

• Off</td></tr>
<tr><td>Record Mode and Record Controls</td><td colspan="3">Record Mode and Record Controls are related. The combined configuration settings are listed below.

Note that stopping and starting the recording creates multiple recording files. Pausing and resuming the recording keeps the recording in a single file.</td></tr>
<tr><td></td><td>Record Mode</td><td>Record Controls</td><td>Result</td></tr>
<tr><td></td><td>Off</td><td>Off</td><td>Calls are not recorded.</td></tr>
</table>

Table continues…

Field	Description		
	Agent Connected	Off	All calls are always recorded from the time the agent joins the call.
	Agent Connected	Pause	All calls are always recorded but the Agent can pause and resume recording.
	Agent Connected	Full	All calls are always recorded from the time the Agent joins the call. Agent has full control on when calls get recorded.
	Whole Call	Off	All calls are always recorded from the time the customer answers.
	Whole Call	Pause	All calls are always recorded from the time the customer answers but the Agent can pause and resume the recording.
	Whole Call	Full	Call recording starts before the agent is connected. All calls are always recorded but the Agent can pause and resume the recording
Agent Call Back Time	Default = 60. Range = 30 - 300. The number of seconds an agent has to make a manual call after a customer hang up. Used when a customer wants to be called on a different number.		
Remote Agent Display Text	Default = Blank. Maximum length = 33. Specify the text string displayed on the remote agent extension if that extension supports displays and the protocol allows it to be transmitted.		
Remote Agent Confirmation Voice Prompt	Default = Blank. Maximum length = 31. Specify the Call Flow Entry point name used to play a greeting to the remote agent when they log in. The actual Entry Point is added as a Modules Entry point using the VMPro Client. The entry point cannot be added as a short code, user or group entry point.		
Remote Agent First Extension Number	Default = 0. The first extension number allocated to a remote agent. It must not conflict with the existing dialing plan. If the range contains existing user extensions, they are used when assigning extensions to remote users.		
Remote Agent Number of Extensions	Default = 0. Maximum = 500. The range of extensions starting from the one above. A user is created for every extension. If the field is edited and the number of extensions is reduced, the number of remote agents that can log in is reduced to the new setting. However, reducing the range does not automatically delete previously created users. Users can only be deleted manually.		

Table continues…

Field	Description
Use Custom Hold Treatment	Default = unchecked. Defines system behavior when a call is placed on hold. When unchecked the the system **Hold Music** setting is used for the system's music on hold source. When checked, the music on hold source is VMPro.
Record while on Hold	Default = unchecked. When the **Use Custom Hold Treatment** box is checked, the **Record while on Hold** setting can be enabled. When unchecked, recording is paused when the call is on hold. When checked, recording continues when the call is on hold.
Trunk Range / IP Office	The number of trunks used by Outbound Contact Express. The default entry is **Trunk Range**: **1-250** for the Primary (**Local**) server. 250 is the maximum number of trunks configured on a single server. Use this table to define the number of trunks managed by the Primary and Secondary systems. The trunk range must match the line numbers used by the Proactive Contact Dialer. Enter only one range per server.

Related Links

System on page 199

System | Contact Center

The Contact Center tab contains the user information required by IP Office to synchronize account information with an an Avaya Contact Center Select (ACCS) system. The information is synchronized using the Contact Center Management Application (CCMA). These settings are only used for the deployment of an ACCS system.

This tab is visible on the Server Edition Primary Server and Standard Mode IP 500 V2 systems.

These settings are mergeable.

Field	Description
Contact Center Application	Default = None. The options are • Avaya Contact Center Select • Avaya IP Office Contact Center
Synchronize to this System	Default = Off. When set to On, the CCMA fields below are enabled.
CCMA Address	Default = Blank Address of the Contact Center Management Application system.
CCMA Username	Default = Blank User name on the Contact Center Management Application system.
CCMA Password	Default = Blank Password on the Contact Center Management Application system.

Related Links

System on page 199

Line

The line settings shown in the system configuration will change according to the types of trunk cards installed in the control unit or added using external expansion modules.

Warning:

Changing Trunk Cards Changing the trunk card installed in an control unit will result in line settings for both the previous trunk card and the currently installed trunk card. In order to change the trunk card type in a particular card slot, the configuration must be defaulted. This does not apply if replacing an existing card with one of a higher capacity or fitting a trunk card into a previously unused slot.

Trunk Incoming Call Routing

Each trunk type can be categorized as either an external trunk or internal trunk. The trunk type affects how the system routes calls received on that trunk and the routing of calls to the trunk.

	External Trunks	Internal Trunks
Trunk Types	**Analog trunks** **T1 Robbed Bit** **E1R2** **ISDN BRI** (excluding So) **ISDN PRI T1** **ISDN PRI E1** **SIP**	**QSIG** (T1, E1 or H.323) **BRI So** **H.323** **SCN** **SES** **SM Line**
Incoming Calls Routed by	All incoming calls are routed by comparison of call details for matches within the system Incoming Call Routes. Line short codes are not used.	Incoming calls are routed by looking for a match to the incoming digits in the following order: • Extension number. • Trunk short codes (excluding ? short code). • System short codes (excluding ? short code). • Trunk ? short code. • System ? short code.

Line Groups

Each system trunk (or in some cases individual trunk channels) can be configured with an **Incoming Group ID** and an **Outgoing Group ID**. These group IDs are used as follows:

-  Incoming Call Routes For incoming calls on external trunks, the Incoming Group ID of the trunk is one of the factors used to match the call to one of the configured incoming call routes.
-  Short Codes - Routing Outgoing Calls For dialing which matches a short code set to a **Dial** feature, the short codes **Line Group ID** can indicate either an ARS form or to use a trunk from set to the same **Outgoing Group ID**. If the call is routed to an ARS form, the short codes in the ARS form will specify the trunks to use by matching **Outgoing Group ID**.

Removing Unused Trunks

In cases where a trunk card is installed but the trunk is not physically connected, it is important to ensure that the trunk is disabled in the configuration. This can be done on most trunks using by setting the line's **Admin** setting to **Out of Service**.

This is especially important with analog trunks. Failure to do this may cause the system to attempt to present outgoing calls to that trunk. Similarly, where the number of channels subscribed is less than those supportable by the trunk type, the unsubscribed channels should be disabled.

Clock Quality

Calls between systems using digital trunks (for example E1, E1R2, T1 PRI and BRI) require an common clock signal. The system will try to obtain this clock signal from an exchange through one of its digital trunks. This is done by setting the Clock Quality setting of that Line to Network. If there are multiple trunks to public exchanges, another trunk can be set as Fallback should the primary clock signal fail. Other trunks should be set as Unsuitable.

Related Links

Configuration Mode Field Descriptions on page 193
Analog Line on page 274
BRI Line on page 281
PRI Trunks on page 287
S0 Line on page 312
H.323 Line on page 315
IP DECT Line on page 327
SIP Line on page 336
Line | SIP DECT Line on page 365
Line | SM Line on page 367
Line | IP Office Line on page 374

Analog Line

Analog trunks can be provided within the systems in the following ways. In all cases the physical ports are labeled as Analog. For full details of installation refer to the IP Office Installation manual.

Using ICLID: The system can route incoming calls using the ICLID received with the call. However ICLID is not sent instantaneously. On analog trunks set to Loop Start ICLID, there will be a short delay while the system waits for any ICLID digits before it can determine where to present the call.

Line Status: Analog line do not indicate call status other than whether the line is free or in use. Some system features, for example retrieving unanswered forwards and making twinned calls make use of the call status indicated by digital lines. This is not possible with analog lines. Once an analog line has been seized, the system has to assume that the call is connected and treats it as having been answered.

Dialing Complete: The majority of North-American telephony services use en-bloc dialing. Therefore the use of a ; is recommended at the end of all dialing short codes that use an N. This is also recommended for all dialing where secondary dial tone short codes are being used.

Ground Start: This type of analog trunk is only supported through the Analog Trunk external expansion module.

Related Links

Line on page 272
Line | Line Settings (Analog) on page 274
Line | Analog Options on page 276

Line | Line Settings (Analog)

This tab covers general settings for an analog line.

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

Field	Description
Line Number	This parameter is not configurable, it is allocated by the system.
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Network Type	Default = Public.

Table continues…

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>This option is available if Restrict Network Interconnect (System | Telephony | Telephony) is enabled. It allows the trunk to be set as either Public or Private. The system will return number busy indication to any attempt to connect a call on a Private trunk to a Public trunk or vice versa. This restriction includes transfers, forwarding and conference calls.

Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.</td></tr>
<tr><td>Telephone Number</td><td>Used to remember the external telephone number of this line to assist with loop-back testing. For information only.</td></tr>
<tr><td>Incoming Group ID</td><td>Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.</td></tr>
<tr><td>Outgoing Group ID</td><td>Default = 0, Range 0 to 99999.

Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID.

For Basic Edition and Standard Edition deployments, the same ID can be used for multiple lines.

In a Server Edition network, the Outgoing Group ID used on a system must also be unique within the network, ie. the same ID cannot be used in the configuration of any lines on another server system in the network.
<table>
<tr><th>Reserved Group ID numbers</th><th>Description</th></tr>
<tr><td>90000 - 99999</td><td>Reserved for system use (not enforced).</td></tr>
<tr><td>99999 and 99998</td><td>In a Server Edition network, reserved for the H.323 lines to the Primary Server and Secondary Server respectively.</td></tr>
<tr><td>999901 to 99930</td><td>In a Server Edition network, reserved for the H.323 lines from the Primary Server to each expansion system in the network.</td></tr>
<tr><td>0</td><td>In a Server Edition network, the ID 0 cannot be used.</td></tr>
<tr><td>98888</td><td>For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.</td></tr>
</table></td></tr>
<tr><td>Outgoing Channels</td><td>Default = 1 (not changeable)</td></tr>
<tr><td>Voice Channels</td><td>Default = 1 (not changeable)</td></tr>
<tr><td>Prefix</td><td>Default = Blank

Enter the number to prefix to all incoming numbers for callback. This is useful if all users must dial a prefix to access an outside line. The prefix is automatically placed in front of all incoming numbers so that users can dial the number back.

For outgoing calls: The system does not strip the prefix, therefore any prefixes not suitable for external line presentation should be stripped using short codes.</td></tr>
</table>

Table continues…

Field	Description
Line Appearance ID	Default = Auto-assigned. Range = 2 to 9 digits. Allows a number to be assigned to the line to identify it. On phone's that support call appearance buttons, a Line Appearance button with the same number will show the status of the line and can be used to answer calls on the line.The line appearance ID must be unique and not match any extension number.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.

Related Links

Analog Line on page 274

Line | Analog Options

This tab covers analog line specific settings. The system wide setting **CLI Type** (**System | Telephony | Tones & Music**) is used for to set the incoming CLI detection method for all analogue trunks.

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

Field	Description
Channel	Set by the system. Shown for information only.
Trunk Type	Default = Loop Start Sets the analog line type. The options are: • **Ground Start**: Ground Start is only supported on trunks provided by the Analog Trunk 16 expansion module. It requires that the module and the control unit are grounded. Refer to the IP Office installation manual. • **Loop Start** • **Loop Start ICLID**: As the system can use ICLID to route incoming calls, on analog Loop Start ICLID trunks there is a few seconds delay while ICLID is received before the call routing can be determined.
Signaling Type	Default = DTMF Dialing Sets the signaling method used on the line. The options are: • **DTMF Dialing** • **Pulse Dialing**
Direction	Default = Both Directions Sets the allowed direction of operation of the line. The options are: • **Incoming** • **Outgoing** • **Both Directions**

Table continues…

Field	Description
Flash Pulse Width	Default = 500ms. Range = 0 to 2550ms. Set the time interval for the flash pulse width.
Await Dial Tone	Default = 3000ms. Range = 0 to 25500ms. Sets how long the system should wait before dialing out.
Echo Cancellation	Default = 16ms. The echo cancellation should only be adjusted as high as required to remove echo problems. Setting it to a higher value than necessary can cause other distortions. Not used with external expansion module trunks. The options are (milliseconds): • **Off** • **8** • **16** • **32** • **64** • **128**
Echo Reduction	Default = On. (ATM4Uv2 card only) Used when impedance matching is not required but echo reduction is.
Mains Hum Filter	Default = Off. If mains hum interference on the lines is detected or suspected, this settings can be used to attempt to remove that interference. Useable with ATM16 trunks and IP500 ATM4U trunks. The options are: • **Off** • **50Hz** • **60Hz**
Impedance	Set the impedance used for the line. This field is only available for certain system locales. The value used for **Default** is set by the system **Locale**. • **Brazil**: Default = 900R Adjustable between 600R and 900R as required by the line provider. • **Korea**: Default = Default (600ohms). In addition to the default impedance settings, an alternate set of impedance values can be selected. • **United States**: Default = Default (600 ohms). In addition to the default impedance setting, the following alternate sets of impedance values **Alternate1**, **Alternate2** and **Alternate3** can be selected. • The following values are used for **Automatic Impedance Matching**: 600+2150nF, 600, 900+2150nF, 900, 220+820||115nF, 370+620||310nF, 270+750||150nF, 320+1050||230nF, 350+1000||210nF, 800+100||210nF.
Quiet Line	This field is only available for certain system locales (see above). The setting may be required to compensate for signal loss on long lines.

Table continues…

Field	Description
Digits to break dial tone	Default = 2. Range = Up to 3 digits. During automatic impedance testing (see below), once the system has seized a line, it dials this digit or digits to the line. In some cases it may be necessary to use a different digit or digits. For example, if analog trunk go via another PBX system or Centrex, it will be necessary to use the external trunk dialing prefix of the remote system plus another digit, for example 92.
Automatic	Default = Yes. (ATM4Uv2 card only) When set to **Yes**, the **Default** value is used. The value used for **Default** is set by the system **Locale**. When set to **No**, the **Impedance** value can be manually selected from the list of possible values: 600 900 270+(750R || 150nF) and 275R + (780R || 150nF) 220+(820R || 120nF) and 220R+ (82R || 115nF) 370+(620R || 310nF) 320+(1050R || 230nF) 370+(820R || 110nF) 275+(780R || 115nF) 120+(820R || 110nF) 350+(1000R || 210nF) 200+(680R || 100nF) 600+2.16µF 900+1µF 900+2.16µF 600+1µF Global Impedance
Automatic Balance Impedance Match	These controls can be used to test the impedance of a line and to then display the best match resulting from the test. Testing should be performed with the line connected but the system otherwise idle. To start testing click **Start**. The system will then send a series of signals to the line and monitor the response, repeating this at each possible impedance setting. Testing can be stopped at any time by clicking **Stop**. When testing is complete, Manager will display the best match and ask whether that match should be used for the line. If **Yes** is selected, Manager will also ask whether the match should be applied to all other analog lines provided by the same analog trunk card or module. Note that on the Analog Trunk Module (ATM16), there are four control devices, each supporting four channels. The impedance is set by the control device for all four channels under its control. Consequently, the impedance match tool only functions on lines 1, 5, 9, and 13.

Table continues…

Field	Description
	Before testing, ensure that the system **Locale** setting (**System | System**) is correctly set. Also check that the system **Companding Law** settings (**System | Telephony | Telephony**) are set correctly. If either needs to be changed, make the required change and save the setting to the system before proceeding with impedance matching. Due to hardware differences, the impedance matching result will vary slightly depending on which type of trunk card or expansion module is being used. **Automatic Balance Impedance Matching**, **Quiet Line** and **Digits to break dial tone** are available for the Bahrain, Egypt, French Canadian, Kuwait, Morocco, Oman, Pakistan, Qatar, Saudi Arabia, South Africa, Turkey, United Arab Emirates, United States and Customize locales.
Allow Analog Trunk to Trunk Connect	Default = Not selected (Off). When not enabled, users cannot transfer or forward external calls back off-switch using an analog trunk if the call was originally made or received on another analog trunk. This prevents transfers to trunks that do not support disconnect clear. If the **Unsupervised Analog Trunk Disconnect Handling** setting (**System | Telephony | Telephony**) is enabled, this setting is greyed out and trunk to trunk connections to any analog trunks are not allowed.
BCC	Default = Not selected [Brazil locale only] A collect call is a call at the receiver's expense and by his permission. If supported by the line provider, BCC (Block Collect Call) can be used to bar collect calls.
Secondary Dial Tone	Default = Off Configures the use of secondary dial tone on analog lines. This is a different mechanism from secondary dial tone using short codes. This method is used mainly within the Russian locale. When selected, the options are: • **Await time:** Default = 3000ms. Range = 0 to 25500ms. Used when secondary dial tone (above) is selected. Sets the delay. • **After n Digits**: Default = 1. Range = 0 to 10. Sets where in the dialing string, the delay for secondary dial tone, should occur. • **Matching Digit**: Default =8. Range = 0 to 9. The digit which, when first matched in the dialing string, will cause secondary dial tone delay.
Long CLI Line	Default = Off The CLI signal on some analog lines can become degraded and is not then correctly detected. If you are sure that CLI is being provided but not detected, selecting this option may resolve the problem.
Modem Enabled	Default = Off The first analog trunk in a control unit can be set to modem operation (V32 with V42 error correction). This allows the trunk to answer incoming modem calls and be used for system maintenance. When on, the trunk can only be used for analog modem calls. The default system short code *9000* can be used to toggle this setting.

Table continues…

Field	Description
	For the IP500 ATM4 Uni Trunk Card Modem, it is not required to switch the card's modem port on/off. The trunk card's V32 modem function can be accessed simply by routing a modem call to the RAS service's extension number. The modem call does not have to use the first analog trunk, instead the port remains available for voice calls.
MWI Standard	Default = None. Release 9.0.3+ When the **System | Voicemail | Voicemail Type** is set to **Analogue MWI**, change this setting to **Bellcore FSK**.
Pulse Dialing	These settings are used for pulse dialing. • **Mark**: Default = 80 (80ms). Range = 0 to 255. Interval when DTMF signal is kept active during transmission of DTMF signals. • **Space**: Default = 80 (80ms). Range = 0 to 255. Interval of silence between DTMF signal transmissions. • **Inter-Digit Pause**: Default = 500ms. Range = 0 to 2550ms. Sets the pause between digits transmitted to the line.
Ring Detection	These settings are used for ring detection. • **Ring Persistency**: Default = Set according to system locale. Range = 0 to 2550ms. The minimum duration of signal required to be recognized. • **Ring Off Maximum**: Default = Set according to system locale. Range = 0 to 25500ms. The time required before signaling is regarded as ended.
Disconnect Clear	Disconnect clear (also known as 'Line Break' or 'Reliable Disconnect') is a method used to signal from the line provider that the call has cleared. The system also uses 'Tone Disconnect', which clears an analog call after 6 seconds of continuous tone, configured through the Busy Tone Detection (**System | Telephony | Tones & Music**) settings. • **Enable:** Default = On Enables the use of disconnect clear. • **Units**: Default = 500ms. Range = 0 to 2550ms. This time must be less than the actual disconnect time period used by the line provider by at least 150ms. If the **Unsupervised Analog Trunk Disconnect Handling** setting (**System | Telephony | Telephony**) is enabled, this setting is greyed out and disconnect clear disabled..
DTMF	These settings are used for DTMF dialing. • **On**: Default = 40ms. Range = 0 to 255ms. The width of the on pulses generated during DTMF dialing. • **Off**: Default = 60ms. Range = 0 to 255ms. The width of the off pulses generated during DTMF dialing.
BCC Flash Pulse Width	[Brazil locale only] Default = 100 (1000ms). Range = 0 to 255. Sets the BCC (Block collect call) flash pulse width.

Table continues…

Field	Description
Gains	These settings are used to adjust the perceived volume on all calls. • **A | D**: Default = 0dB. Range =-10.0dB to +6.0dB in 0.5dB steps. Sets the analog to digital gain applied to the signal received from the trunk by the system. To conform with the Receive Objective Loudness Rating at distances greater than 2.7km from the central office, on analog trunks a receive gain of 1.5dB must be set. • **D | A**: Default = 0dB. Range =-10.0dB to +6.0dB in 0.5dB steps. Sets the digital to analog gain applied to the signal from the system to the trunk. • **Voice Recording**: Default = Low Used to adjust the volume level of calls recorded by voicemail. The ptions are: - **Low** - **Medium** - **High**

Related Links

Analog Line on page 274

BRI Line

BRI trunks are provided by the installation of a BRI trunk card into the control unit. The cards are available in different variants with either 2 or 4 physical ports. Each port supports 2 B-channels for calls. For full details of installation refer to the IP Office Installation manual.

Point-to-Point or Multipoint

BRI lines can be used in either Point-to-Point or Point-to-Multipoint mode. Point-to-Point lines are used when only one device terminates a line in a customer's office. Point-to-Multipoint lines are used when more than one device may be used on the line at the customer's premises. There are major benefits in using Point-to-Point lines:-

- The exchange knows when the line/terminal equipment is down/dead, thus it will not offer calls down that line. If the lines are Point-to-Multipoint, calls are always offered down the line and fail if there is no response from the terminal equipment. So if you have two Point-to-Multipoint lines and one is faulty 50% of incoming calls fail.
- You get a green LED on the Control Unit when the line is connected. With Point-to-Multipoint lines some exchanges will drop layer 1/2 signals when the line is idle for a period.
- The timing clock is locked to the exchange. If layer 1/2 signals disappear on a line then the Control Unit will switch to another line, however this may result in some audible click when the switchover occurs.

The system's default Terminal Equipment Identifier (TEI) will normally allow it to work on Point-to-Point or Point-to-Multipoint lines. However if you intend to connect multiple devices simultaneously to an BRI line, then the TEI should be set to 127. With a TEI of 127, the control unit will ask the exchange to allocate a TEI for operation.

Note:

When connected to some manufactures equipment, which provides an S0 interface (BRI), a defaulted Control Unit will not bring up the ISDN line. Configuring the Control Unit to a TEI of 127 for that line will usually resolve this.

Related Links

Line on page 272
Line | BRI Line on page 282
Line | Channels (BRI) on page 286

Line | BRI Line

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

Field	Description
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Line Number	This parameter is not configurable; it is allocated by the system.
Line Sub Type	Default = ETSI Select to match the particular line type provided by the line provider. IP500 BRI daughter cards can be configured for So (S-Bus) operation for connection to ISDN terminal devices. Note that this requires the addition of terminating resistors at both the system and remote ends, and the use of a suitable cross-over cable. For full details refer to the IP Office Installation manual.
Network Type	Default = Public. This option is available if **Restrict Network Interconnect** (**System | Telephony | Telephony**) is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Telephone Number	Used to remember the external telephone number of this line to assist with loop-back testing. For information only.

Table continues…

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Incoming Group ID</td><td>Default = 0, Range 0 to 99999.

The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.</td></tr>
<tr><td>Outgoing Group ID</td><td>Default = 0, Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID.

For Basic Edition and Standard Edition deployments, the same ID can be used for multiple lines.

In a Server Edition network, the Outgoing Group ID used on a system must also be unique within the network, ie. the same ID cannot be used in the configuration of any lines on another server system in the network.
<table>
<tr><td>Reserved Group ID numbers</td><td>Description</td></tr>
<tr><td>90000 - 99999</td><td>Reserved for system use (not enforced).</td></tr>
<tr><td>99999 and 99998</td><td>In a Server Edition network, reserved for the H.323 lines to the Primary Server and Secondary Server respectively.</td></tr>
<tr><td>999901 to 99930</td><td>In a Server Edition network, reserved for the H.323 lines from the Primary Server to each expansion system in the network.</td></tr>
<tr><td>0</td><td>In a Server Edition network, the ID 0 cannot be used.</td></tr>
<tr><td>98888</td><td>For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.</td></tr>
</table></td></tr>
<tr><td>Prefix</td><td>Default = Blank. The prefix is used in the following ways:

• For incoming calls: The ISDN messaging tags indicates the call type (National, International or Unknown). If the call type is unknown, then the number in the Prefix field is added to the ICLID.

• For outgoing calls: The prefix is not stripped, therefore any prefixes not suitable for external line presentation should be stripped using short codes.</td></tr>
<tr><td>National Prefix</td><td>Default = 0

This indicates the digits to be prefixed to a incoming national call. When a number is presented from ISDN as a "national number" this prefix is added. For example 1923000000 is converted to 01923000000.</td></tr>
<tr><td>International Prefix</td><td>Default = 00

This indicates the digits to be prefixed to an incoming international call. When a number is presented from ISDN as an "international number" this prefix is added. For example 441923000000 is converted to 00441923000000.</td></tr>
</table>

Table continues…

Field	Description
TEI	Default = 0 The Terminal Equipment Identifier. Used to identify each device connected to a particular ISDN line. For Point-to-Point lines this is 0. It can also be 0 on a Point to Multipoint line, however if multiple devices are sharing a Point-to-Multipoint line it should be set to 127 which results in the exchange allocating the TEI's to be used.
Number of Channels	Default = 2. Range = 0 to 2. Defines the number of operational channels that are available on this line.
Outgoing Channels	Default = 2. Range = 0 to 2. This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as Number of Channels field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls.
Voice Channels	Default = 2. Range = 0 to 2. The number of channels available for voice use.
Data Channels	Default = 2. Range = 0 to 2. The number of channels available for data use. If left blank, the value is 0.
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available. • Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source. • In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.
Add 'Not-end-to-end ISDN' Information Element	Default = Never*. Sets whether the optional 'Not end-to-end ISDN' information element should be added to outgoing calls on the line. The options are **Never**, **Always** or **POTS** (only if the call was originated by an analog extension). *The default is **Never** except for the following locales; for Italy the default is **POTS**, for New Zealand the default is **Always**.
Progress Replacement	Default = None.

Table continues…

Field	Description
	Progress messages are defined in the Q.931 ISDN connection control signaling protocol. Generally, If a progress message is sent, the caller does not get connected and so typically does not accrue call costs. Not all ISDN lines support Q.931 Progress messages. Use this setting to configure alternative signaling to the ISDN line for internally generated Progress messages. The options are: • **Alerting**: Map to Q.931 Alerting. The call is not connected. The caller does not hear the message and typically does not accrue call costs. • **Connect**: Map to Q.931 Connect. The caller hears the message and typically will accrue call costs.
Supports Partial Rerouting	Default = Off. Partial rerouting (PR) is an ISDN feature. It is supported on external (non-network and QSIG) ISDN exchange calls. When an external call is transferred to another external number, the transfer is performed by the ISDN exchange and the channels to the system are freed. Use of this service may need to be requested from the line provider and may incur a charge.
Force Number Plan to ISDN	Default = Off. This option is only configurable when **Support Partial Rerouting** is also enabled. When selected, the plan/type parameter for Partial Rerouting is changed from **Unknown/Unknown** to **ISDN/Unknown**.
Send Redirecting Number	Default = Off. This option can be used on ISDN trunks where the redirecting service is supported by the trunk provider. Where supported, on twinned calls the caller ID of the original call is passed through to the twinning destination. This option is only used for twinned calls.
Support Call Tracing	Default = Off. The system supports the triggering of malicious caller ID (MCID) tracing at the ISDN exchange. Use of this feature requires liaison with the ISDN service provider and the appropriate legal authorities to whom the call trace will be passed. The user will also need to be enabled for call tracing and be provider with either a short code or programmable button to activate MCID call trace. Refer to Malicious Call Tracing in the Telephone Features section for full details.
Active CCBS Support	Default = Off. Call completion to a busy subscriber (CCBS). It allows automatic callback to be used on outgoing ISDN calls when the destination is busy. This feature can only be used on point-to-point trunks. Use of this service may need to be requested from the line provider and may incur a charge.
Passive CCBS	Default = Off.
Cost Per Charging Unit	Advice of charge (AOC) information can be display on T3/T3IP phones and output in SMDR. The information is provided in the form of charge units. This setting is used to enter the call cost per charging unit set by the line provider. The values are 1/10,000th of a currency unit. For example if the call cost per unit is £1.07, a value of 10700 should be set on the line. Refer to Advice of Charge.

Table continues…

Field	Description
Send original calling party for forwarded and twinning calls	Default = Off. (Release 9.0.3) Use the original calling party ID when forwarding calls or routing twinned calls. Note that the values on the **System | Twinning** tab override this if set. This setting is mergeable. This setting applies to the following ISDN lines: • PRI24 with subtypes PRI, ETSI and ETSI CHI • PRI30 with subtypes ETSI and ETSI CHI
Originator number for forwarded and twinning calls	Default = blank. (Release 9.0.3) The number used as the calling party ID when forwarding calls or routing twinned calls. This field is grayed out when the **Send original calling party for forwarded and twinning calls** setting is enabled. Note that the values on the **System | Twinning** tab override this, if set. This setting is mergeable. This setting applies to the following ISDN lines: • PRI24 with subtypes PRI, ETSI and ETSI CHI • PRI30 with subtypes ETSI and ETSI CHI

Related Links

BRI Line on page 281

Line | Channels (BRI)

This tab allows settings for individual channels within the trunk to be adjusted. To edit a channel either double-click on it or click the channel and then select **Edit**.

To edit multiple channels at the same time, select the required channels using Ctrl or Shift and then click **Edit**. When editing multiple channels, fields that must be unique such as **Line Appearance ID** are not shown.

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

Field	Description
Line Appearance ID	Default = Auto-assigned. Range = 2 to 9 digits. Used for configuring Line Appearances with button programming. The line appearance ID must be unique and not match any extension number. Line appearance is not supported for trunks set to QSIG operation and is not recommended for trunks be used for DID.

Related Links

BRI Line on page 281

PRI Trunks

PRI trunks are provided by the installation of a PRI trunk card into the control unit. avThe IP500 PRI-U trunk card can be configured (see below) to one of those line types. The cards are also available with either 1 or 2 physical ports. The number of B-channels supported by each physical port depends on the line type of the card.

- **E1**: 30 B-channels and 1 D-channel per port.
- **T1**: 24 B-channels per port.
- **US PRI**: 23 B-channels and 1 D-channel per port.
- **E1-R2**: 30 B-channels and 1 D-channel per port.

For full details of installation refer to the IP Office Installation manual.

IP500 PRI-U Trunk Card Line Type

The IP500 PRI-U card can be configured to support either E1, T1 or E1-R2 PRI line types. To select the line type required, right-click on the line in the group or navigation pane and select **Change Universal PRI Card Line Type**.

The control unit supports 8 B-channels on each IP500 PRI-U card fitted. Additional B-channels up to the full capacity of IP500 PRI-U ports installed require licenses added to the configuration. D-channels are not affected by licensing.

For ETSI and QSIG trunks, license instances are consumed by the number of calls in progress on B-channels.

For T1, E1R2 and ETSI CHI trunks, licenses instances are consumed by the channels set as in service.

Related Links

Line on page 272
E1 Line on page 287
E1 R2 Line on page 295
T1 Line on page 300
T1 PRI Line on page 306

E1 Line

Related Links

PRI Trunks on page 287
Line | E1 PRI Line on page 288
Line | E1 Short Codes on page 293
Line | E1 PRI Channels on page 293

Line | E1 PRI Line

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

Field	Description
Line Number	This parameter is not configurable; it is allocated by the system.
Line Sub Type	Select to match the particular line type provided by the line provider. The options are: • **ETSI** • **ETSI CHI** • **QSIG A** • **QSIG B** **ETSI CHI** is used to send the channel allocation ID (CHI) in the call setup signalling. This is a request to use a particular B-channel rather than use any B-channel allocated by the central office exchange. QSIG trunks trunks are not supported on IP500 V2 systems without IP500 Voice Networking licenses.
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Network Type	Default = Public. This option is available if **Restrict Network Interconnect** (**System | Telephony | Telephony**) is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Telephone Number	Used to remember the external telephone number of this line to assist with loop-back testing. For information only.
Channel Allocation	Default = 30|1. For lines set to **ETSI CHI**, this option allows the system to select the default order in which channels should be used for outgoing calls. Typically this is set as the opposite of the default order in which the central office exchange uses channels for incoming calls. For lines set to the **Line Sub Type** of **ETSI CHI**, the **Incoming Group ID** is set as part of the individual channel settings.

Table continues…

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Incoming Group ID</td><td>Default = 0, Range 0 to 99999.

The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.</td></tr>
<tr><td>Outgoing Group ID</td><td>Default = 0, Range 0 to 99999.

Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID.

For Basic Edition and Standard Edition deployments, the same ID can be used for multiple lines.

In a Server Edition network, the Outgoing Group ID used on a system must also be unique within the network, ie.

the same ID cannot be used in the configuration of any lines on another server system in the network.
<table>
<tr><th>Reserved Group ID numbers</th><th>Description</th></tr>
<tr><td>90000 - 99999</td><td>Reserved for system use (not enforced).</td></tr>
<tr><td>99999 and 99998</td><td>In a Server Edition network, reserved for the H.323 lines to the Primary Server and Secondary Server respectively.</td></tr>
<tr><td>999901 to 99930</td><td>In a Server Edition network, reserved for the H.323 lines from the Primary Server to each expansion system in the network.</td></tr>
<tr><td>0</td><td>In a Server Edition network, the ID 0 cannot be used.</td></tr>
<tr><td>98888</td><td>For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.</td></tr>
</table></td></tr>
<tr><td>Prefix</td><td>Default = Blank.

The prefix is used in the following ways:

• For incoming calls The ISDN messaging tags indicates the call type (National, International or Unknown). If the call type is unknown, then the number in the Prefix field is added to the ICLID.

• For outgoing calls The prefix is not stripped, therefore any prefixes not suitable for external line presentation should be stripped using short codes.</td></tr>
<tr><td>National Prefix</td><td>Default = 0

This indicates the digits to be prefixed to a incoming national call. When a number is presented from ISDN as a "national number" this prefix is added. For example 1923000000 is converted to 01923000000.</td></tr>
<tr><td>International Prefix</td><td>Default = 00</td></tr>
</table>

Table continues…

Field	Description
	This indicates the digits to be prefixed to an incoming international call. When a number is presented from ISDN as an "international number" this prefix is added. For example 441923000000 is converted to 00441923000000.
TEI	Default = 0 The Terminal Equipment Identifier. Used to identify each Control Unit connected to a particular ISDN line. For Point to Point lines this is typically (always) 0. It can also be 0 on a Point to Multi-Point line, however if multiple devices are sharing a Point to Multi-Point line it should be set to 127 which results in the exchange deciding on the TEI's to be used.
Number of Channels	Defines the number of operational channels that are available on this line. Up to 30 for E1 PRI, 23 for T1 PRI.
Outgoing Channels	This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as **Number of Channels** field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls. Only available when the **Line Sub Type** is set to **ETSI**.
Voice Channels	The number of channels available for voice use. Only available when the **Line Sub Type** is set to **ETSI**.
Data Channels	The number of channels available for data use. Only available when the **Line Sub Type** is set to **ETSI**.
CRC Checking	Default = On Switches CRC on or off.
Line Signalling	Default = CPE This option is not used for lines where the **Line SubType** is set to **QSIG**. Select either **CPE** (customer premises equipment) or **CO** (central office). The **CO** feature is intended to be used primarily as a testing aid. It allows PRI lines to be tested in a back-to-back configuration, using crossover cables. The CO feature operates on this line type by modifying the way in which incoming calls are disconnected for system configuration in Brazil and Argentina. In these locales, the CO setting uses Forced-Release instead of Clear-Back to disconnect incoming calls. The Brazilian Double-Seizure mechanism, used to police Collect calls, is also disabled in CO mode.
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available. • Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source.

Table continues…

Field	Description
	• In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.
Add 'Not-end-to-end ISDN' Information Element	Default = Never Sets whether the optional 'Not end-to-end ISDN' information element should be added to outgoing calls on the line. The options are: • **Never** • **Always** • **POTS**(only if the call was originated by an analog extension). The default is **Never** except for the following locales; for Italy the default is **POTS**, for New Zealand the default is **Always**.
Progress Replacement	Default = None. Progress messages are defined in the Q.931 ISDN connection control signaling protocol. Generally, If a progress message is sent, the caller does not get connected and so typically does not accrue call costs. Not all ISDN lines support Q.931 Progress messages. Use this setting to configure alternative signaling to the ISDN line for internally generated Progress messages. The options are: • **Alerting**: Map to Q.931 Alerting. The call is not connected. The caller does not hear the message and typically does not accrue call costs. • **Connect**: Map to Q.931 Connect. The caller hears the message and typically will accrue call costs.
Supports Partial Rerouting	Default = Off. Partial rerouting (PR) is an ISDN feature. It is supported on external (non-network and QSIG) ISDN exchange calls. When an external call is transferred to another external number, the transfer is performed by the ISDN exchange and the channels to the system are freed. Use of this service may need to be requested from the line provider and may incur a charge.
Force Number Plan to ISDN	Default = Off. This option is only configurable when **Support Partial Rerouting** is also enabled. When selected, the plan/type parameter for Partial Rerouting is changed from **Unknown/Unknown** to **ISDN/Unknown**.
Send Redirecting Number	Default = Off. This option can be used on ISDN trunks where the redirecting service is supported by the trunk provider. Where supported, on twinned calls the caller ID of the original call is passed through to the twinning destination. This option is only used for twinned calls.
Support Call Tracing	Default = Off.

Table continues…

Field	Description
	The system supports the triggering of malicious caller ID (MCID) tracing at the ISDN exchange. Use of this feature requires liaison with the ISDN service provider and the appropriate legal authorities to whom the call trace will be passed. The user will also need to be enabled for call tracing and be provider with either a short code or programmable button to activate MCID call trace. Refer to Malicious Call Tracing in the Telephone Features section for full details.
Active CCBS Support	Default = Off. Call completion to a busy subscriber (CCBS). It allows automatic callback to be used on outgoing ISDN calls when the destination is busy. This feature can only be used on point-to-point trunks. Use of this service may need to be requested from the line provider and may incur a charge.
Passive CCBS	Default = Off.
Cost Per Charging Unit	Advice of charge (AOC) information can be display on T3/T3IP phones and output in SMDR. The information is provided in the form of charge units. This setting is used to enter the call cost per charging unit set by the line provider. The values are 1/10,000th of a currency unit. For example if the call cost per unit is £1.07, a value of 10700 should be set on the line. Refer to Advice of Charge.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.
Send original calling party for forwarded and twinning calls	Default = Off. (Release 9.0.3) Use the original calling party ID when forwarding calls or routing twinned calls. Note that the values on the **System | Twinning** tab override this if set. This setting is mergeable. This setting applies to the following ISDN lines: • PRI24 with subtypes PRI, ETSI and ETSI CHI • PRI30 with subtypes ETSI and ETSI CHI
Originator number for forwarded and twinning calls	Default = blank. (Release 9.0.3) The number used as the calling party ID when forwarding calls or routing twinned calls. This field is grayed out when the **Send original calling party for forwarded and twinning calls** setting is enabled. Note that the values on the **System | Twinning** tab override this, if set. This setting is mergeable. This setting applies to the following ISDN lines: • PRI24 with subtypes PRI, ETSI and ETSI CHI • PRI30 with subtypes ETSI and ETSI CHI

The following fields are shown for a US T1 trunk card set to ETSI or QSIG operation. These cards have the same settings E1 PRI trunk cards set to ETSI or QSIG but only support 23 channels.

Field	Description
CSU Operation	Check this field to enable the T1 line to respond to loop-back requests from the line.

Table continues…

Field	Description
Haul Length	Default = 0-115 feet Sets the line length to a specific distance.
Channel Unit	Default = Foreign Exchange This field should be set to match the channel signaling equipment provided by the Central Office. The options are Foreign Exchange, Special Access or Normal.

Related Links

E1 Line on page 287

Line | E1 Short Codes

For some types of line, Line short codes can be applied to any digits received with incoming calls.

The line Short Code tab is shown for the following trunk types which are treated as internal or private trunks: **QSIG** (T1, E1, H.323), **BRI S0**, **H.323**, **SCN**, **IP Office**. Incoming calls on those types of trunk are not routed using **Incoming Call Route** settings. Instead the digits received with incoming calls are checked for a match as follows:

Extension number (including remote numbers in a multi-site network).

- Line short codes (excluding ? short code).
- System short codes (excluding ? short code).
- Line ? short code.
- System ? short code.

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

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

Related Links

E1 Line on page 287

Line | E1 PRI Channels

This tab allows settings for individual channels within the trunk to be adjusted. To edit a channel either double-click on it or click the channel and then select **Edit**.

To edit multiple channels at the same time, select the required channels using Ctrl or Shift and then click **Edit**. When editing multiple channels, fields that must be unique such as **Line Appearance ID** are not shown.

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

Field	Description
Line Appearance ID	Default = Auto-assigned. Range = 2 to 9 digits. Used for configuring Line Appearances with button programming. The line appearance ID must be unique and not match any extension number. Line

Field	Description
	appearance is not supported for trunks set to QSIG operation and is not recommended for trunks be used for DID. If the trunk **Line Sub Type** is set to **ETSI CHI**, outgoing line appearance calls must use the corresponding channel.

The following additional fields are shown for lines where the **Line Sub Type** is set to **ETSI CHI**.

Field	Description	
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.	
Outgoing Group ID	Default = 0, Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID. For Basic Edition and Standard Edition deployments, the same ID can be used for multiple lines. In a Server Edition network, the **Outgoing Group ID** used on a system must also be unique within the network, ie. the same ID cannot be used in the configuration of any lines on another server system in the network.	
	Reserved Group ID numbers	Description
	90000 - 99999	Reserved for system use (not enforced).
	99999 and 99998	In a Server Edition network, reserved for the H.323 lines to the Primary Server and Secondary Server respectively.
	999901 to 99930	In a Server Edition network, reserved for the H.323 lines from the Primary Server to each expansion system in the network.
	0	In a Server Edition network, the ID 0 cannot be used.
	98888	For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.
Direction	Default = Bothways The direction of calls on the channel. The options are: • **Incoming** • **Outgoing** • **Bothways**	
Bearer	Default = Any	

Table continues…

Field	Description
	The type of traffic carried by the channel. The options are: • **Voice** • **Data** • **Any**
Admin	Default = Out of Service. This field can be used to indicate whether the channel is in use or not. On trunks where only a limited number of channels have been requested from the trunk provider (known as sub-equipped trunks), those channels not provided should be set as **Out of Service**. For channels that are available but are temporarily not being used select **Maintenance**.
Tx Gain	Default = 0dB. Range = -10dBb to +5dB. The transmit gain in dB.
Rx Gain	Default = 0dB. Range = -10dBb to +5dB. The receive gain in dB.

Related Links

E1 Line on page 287

E1 R2 Line

Related Links

PRI Trunks on page 287
Line | E1-R2 Options on page 295
Line | E1-R2 Channels on page 297
Line | E1 R2 MFC Group on page 298
Line | E1-R2 Advanced on page 299

Line | E1-R2 Options

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

Field	Description
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Network Type	Default = Public. This option is available if **Restrict Network Interconnect** (**System | Telephony | Telephony**) is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a

Table continues…

Field	Description
	Private trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Line Number	Allocated by the system.
Line SubType	Default = E1-R2 The options are: • **E1-R2** • **ETSI** • **QSIGA** • **QSIGB** QSIG trunks trunks are not supported on IP500 V2 systems without IP500 Voice Networking licenses.
Channel Allocation	Default = 30 | 1 The order, **30 | 1** or **1 | 30**, in which channels are used.
Country (Locale)	Default = Mexico. Select the locale that matches the area of usage. Note that changing the locale will return the MFC Group settings to the defaults for the selected locale. Currently supported locales are: • **Argentina** • **Brazil** • **China** • **India** • **Korea** • **Mexico** • **None**
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected. The table at the base of the form displays the settings for the individual channels provided by the line. For details of the channel settings see the E1-R2 Channel form. To edit a channel, either double-click on it or right-click and select **Edit**. This will display the Edit Channel dialog box. To edit multiple channels at the same time select the channels whilst pressing the Shift or Ctrl key. Then right-click and select **Edit**.

Related Links

E1 R2 Line on page 295

Line | E1-R2 Channels

This tab allows settings for individual channels within the trunk to be adjusted. To edit a channel, select the required channel or channels and click **Edit**.

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

The channel settings are split into two sub-tabs, **E1R2 Edit Channel** and **Timers**.

The **Timers** tab displays the various timers provided for E1-R2 channels. These should only be adjusted when required to match the line provider's settings.

Field	Descriptions	
Channel	The channel or channels being edited.	
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.	
Outgoing Group ID	Default = 0, Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID. For Basic Edition and Standard Edition deployments, the same ID can be used for multiple lines. In a Server Edition network, the **Outgoing Group ID** used on a system must also be unique within the network, ie. the same ID cannot be used in the configuration of any lines on another server system in the network.	
	Reserved Group ID numbers	Description
	90000 - 99999	Reserved for system use (not enforced).
	99999 and 99998	In a Server Edition network, reserved for the H.323 lines to the Primary Server and Secondary Server respectively.
	999901 to 99930	In a Server Edition network, reserved for the H.323 lines from the Primary Server to each expansion system in the network.
	0	In a Server Edition network, the ID 0 cannot be used.
	98888	For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.
Direction	Default = Both Directions The direction of calls on the channel. The options are: • **Incoming** • **Outgoing** • **Both Directions**	

Table continues…

Field	Descriptions
Bearer	Default = Any The type of traffic carried by the channel. The options are: • **Voice** • **Data** • **Any**
Line Signaling Type	Default = R2 Loop Start The signaling type used by the channel. Current supported options are: • **R2 Loop Start** • **R2 DID** • **R2 DOD** • **R2 DIOD** • **Tie Immediate Start** • **Tie Wink Start** • **Tie Delay Dial** • **Tie Automatic** • **WAN Service** • **Out of Service**
Dial Type	Default = MFC Dialing The type of dialing supported by the channel. The options are:, or . • **MFC Dialing** • **Pulse Dialing** • **DTMF Dialing**

Related Links

E1 R2 Line on page 295

Line | E1 R2 MFC Group

These tabs show the parameter assigned to each signal in an MFC group. The defaults are set according to the Country (Locale) on the Line tab. All the values can be returned to default by the **Default All** button on the **Advanced** tab.

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

To change a setting either double-click on it or right-click and select **Edit**.

Related Links

E1 R2 Line on page 295

Line | E1-R2 Advanced

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

Field	Description
Zero Suppression	Default = HDB3 Selects the method of zero suppression used (HDB3 or AMI).
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available. • Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source. • In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available. • Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source. • In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.
Pulse Metering Bit	Default = A Bit Sets which bit should be used to indicate the pulse metering signal. The options are: • **A Bit** • **B Bit** • **C Bit**
Line Signaling	Default = CPE

Table continues…

Field	Description
	The options are: • **CPE** • **CO** • **CO** The feature is intended to be used primarily as a testing aid. It allows T1 and E1 lines to be tested in a back-to-back configuration, using crossover (QSIG) cables. The CO feature operates by modifying the way in which incoming calls are disconnected for system configuration in Brazil and Argentina. In these locales, the CO setting uses Forced-Release instead of Clear-Back to disconnect incoming calls. The Brazilian Double-Seizure mechanism used to police Collect calls, is also disabled in CO mode.
Incoming Routing Digits	Default = 4 Sets the number of incoming digits used for incoming call routing.
CRC Checking	Default = On Switches CRC on or off.
Default All Group Settings	Default the MFC Group tab settings.
Line Signaling Timers	To edit one of these timers, either double-click on the timer or right-click on a timer and select the action required.

Related Links

E1 R2 Line on page 295

T1 Line

Related Links

PRI Trunks on page 287
Line | US T1 Line on page 300
Line | T1 Channels on page 303

Line | US T1 Line

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

Field	Description
Line Number	Allocated by the system.
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.

Table continues…

Field	Description
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Network Type	Default = Public. This option is available if **Restrict Network Interconnect** (**System | Telephony | Telephony**) is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Line Sub Type	Default = T1 Set to T1 for a T1 line.
Channel Allocation	Default = 24 | 1 The order, 24 to 1 or 1 to 24, in which channels are used.
Prefix	Default = Blank Enter the number to prefix to all incoming numbers for callback. This is useful if all users must dial a prefix to access an outside line. The prefix is automatically placed in front of all incoming numbers so that users can dial the number back.
Framing	Default = ESF Selects the type of signal framing used. The options are: • **ESF** • **D4**
Zero Suppression	Default = B8ZS Selects the method of zero suppression used. The options are: • **B8ZS** • **AMI ZCS**
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available.

Table continues…

Field	Description
	• Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source. • In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.
Haul Length	Default = 0-115 feet. Sets the line length to a specific distance.
Channel Unit	Default = Foreign Exchange This field should be set to match the channel signaling equipment provided by the Central Office. The options are: • **Foreign Exchange** • **Special Access** • **Normal**
CRC Checking	Default = On Turns CRC on or off.
Line Signaling	Default = CPE This field affects T1 channels set to Loop-Start or Ground-Start. The field can be set to either CPE (Customer Premises Equipment) or CO (Central Office). This field should normally be left at its default of CPE. The setting CO is normally only used in lab back-to-back testing.
Incoming Routing Digits	Default=0 (present call immediately) Sets the number of routing digits expected on incoming calls. This allows the line to present the call to the system once the expected digits have been received rather than waiting for the digits timeout to expire. This field only affects T1 line channels set to E&M Tie, E&M DID, E&M Switched 56K and Direct Inward Dial.
CSU Operation	Enable this field to enable the T1 line to respond to loop-back requests from the line.
Enhanced Called Party Number	Default = Off This option is not supported for systems set to the United States locale. Normally the dialed number length is limited to 15 digits. Selecting this option increases the allowed dialed number length to 30 digits.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.

Related Links

T1 Line on page 300

Line | T1 Channels

The settings for each channel can be edited. Users have the option of editing individual channels by double-clicking on the channel or selecting and editing multiple channels at the same time. Note that the Line Appearance ID cannot be updated when editing multiple channels.

When editing a channel or channels, the settings available are displayed on two sub-tabs; T1 Edit Channel and Timers.

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

T1 Edit Channel Settings

Field	Description	
Channel	Allocated by the system.	
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.	
Outgoing Group ID	Default = 0, Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID. For Basic Edition and Standard Edition deployments, the same ID can be used for multiple lines. In a Server Edition network, the **Outgoing Group ID** used on a system must also be unique within the network, ie. the same ID cannot be used in the configuration of any lines on another server system in the network.	
	Reserved Group ID numbers	Description
	90000 - 99999	Reserved for system use (not enforced).
	99999 and 99998	In a Server Edition network, reserved for the H.323 lines to the Primary Server and Secondary Server respectively.
	999901 to 99930	In a Server Edition network, reserved for the H.323 lines from the Primary Server to each expansion system in the network.
	0	In a Server Edition network, the ID 0 cannot be used.
	98888	For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.
Line Appearance ID	Default = Auto-assigned. Range = 2 to 9 digits. Used for configuring Line Appearances with button programming. The line appearance ID must be unique and not match any extension number. Line appearance is not	

Table continues…

Field	Description
	supported for trunks set to QSIG operation and is not recommended for trunks be used for DID.
Direction	Default = Bothway The direction of calls on the channel. The options are: • **Incoming** • **Outgoing** • **Bothway**
Bearer	Default = Any The type of traffic carried by the channel. The options are: • **Voice** • **Data** • **Any**
Type	Default = Out of Service The T1 emulates the following connections: • **Ground-Start** • **Loop-Start** • **E&M - TIE** • **E&M - DID** • **E&M Switched 56K** • **Direct Inward Dial** • **Clear Channel 64K** • **Out of Service** Trunks set to **E&M - DID** will only accept incoming calls. If **E&M - TIE** is selected and the **Outgoing Trunk Type** is set to **Automatic**, no secondary dial tone is provided for outgoing calls on this line/trunk.
Dial Type	Default = DTMF Dial Select the dialing method required. The options are: • **DTMF Dial** • **Pulse Dial**
Incoming Trunk Type	Default = Wink-Start Used for E&M types only. The handshake method for incoming calls. The options are: • **Automatic** • **Immediate** • **Delay Dial**

Table continues…

Field	Description
	• **Wink-Start**
Outgoing Trunk Type	Default = Wink-Start Used for E&M types only. The handshake method for outgoing calls. The options are: • **Automatic** • **Immediate** • **Delay Dial** • **Wink-Start** If the line Type is set to **E&M-TIE** and the **Outgoing Trunk Type** is set to **Automatic**, no secondary dial tone is provided for outgoing calls on this line/trunk.
Tx Gain	Default = 0dB. The transmit gain in dB.
Rx Gain	Default = 0dB. The receive gain in dB.

Timer Settings

This sub-tab allows various timers relating to operation of an individual channel to be adjusted. These should only be adjusted to match the requirements of the line provider. The following is a list of the default values. To reset a value, click on the current value and then right click and select from the default, minimize and maximize options displayed.

Incoming Automatic Delay: 410.

Incoming Wink Delay: 100.

Wink Signal: 200.

Incoming Dial Guard: 50.

First Incoming Digit: 15000.

Incoming Inter Digit: 5000.

Maximum Inter Digit: 300.

Flash Hook Detect: 240.

Incoming Disconnect: 300.

Incoming Disconnect Guard: 800.

Disconnected Signal Error: 240000.

Outgoing Disconnect: 300.

Outgoing Disconnect Guard: 800.

Ring Verify Duration: 220.

Ring Abandon: 6300.

Ping Verify: 600.

Silent Interval: 1100.

Outgoing Seizure: 10.

Wink Start: 5000.

Wink Validated: 80.

Wink End: 350.

Delay End: 5000.

Outgoing Dial Guard: 590.

Outgoing IMM Dial Guard: 1500.

Outgoing Pulse Dial Break: 60.

Outgoing Pulse Dial Make: 40.

Outgoing Pulse Dial Inter Digit: 720.

Outgoing Pulse Dial Pause: 1500.

Flash Hook Generation: 500.

Outgoing End of Dial: 1000.

Answer Supervision: 300.

Incoming Confirm: 20.

Long Ring Time: 1100.

Related Links

T1 Line on page 300

T1 PRI Line

Related Links

PRI Trunks on page 287
Line | Line (T1 ISDN) on page 306
Channels (T1 ISDN) on page 309
Line | TNS (T1 ISDN) on page 311
Line | Special (T1 ISDN) on page 311
Line | Call By Call (US PRI) on page 312

Line | Line (T1 ISDN)

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

Variable	Description
Line Number	Allocated by the system.
Card/Module	Indicates the card slot or expansion module being used for the trunk device providing the line. For IP500 V2 control units: 1 to 4 match the slots on the front of the control unit from left to right. Expansion modules are numbered from 5 upwards, for example trunks on the module in Expansion Port 1 are shown as 5.
Port	Indicates the port on the Card/Module above to which the configuration settings relate.
Network Type	Default = Public. This option is available if **Restrict Network Interconnect** (**System | Telephony | Telephony**) is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Line Sub Type	: Default = PRI Set to **PRI**. If set to T1 see Line Form (T1). If set to **ETSI**, **ETSI CHI**, **QSIG A** or **QSIG B** see Line (E1). QSIG trunks trunks are not supported on IP500 V2 systems without IP500 Voice Networking licenses.
Channel Allocation	Default = 23 | 1 The order, 23 to 1 or 1 to 23, in which channels are used.

Table continues…

Variable	Description
Switch Type	Default = NI2 The options are • **4ESS** • **5ESS** • **DMS100** • **NI2**
Provider	Default = Local Telco Select the PSTN service provider (**AT&T**, **Sprint**, **WorldCom** or **Local Telco**).
Prefix	Default = Blank Enter the number to prefix to all incoming numbers for callback. This is useful if all users must dial a prefix to access an outside line. The prefix is automatically placed in front of all incoming numbers so that users can dial the number back.
Add 'Not-end-to-end ISDN' Information Element	Default = Never*. Sets whether the optional 'Not end-to-end ISDN' information element should be added to outgoing calls on the line. The options are • **Never** • **Always** • **POTS** (only if the call was originated by an analog extension) *The default is **Never** except for the following locales; for Italy the default is **POTS**, for New Zealand the default is **Always**.
Progress Replacement	Default = None. Progress messages are defined in the Q.931 ISDN connection control signaling protocol. Generally, If a progress message is sent, the caller does not get connected and so typically does not accrue call costs. Not all ISDN lines support Q.931 Progress messages. Use this setting to configure alternative signaling to the ISDN line for internally generated Progress messages. The options are: • **Alerting**: Map to Q.931 Alerting. The call is not connected. The caller does not hear the message and typically does not accrue call costs. • **Connect**: Map to Q.931 Connect. The caller hears the message and typically will accrue call costs.
Send Redirecting Number	Default = Off. This option can be used on ISDN trunks where the redirecting service is supported by the trunk provider. Where supported, on twinned calls the caller ID of the original call is passed through to the twinning destination. This option is only used for twinned calls.

Table continues…

Variable	Description
Send Names	This option is available when the **Switch Type** above is set to **DMS100**. If set, names are sent in the display field. The **Z** shortcode character can be used to specify the name to be used.
Names Length	Set the allowable length for names, up to 15 characters, when **Send Names** is set above.
Test Number	Used to remember the external telephone number of this line to assist with loop-back testing. For information only.
Framing	Default = ESF Selects the type of signal framing used (ESF or D4).
Zero Suppression	Default = B8ZS Selects the method of zero suppression used (B8ZS or AMI ZCS).
Clock Quality	Default = Network Refer to the IP Office Installation Manual for full details. This option sets whether the system should try to take its clock source for call synchronization and signalling from this line. Preference should always be given to using the clock source from a central office exchange if available by setting at least one exchange line to **Network**. • If multiple lines are set as **Network**, the order in which those lines are used is described in the IP Office Installation Manual. If additional lines are available, **Fallback** can be used to specify a clock source to use should the **Network** source not be available. • Lines from which the clock source should not be taken should be set as **Unsuitable**. • If no clock source is available, the system uses its own internal 8KHz clock source. • In scenarios where several systems are network via digital trunk lines, care must be taken to ensure that all the systems use the same clock source. The current source being used by a system is reported within the System Status Application.
CSU Operation	Tick this field to enable the T1 line to respond to loop-back requests from the line.
Haul Length	Default = 0-115 feet Sets the line length to a specific distance.
Channel Unit	Default = Foreign Exchange This field should be set to match the channel signaling equipment provided by the Central Office. The options are • **Foreign Exchange** • **Special Access** • **Normal**

Table continues…

Variable	Description
CRC Checking	Default = On Turns CRC on or off.
Line Signaling	The field can be set to either **CPE** (Customer Premises Equipment) or **CO** (Central Office). This field should normally be left at its default of **CPE**. The setting **CO** is normally only used in lab back-to-back testing.
Incoming Routing Digits	Default=0 (present call immediately) Sets the number of routing digits expected on incoming calls. This allows the line to present the call to the system once the expected digits have been received rather than waiting for the digits timeout to expire. This field only affects T1 line channels set to **E&M Tie**, **E&M DID**, **E&M Switched 56K** and **Direct Inward Dial**.
Admin	Default = In Service. This field allows a trunk to be taken out of service if required for maintenance or if the trunk is not connected.

Related Links

T1 PRI Line on page 306

Channels (T1 ISDN)

This tab allows settings for individual channels within the trunk to be adjusted. This tab is not available for trunks sets to ETSI or QSIG mode.

Usability

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

Configuration Settings

Channel Allocated by the system.

Incoming Group ID: Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.

Outgoing Group ID: Default = 0, Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID.

For Basic Edition and Standard Edition deployments, the same ID can be used for multiple lines.

In a Server Edition network, the **Outgoing Group ID** used on a system must also be unique within the network, ie. the same ID cannot be used in the configuration of any lines on another server system in the network.

Reserved Group ID numbers	Description
90000 - 99999	Reserved for system use (not enforced).

Table continues…

99999 and 99998	In a Server Edition network, reserved for the H.323 lines to the Primary Server and Secondary Server respectively.
999901 to 99930	In a Server Edition network, reserved for the H.323 lines from the Primary Server to each expansion system in the network.
0	In a Server Edition network, the ID 0 cannot be used.
98888	For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.

Line Appearance ID: Default = Auto-assigned. Range = 2 to 9 digits. Used for configuring Line Appearances with button programming. The line appearance ID must be unique and not match any extension number.

Direction: Default = Both Directions The direction of calls on the channel (**Incoming**, **Outgoing** or **Both Directions**).

Bearer: Default = Any The type of traffic carried by the channel (**Voice**, **Data** or **Any**).

Service: Default = None. If the line provider is set to AT&T, select the type of service provided by the channel. The options are:

Call by Call

SDN (inc GSDN)

MegaCom 800

MegaCom

Wats

Accunet

ILDS

I800

ETN

Private Line

AT&T Multiquest

For other providers, the service options are **None** or **No Service**.

Admin: Default = Out of Service Used to indicate the channel status (**In Service**, **Out of Service** or **Maintenance**).

Tx Gain: Default = 0dB The transmit gain in dB.

Rx Gain: Default = 0dB The receive gain in dB.

Related Links

T1 PRI Line on page 306

Line | TNS (T1 ISDN)

This tab is shown when the line Provider is set to AT&T. It allows the entry of the Network Selection settings. These are prefixes for alternative long distance carriers. When a number dialed matches an entry in the table, that pattern is stripped from the number before being sent out. This table is used to set field in the TNS (Transit Network Selection) information element for 4ESS and 5ESS exchanges. It is also used to set fields in the NSF information element.

Usability

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

Configuration Settings

TNS Code: The pattern for the alternate long distance carrier. For example: The pattern 10XXX is added to this tab. If 10288 is dialed, 10 is removed and 288 is placed in the TNS and NSF information.

Related Links

T1 PRI Line on page 306

Line | Special (T1 ISDN)

This tab is shown when the line Provider is set to AT&T. This table is used to set additional fields in the NSF information element after initial number parsing by the TNS tab. These are used to indicate the services required by the call. If the channel is set to Call by Call, then further parsing is done using the records in the Call by Call tab.

Usability

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

Configuration Settings

Short code: The number which results from the application of the rules specified in the User or System Short code tables and the Network Selection table and the Call-by-call table to the number dialed by the user.

Number: The number to be dialed to line.

Special: Default = No Operator (**No Operator**, **Local Operator** or **Presubscribed Operator**).

Plan: Default = National (**National** or **International**).

Typical values are:

Short Code	Number	Service
011N	N	No Operator, International
010N	N	Local Operator, International
01N	N	Local Operator, National
00N	N	Presubscribed Operator, National
0N	N	Presubscribed Operator, National
1N	1N	No operator, National

Related Links

T1 PRI Line on page 306

Line | Call By Call (US PRI)

This tab is shown when the line Provider is set to AT&T. Settings in this tab are only used when calls are routed via a channel which has its **Service** set to **Call by Call**.

It allows short codes to be created to route calls to a different services according to the number dialed. Call By Call reduces the costs and maximizes the use of facilities. Call By Call chooses the optimal service for a particular call by including the Bearer capability in the routing decision. This is particularly useful when there are limited resources.

Usability

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

Configuration Settings

Short Code: The number which results from the application of the rules specified in the User or System Short code tables and the Network Selection table to the number dialed by the user.

Number: The number to be dialed to line.

Bearer: Default = Any The type of channel required for the call (Voice, Data or Any).

Service: Default = AT&T The service required by the call. The options are:

Call by Call

SDN (inc GSDN)

MegaCom 800

MegaCom

Wats

Accunet

ILDS

I800

ETN

Private Line

AT&T Multiquest

Related Links

T1 PRI Line on page 306

S0 Line

These settings are used for S0 ports provided by an S08 expansion module connected a control unit. For full details of installation refer to the IP Office Installation manual.

Though displayed as lines, these BRI ports are used for connection of ISDN2 devices such as video conferencing units or ISDN PC cards.

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.

Related Links

Line on page 272
Line | S0 Line on page 313
Line | S0 Short Codes on page 315
Line | S0 Channels on page 315

Line | S0 Line

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

Field	Description
Line Number	This parameter is not configurable. It is allocated by the system.
Telephone Number	Used to remember the telephone number of this line. For information only.
Prefix	Default = Blank. The prefix is used in the following ways: • **For incoming calls** The ISDN messaging tags indicates the call type (National, International or Unknown). If the call type is unknown, then the number in the Prefix field is added to the ICLID. • **For outgoing calls** The prefix is not stripped, therefore any prefixes not suitable for external line presentation should be stripped using short codes.
National Prefix	Default = 0 This indicates the digits to be prefixed to a incoming national call. When a number is presented from ISDN as a "national number" this prefix is added. For example 1923000000 is converted to 01923000000.
International Prefix	Default = 00 This indicates the digits to be prefixed to an incoming international call. When a number is presented from ISDN as an "international number" this prefix is added. For example 441923000000 is converted to 00441923000000.
Incoming Group ID	Default = 0, Range 0 to 99999. The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming

Table continues…

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>call route is then used to route incoming calls. The same ID can be used for multiple lines.</td></tr>
<tr><td>Outgoing Group ID</td><td>Default = 0, Range 0 to 99999.

Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID.

For Basic Edition and Standard Edition deployments, the same ID can be used for multiple lines.

In a Server Edition network, the Outgoing Group ID used on a system must also be unique within the network, ie. the same ID cannot be used in the configuration of any lines on another server system in the network.
<table>
<tr><td>Reserved Group ID numbers</td><td>Description</td></tr>
<tr><td>90000 - 99999</td><td>Reserved for system use (not enforced).</td></tr>
<tr><td>99999 and 99998</td><td>In a Server Edition network, reserved for the H.323 lines to the Primary Server and Secondary Server respectively.</td></tr>
<tr><td>999901 to 99930</td><td>In a Server Edition network, reserved for the H.323 lines from the Primary Server to each expansion system in the network.</td></tr>
<tr><td>0</td><td>In a Server Edition network, the ID 0 cannot be used.</td></tr>
<tr><td>98888</td><td>For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.</td></tr>
</table></td></tr>
<tr><td>TEI</td><td>Default = 0

Not used. The Control Unit will ignore any entry.</td></tr>
<tr><td>Number of Channels</td><td>Default = 2

Defines the number of operational channels that are available on this line. 2 for BRI and up to 30 for PRI - depending upon the number of channels subscribed.</td></tr>
<tr><td>Outgoing Channels</td><td>Default = 2

This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as Number of Channels field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls.</td></tr>
<tr><td>Voice Channels</td><td>Default = 2

The number of channels available for voice use.</td></tr>
<tr><td>Data Channels</td><td>Default = 2</td></tr>
</table>

Table continues…

Field	Description
	The number of channels available for data use. If left blank the value is 0.

Related Links

S0 Line on page 312

Line | S0 Short Codes

For some types of line, Line short codes can be applied to any digits received with incoming calls.

The line Short Code tab is shown for the following trunk types which are treated as internal or private trunks: **QSIG** (T1, E1, H.323), **BRI S0**, **H.323**, **SCN**, **IP Office**. Incoming calls on those types of trunk are not routed using **Incoming Call Route** settings. Instead the digits received with incoming calls are checked for a match as follows:

Extension number (including remote numbers in a multi-site network).

- Line short codes (excluding ? short code).
- System short codes (excluding ? short code).
- Line ? short code.
- System ? short code.

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

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

Related Links

S0 Line on page 312

Line | S0 Channels

For S0 channels this form is not used.

Related Links

S0 Line on page 312

H.323 Line

These lines are added manually. They allow voice calls to be routed over data links within the system. They are therefore dependent on the IP data routing between the system and the destination having being configured and tested.

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

Network Assessments

Not all data connections are suitable for voice traffic. A network assessment is required for internal network connections. For external network connections a service level agreement is required from the service provider. Avaya cannot control or be held accountable for the suitability of a data connection for carrying voice traffic.

QSIG trunks trunks are not supported on IP500 V2 systems without IP500 Voice Networking licenses.

Related Links

Line on page 272
Line | H.323 VoIP Line on page 316
Line | H.323 Short Codes on page 318
Line | H.323 VoIP Settings on page 318

Line | H.323 VoIP Line

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

Field	Description
Line Number	Range = 1 to 349. Enter the line number that you wish. Note that this must be unique.
Telephone Number	Used to remember the telephone number of this line. For information only.
Network Type	Default = Public. This option is available if **Restrict Network Interconnect** (**System | Telephony | Telephony**) is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Prefix	Default = Blank. The prefix is used in the following ways: • **For incoming calls** The ISDN messaging tags indicates the call type (National, International or Unknown). If the call type is unknown, then the number in the Prefix field is added to the ICLID. • **For outgoing calls** The prefix is not stripped, therefore any prefixes not suitable for external line presentation should be stripped using short codes.
National Prefix	Default = 0 This indicates the digits to be prefixed to a incoming national call. When a number is presented from ISDN as a "national number" this prefix is added. For example 1923000000 is converted to 01923000000.

Table continues…

Field	Description
International Prefix	Default = 00 This indicates the digits to be prefixed to an incoming international call. When a number is presented from ISDN as an "international number" this prefix is added. For example 441923000000 is converted to 00441923000000.
Location	Default = Cloud. Specify a location to associate the extension with a physical location. Associating an extension with a location: • Allows emergency services to identify the source of an emergency call. • Allows you to configure call access control settings for the location. The drop down list contains all locations that have been defined in the **Location** form.
Description	Default = Blank. Maximum 31 characters. Use this field to enter a description of this configuration.
Outgoing Group ID	Default = 0. Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID. The same ID can be used for multiple lines. In a Server Edition network, the **Outgoing Group ID** used on a system must also be unique within the network, ie. the same ID cannot be used in the configuration of any lines on another server system in the network. The IDs 99999 and 99998 which are reserved for the H.323 lines to the Primary Server and Secondary Server respectively. The IDs 999901 to 99930 are reserved for the H.323 lines from the Primary Server to each expansion system in the network. The ID 0 cannot be used in a Server Edition network.
Number of Channels	Default = 20, Range 0 to 250; 0 to 500 for Server Edition Select systems. Defines the number of operational channels that are available on this line.
Outgoing Channels	Default = 20, Range 0 to 250; 0 to 500 for Server Edition Select systems.. This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as Number of Channels field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls.
Voice Channels	Default = 20, Range 0 to 250; 0 to 500 for Server Edition Select systems. The number of channels available for voice use.
TEI	Default = 0. Range = 0 to 127. The Terminal Equipment Identifier. Used to identify each Control Unit connected to a particular ISDN line. For Point to Point lines this is typically (always) 0. It can also be 0 on a Point to Multi-Point line, however if multiple devices are actually sharing a Point to Multi-Point line it should be set to 127 which will result in the exchange deciding on the TEI's to be used by this Control Unit.

Related Links

H.323 Line on page 315

Line | H.323 Short Codes

For some types of line, Line short codes can be applied to any digits received with incoming calls.

The line Short Code tab is shown for the following trunk types which are treated as internal or private trunks: **QSIG** (T1, E1, H.323), **BRI S0**, **H.323**, **SCN**, **IP Office**. Incoming calls on those types of trunk are not routed using **Incoming Call Route** settings. Instead the digits received with incoming calls are checked for a match as follows:

Extension number (including remote numbers in a multi-site network).

- Line short codes (excluding ? short code).
- System short codes (excluding ? short code).
- Line ? short code.
- System ? short code.

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

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

Related Links

H.323 Line on page 315

Line | H.323 VoIP Settings

These settings have changed in release 9.1. View the 9.0 settings on page 320.

This form is used to configure the VoIP setting applied to calls on the H.323 line.

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

Field	Description
Gateway IP Address	Default = Blank Enter the IP address of the gateway device at the remote end.
Port	Default = 1720 The H.323 line is identified by the IP Address:Port value. Specifying a unique port value for this IP address allows multiple lines to use the same IP address.
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. The available codecs in default preference order are: • **G.711 A-Law** • **G.711 U-LAW** • **G.729** • **G.723.1**

Table continues…

Field	Description
	Note that the default order for G.711 codecs will vary to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition, it is supported on Primary Server, Secondary Server and Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo. The codecs available in this form are set through the **System Codec** list (**System | System Codec**). The options are: • **System Default** This is the default setting. When selected, the codec list below matches the codecs set in the system wide list. • **Custom** This option allows specific configuration of the codec preferences to be different from the system list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.
Supplementary Services	Default = H450. Selects the supplementary service signaling method for use across the H.323 trunk. The remote end of the trunk must support the same option. The options are: • **None**: No supplementary services are supported. • **H450**: Use for H.323 lines connected to another PBX or device that uses H450. • **QSIG**: Use for H.323 lines connected to another PBX or device that uses QSIG.
Call Initiation Timeout	Default = 4 seconds. Range = 1 to 99 seconds. This option sets how long the system should wait for a response to its attempt to initiate a call before following the alternate routes set in an ARS form.
VoIP Silence Suppression	Default = Off. When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.
Enable FastStart for non-Avaya IP Phones	Default = Off A fast connection procedure. Reduces the number of messages that need to be exchanged before an audio channel is created.
Fax Transport Support	Default = Off This option is only supported on trunks with their **Supplementary Services** set to **IP Office SCN** or **IP Office Small Community Network - Fallback**. Fax relay is supported across H.323 multi-site network lines with **Fax Transport Support** selected. This will use 2 VCM channels in each of the systems. Fax relay is only supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 and or IP500 Combo cards. Fax relay is supported on Server Edition Linux servers.
Local Tones	Default = Off

Table continues…

Field	Description
	When selected, the tones are generated by the local system to which the phone is registered. This option should not be used with lines being used for a multi-site network.
DTMF Support	Default = Out of Band DTMF tones can be sent to the remote end either as DTMF tones within the calls audio path (**In Band**) or a separate signals (**Out of Band**). Out of Band is recommended for compression modes such as G.729 and G.723 compression modes where DTMF in the voice stream could become distorted.
Allow Direct Media Path	Default = On This settings controls whether IP calls must be routed via the system or can be routed 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.
Progress Ends Overlap Send	Default = Off. Some telephony equipment, primarily AT&T switches, over IP trunks send a H.323 Progress rather than H.323 Proceeding message to signal that they have recognized the digits sent in overlap state. By default the system expects an H.323 Proceeding message. This option is not available by default. If required, the value **ProgressEndsOverlapSend** must be entered into the Source Numbers tab of the NoUser user.
Default Name From Display IE	Default = Off. When set, the Display IE is used as the default source for the name.

Related Links

H.323 Line on page 315
Line | H.323 VoIP Settings (Release 9.0) on page 320

Line | H.323 VoIP Settings (Release 9.0)

This form is used to configure the VoIP setting applied to calls on the H.323 line.

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

The VoIP settings available for an H.323 trunk depend on the **Supplementary Services** setting.

- Standard H.323 line VoIP Settings are applicable to trunks with their **Supplementary Services** set to **H450**, **QSIG** or **None**.
- SCN H.323 line VoIP Settings are applicable to H.323 trunks with their **Supplementary Services** set to **IP Office SCN** or **IP Office SCN - Fallback**.

Related Links

Line | H.323 VoIP Settings on page 318
Standard H.323 VoIP Settings (Release 9.0) on page 321
SCN H.323 VoIP Settings (Release 9.0) on page 324

Standard H.323 VoIP Settings (Release 9.0)

The following settings are applicable to trunks with their **Supplementary Services** set to other than **IP Office SCN** or **IP Office Small Community Network - Fallback**.

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

Field	Description
Gateway IP Address	Default = Blank Enter the IP address of the gateway device at the remote end.
Port	Default = 1720 The H.323 line is identified by the IP Address:Port value. Specifying a unique port value for this IP address allows multiple lines to use the same IP address.
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. The available codecs in default preference order are: • **G.711 A-Law** • **G.711 U-LAW** • **G.729** • **G.723.1** Note that the default order for G.711 codecs will vary to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition, it is supported on Primary Server, Secondary Server and Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo. The codecs available in this form are set through the **System Codec** list (**System | System Codec**). The options are: • **System Default** This is the default setting. When selected, the codec list below matches the codecs set in the system wide list. • **Custom** This option allows specific configuration of the codec preferences to be different from the system list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.

Table continues…

Field	Description
Supplementary Services	Default = IP Office SCN Selects the supplementary service signaling method for use across the H.323 trunk. The remote end of the trunk must support the same option. The options are: • **None**: No supplementary services are supported. • **H450**: Use for H.323 lines connected to another PBX or device that uses H450. • **QSIG**: Use for H.323 lines connected to another PBX or device that uses QSIG. • **IP Office SCN**: This option is used for H.323 trunks within a multi-site network. The systems within a multi-site network automatically exchange information about users and extensions, allowing remote users to be called without any additional configuration on the local system. For full details of Small Community Network operation see Small Community Networking. For full details of a Server Edition network, see Server Edition Mode. • **IP Office SCN - Fallback**: This option is used for a multi-site network trunk connection as above, where the system at the end of the trunk will try to take over the selected **SCN Backup Options** if this system is not visible within the multi-site network for a period of more than 3 minutes. See Small Community Network Fallback. Note that both ends of the SCN trunk connection must be set to fallback. On the system requesting backup, the required **SCN Backup Options** are selected, indicating that it is requesting backup. A single system can only request backup from one other system. A system providing backup can provide backup for up to 7 other systems.
Location	Default = Cloud. Specify a location to associate the extension with a physical location. Associating an extension with a location: • Allows emergency services to identify the source of an emergency call. • Allows you to configure call access control settings for the location. The drop down list contains all locations that have been defined in the **Location** form.
Call Initiation Timeout	Default = 4 seconds. Range = 1 to 99 seconds. This option sets how long the system should wait for a response to its attempt to initiate a call before following the alternate routes set in an ARS form.
VoIP Silence Suppression	Default = Off When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.
Enable FastStart for non-Avaya IP Phones	Default = Off

Table continues…

Field	Description
	A fast connection procedure. Reduces the number of messages that need to be exchanged before an audio channel is created.
Fax Transport Support	Default = Off This option is only supported on trunks with **Supplementary Services** set to **IP Office SCN** or **IP Office Small Community Network - Fallback**. Fax relay is supported across H.323 multi-site network lines with **Fax Transport Support** selected. This will use 2 VCM channels in each of the systems. Fax relay is only supported on IP500/IP500 V2 systems with IP500 VCM, IP500 VCM V2 and or IP500 Combo cards. Fax relay is supported on Server Edition Linux servers.
Local Tones	Default = Off When selected, the tones are generated by the local system to which the phone is registered. This option should not be used with lines being used for a multi-site network.
DTMF Support	Default = Out of Band DTMF tones can be sent to the remote end either as DTMF tones within the calls audio path (**In Band**) or a separate signals (**Out of Band**). Out of Band is recommended for compression modes such as G.729 and G.723 compression modes where DTMF in the voice stream could become distorted. For trunks with **Supplementary Services** set to **IP Office SCN** or **IP Office SCN - Fallback**, this option is fixed to **Out of Band**.
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.
Progress Ends Overlap Send	Default = Off. Some telephony equipment, primarily AT&T switches, over IP trunks send a H.323 Progress rather than H.323 Proceeding message to signal that they have recognized the digits sent in overlap state. By default the system expects an H.323 Proceeding message. This option is not available by default. If required, the value **ProgressEndsOverlapSend** must be entered into the Source Numbers tab of the NoUser user.
Default Name From Display IE	Default = Off. When set, the Display IE is used as the default source for the name.

Related Links

Line | H.323 VoIP Settings (Release 9.0) on page 320

SCN H.323 VoIP Settings (Release 9.0)

The following settings are applicable to H.323 trunks with their **Supplementary Services** set to **IP Office SCN** or **IP Office SCN - Fallback**.

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

Server Edition Network Usage

In a Server Edition network, all systems are linked in a star topography to the the Primary Server, using an H.323 IP trunk with its **Outgoing Group ID** set to **99999**. If the network also includes a Secondary Server, all systems are also linked to the Secondary Server using an H.323 IP trunk with its **Outgoing Group IP** set to **99998**.

These are the only H.323 IP trunks supported within the Server Edition network.

Field	Description
Gateway IP Address	Default = Blank Enter the IP address of the gateway device at the remote end. This address must not be shared by any other IP line (H.323, SIP, SES or IP DECT).
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. The available codecs in default preference order are: • **G.711 A-Law** • **G.711 U-LAW** • **G.729** • **G.723.1** Note that the default order for G.711 codecs will vary to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition, it is supported on Primary Server, Secondary Server and Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo. The codecs available in this form are set through the **System Codec** list (**System | System Codec**). The options are: • **System Default** This is the default setting. When selected, the codec list below matches the codecs set in the system wide list. • **Custom** This option allows specific configuration of the codec preferences to be different from the system list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.

Table continues…

Field	Description
Supplementary Services	Default = IP Office SCN Selects the supplementary service signaling method for use across the H.323 trunk. The remote end of the trunk must support the same option. The options are: • **None**: No supplementary services are supported. • **H450**: Use for H.323 lines connected to another PBX or device that uses H450. • **QSIG**: Use for H.323 lines connected to another PBX or device that uses QSIG. • **IP Office SCN**: This option is used for H.323 trunks within a multi-site network. The systems within a multi-site network automatically exchange information about users and extensions, allowing remote users to be called without any additional configuration on the local system. For full details of Small Community Network operation see Small Community Networking. For full details of a Server Edition network, see Server Edition Mode. • **IP Office SCN - Fallback**: This option is used for a multi-site network trunk connection as above, where the system at the end of the trunk will try to take over the selected **SCN Backup Options** if this system is not visible within the multi-site network for a period of more than 3 minutes. See Small Community Network Fallback. Note that both ends of the SCN trunk connection must be set to fallback. On the system requesting backup, the required **SCN Backup Options** are selected, indicating that it is requesting backup. A single system can only request backup from one other system. A system providing backup can provide backup for up to 7 other systems.
SCN Backup Options These options are only available when the **Supplementary Services** option is set to **IP Office - Fallback**. The intention of this feature is to attempt to maintain a minimal level of operation while problems with the local system are resolved.	
Backs up my IP Phones	Default = On. This option is used for Avaya 1600, 4600, 5600 and 9600 Series phones registered with the system. When selected, it will share information about the registered phones and users on those phones with the other system. If the local system is no longer visible to the phones, the phones will reregister with the other system. The users who were currently on those phones will appear on the other system as if they had hot desked. Note that when the local system is restored to the network, the phones will not automatically re-register with it. A phone reset via either a phone power cycle or using the System Status Application is required. When phones have registered with the other system, they will show an **R** on their display. If using resilience backup to support Avaya IP phones, **Auto-create Extn** and **Auto-create User** should not be left enabled after initial configuration or any

Table continues…

Field	Description
	subsequent addition of new extensions and users. Leaving auto-create options enabled on a system that is a failover target may cause duplicate extension/user records on the multi-site network under multiple failure scenarios.
Backs up my Hunt Groups	Default = On. When selected, any hunt groups the local system is advertising to the network are advertised from the other system when fallback is required. The trigger for this occurring is Avaya H.323 phones registered with the local system registering with the other system, ie. **Backs up my IP Phones** above must also be enabled. In a Server Edition network this option is only available on the H.323 trunk from the Primary Server to the Secondary Server. When used, the only hunt group members that will be available are as follows: • If the group was a distributed hunt group, those members who were remote members on other systems still visible within the network. • Any local members who have hot desked to another system still visible within the network. When the local system becomes visible to the other system again, the groups will return to be advertised from the local system.
Backs up my Voicemail	Default = On. This option can be used if the local system is hosting the Voicemail Pro server being used by the network. If selected, when the local system is no longer visible to the voicemail server, the other system will act as host for the voicemail server. In a Server Edition network this option is only available on the H.323 trunk from the Primary Server to the Secondary Server. It is assumed as being on an is automatically set by the Resilience Administration tool. The option: • requires the other system to have licenses for the Voicemail Pro features that are required to operate during any fallback period. • requires Voicemail Pro 5.0+.
Call Initiation Timeout	Default = 4 seconds. Range = 1 to 99 seconds. This option sets how long the system should wait for a response to its attempt to initiate a call before following the alternate routes set in an ARS form.
VoIP Silence Suppression	Default = Off. When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.
Fax Transport Support	Default = Off This option is only supported on trunks with their **Supplementary Services** set to **IP Office SCN** or **IP Office Small Community Network - Fallback**. Fax relay is supported across H.323 multi-site network lines with **Fax Transport Support**

Table continues…

Field	Description
	selected. This will use 2 VCM channels in each of the systems. Fax relay is only supported on IP500/IP500 V2 systems with IP500 VCM, IP500 VCM V2 and or IP500 Combo cards. Fax relay is supported on Server Edition Linux servers.
Local Tones	Default = Off. When selected, the tones are generated by the local system to which the phone is registered. This option should not be used with lines being used for a multi-site network.
DTMF Support	Default = Out of Band DTMF tones can be sent to the remote end either as DTMF tones within the calls audio path (**In Band**) or a separate signals (**Out of Band**). Out of Band is recommended for compression modes such as G.729 and G.723 compression modes where DTMF in the voice stream could become distorted. For trunks with **Supplementary Services** set to **IP Office SCN** or **IP Office SCN - Fallback**, this option is fixed to **Out of Band**.
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.

Related Links

Line | H.323 VoIP Settings (Release 9.0) on page 320

IP DECT Line

This type of line can be manually added. They are used to route voice calls over an IP data connection to an Avaya IP DECT system. Only one IP DECT line can be added to a system. Refer to the IP DECT R4 Installation manual for full details.

Currently, only one IP DECT line is supported on a system.

Related Links

Line on page 272
Line | IP DECT Line on page 328

Line | IP DECT Gateway on page 328
Line | IP DECT VoIP on page 333

Line | IP DECT Line

These settings have changed in release 9.1. View the 9.0 settings. on page 328

When creating an IP DECT line, these settings are mergeable. You can also remove an IP DECT line without rebooting. The following actions are not meregable:

- Changing an existing IP DECT line.
- Changing an IP DECT line that has been imported into the configuration.

Field	Description
Line Number	This number is allocated by the system and is not adjustable.
Associated Extensions	Lists all the DECT extensions associated with the IP DECT line.
Description	Default = Blank. Maximum 31 characters. Use this field to enter a description of this configuration.

Related Links

IP DECT Line on page 327
Line | IP DECT Line (9.0) on page 328

Line | IP DECT Line (9.0)

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

Field	Description
Line Number	This number is allocated by the system and is not adjustable.
Associated Extensions	Lists all the DECT extensions associated with the IP DECT line.

Related Links

Line | IP DECT Line on page 328

Line | IP DECT Gateway

These settings have changed in release 9.1. View the release 9.0 settings. on page 331

This form is used to configure aspects of information exchange between the IP Office and IP DECT systems.

When creating an IP DECT line, these settings are mergeable. You can also remove an IP DECT line without rebooting. The following actions are not meregable:

- Changing an existing IP DECT line.
- Changing an IP DECT line that has been imported into the configuration.

Field	Description
Auto-Create Extension	Default = Off. If enabled, subscription of a handset with the DECT system causes the auto-creation of a matching numbered extension within the system configuration if one does not already exist.
Auto-Create User	Default = Off. This option is only usable if **Auto-Create Extension** is also enabled. If enabled, subscription of a handset with the DECT system causes the auto-creation of a matching user within the system configuration if one does not already exist.
Enable DHCP Support	Default = Off This option is not supported for use with Avaya IP DECT R4. The IP DECT base stations require DHCP and TFTP support. Enable this option if the system is being used to provide that support, using IP addresses from its DHCP range (LAN1 or LAN2) and its TFTP server setting. If not enabled, alternate DHCP and TFTP options must be provided during the IP DECT installation. • If it is desired to use the system for DHCP support of the ADMM and IP DECT base stations only, the system address range should be set to match that number of addresses. Those addresses are then taken during the system restart and will not be available for other DHCP responses following the restart. • For larger IP DECT installations, the use of a non-embedded TFTP software option other than Manager is recommended.
Boot File	Default = ADMM_RFP_1_0_0.tftp. Range = Up to 31 characters. The name and path of the ADMM software file. The path is relative to the TFTP server root directory.
ADMM MAC Address	Default = 00:00:00:00:00:00 This field must be used to indicate the MAC address of the IP DECT base station that should load the ADMM software file and then act as the IP DECT system's ADMM. The address is entered in hexadecimal format using comma, dash, colon or period separators.
VLAN ID	Default = Blank. Range = 0 to 4095. If VLAN is being used by the IP DECT network, this field sets the VLAN address assigned to the base stations by the system if Enable DHCP Support is selected. • The system itself does not apply or use VLAN marking. It is assumed that the addition of VLAN marking and routing of VLAN traffic is performed by other switches within the customer network. • An ID of zero is not recommended for normal VLAN operation. • When blank, no VLAN option is sent to the IP DECT base station.
Base Station Address List	Default = Empty This box is used to list the MAC addresses of the IP DECT base stations, other than the base station being used as the ADMM and entered in the ADMM MAC Address field. Right-click on the list to select Add or Delete. or use the Insert and Delete keys. The

Table continues…

Field	Description
	addresses are entered in hexadecimal format using comma, dash, colon or period separators.
Enable Provisioning This option can be used with DECT R4 systems. It allows the setting of several values in the system configuration that previously needed to be set separately in the master base stations configuration. For full details refer to the DECT R4 Installation manual. The use of provisioning requires the system security settings to include an **IPDECT Group**.	
SARI/PARK	Default = 0 Enter the PARK (Portable Access Rights Key) license key of the DECT R4 system. DECT handset users enter this key when subscribing to the DECT system.
Subscriptions	Default = Disabled Select the method of subscription supported for handsets subscribing to the DECT R4 system. The options are: • **Disabled**:Disables subscription of handsets. • **Auto-Create**: Allow anonymous subscription of handsets. Once subscribed, the handset is assigned a temporary extension number. That extension number can be confirmed by dialing ***#**. A new extension number can be specified by dialing <Extension Number>*<Login Code>**#**. The **Auto-Create Extension** and **Auto-Create User** settings above should also be enabled. While configured to this mode, Manager will not allow the manual addition of new IP DECT extensions. • **Preconfigured**: Allow subscription only against existing IP DECT extensions records in the system configuration. The handset IPEI number is used to match the subscribing handset to a system extension.
Authentication Code	Default = Blank. Set an authentication code that DECT handset users should enter when subscribing to the DECT system.
Enable Resiliency Default = Off. Enables resiliency on the IP DECT Line. To configure resiliency, you must also configure an IP Office Line with **Backs up my IP Dect Phones** set to **On**.	
Status Enquiry Period	Default = 30 seconds. The period between successive verifications on the H.323 channel. The smaller the interval, the faster the IP DECT system recognizes that IP Office is down.
Prioritize Primary	Default = Off. Only available when **Enable Provisioning** is set to **On**. Set to **On** for automatic fail-over recovery. When on, the IP DECT system switches automatically from the backup IP Office to the "primary" IP Office.

Table continues…

Field	Description
	Note that the IP DECT system does not switch back automatically from the backup IP Office to the primary. The IP DECT system must be manually switched using Web Manager.
Supervision Timeout	Default = 120 seconds. Only available when **Enable Provisioning** is set to **On**. The period of time the IP DECT system will wait between attempts to switch from the backup IP Office to its "primary" IP Office.

Related Links

IP DECT Line on page 327
Line | IP DECT Gateway (9.0) on page 331

Line | IP DECT Gateway (9.0)

This form is used to configure aspects of information exchange between the IP Office and IP DECT systems.

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

Field	Description
Auto-Create Extension	Default = Off. If enabled, subscription of a handset with the DECT system causes the auto-creation of a matching numbered extension within the system configuration if one does not already exist.
Auto-Create User	Default = Off. This option is only usable if **Auto-Create Extension** is also enabled. If enabled, subscription of a handset with the DECT system causes the auto-creation of a matching user within the system configuration if one does not already exist.
Enable DHCP Support	Default = Off This option is not supported for use with Avaya IP DECT R4. The IP DECT base stations require DHCP and TFTP support. Enable this option if the system is being used to provide that support, using IP addresses from its DHCP range (LAN1 or LAN2) and its TFTP server setting. If not enabled, alternate DHCP and TFTP options must be provided during the IP DECT installation. • If it is desired to use the system for DHCP support of the ADMM and IP DECT base stations only, the system address range should be set to match that number of addresses. Those addresses are then taken during the system restart and will not be available for other DHCP responses following the restart. • For larger IP DECT installations, the use of a non-embedded TFTP software option other than Manager is recommended.
Boot File	Default = ADMM_RFP_1_0_0.tftp. Range = Up to 31 characters.

Table continues…

Field	Description
	The name and path of the ADMM software file. The path is relative to the TFTP server root directory.
ADMM MAC Address	Default = 00:00:00:00:00:00 This field must be used to indicate the MAC address of the IP DECT base station that should load the ADMM software file and then act as the IP DECT system's ADMM. The address is entered in hexadecimal format using comma, dash, colon or period separators.
VLAN ID	Default = Blank. Range = 0 to 4095. If VLAN is being used by the IP DECT network, this field sets the VLAN address assigned to the base stations by the system if Enable DHCP Support is selected. • The system itself does not apply or use VLAN marking. It is assumed that the addition of VLAN marking and routing of VLAN traffic is performed by other switches within the customer network. • An ID of zero is not recommended for normal VLAN operation. • When blank, no VLAN option is sent to the IP DECT base station.
Base Station Address List	Default = Empty This box is used to list the MAC addresses of the IP DECT base stations, other than the base station being used as the ADMM and entered in the ADMM MAC Address field. Right-click on the list to select Add or Delete. or use the Insert and Delete keys. The addresses are entered in hexadecimal format using comma, dash, colon or period separators.
Enable Provisioning	This option can be used with DECT R4 systems. It allows the setting of several values in the system configuration that previously needed to be set separately in the master base stations configuration. For full details refer to the DECT R4 Installation manual. The use of provisioning requires the system security settings to include an **IPDECT Group**.
SARI/PARK	Default = 0 Enter the PARK (Portable Access Rights Key) license key of the DECT R4 system. DECT handset users enter this key when subscribing to the DECT system.
Subscriptions	Default = Disabled Select the method of subscription supported for handsets subscribing to the DECT R4 system. The options are: • **Disabled**:Disables subscription of handsets. • **Auto-Create**: Allow anonymous subscription of handsets. Once subscribed, the handset is assigned a temporary extension number. That extension number can be confirmed by dialing ***#**. A new extension number can be specified by dialing <Extension Number>***<Login Code>**#**. The **Auto-Create Extension** and **Auto-Create User** settings above should also be enabled. While configured to this mode, Manager will not allow the manual addition of new IP DECT extensions. • **Preconfigured**: Allow subscription only against existing IP DECT extensions records in the system configuration. The handset IPEI number is used to match the subscribing handset to a system extension.

Table continues…

Field	Description
Authentication Code	Default = Blank. Set an authentication code that DECT handset users should enter when subscribing to the DECT system.

Related Links

Line | IP DECT Gateway on page 328

Line | IP DECT VoIP

These settings have changed in release 9.1. View the release 9.0 settings. on page 334

This form is used to configure the VoIP setting applied to calls on the IP DECT line.

When creating an IP DECT line, these settings are mergeable. You can also remove an IP DECT line without rebooting. The following actions are not meregable:

- Changing an existing IP DECT line.
- Changing an IP DECT line that has been imported into the configuration.

Field	Description
Gateway IP Address	Default = Blank. Enter the IP address of the gateway device at the remote end. This address must not be shared by any other IP line (H.323, SIP, SES or IP DECT).
Standby IP Address	Default = Blank. IP Address of the Standby Master IP Base Station or the second Mirror Base Station. When the primary Mirror Base Station or Master Base Station is offline the second Mirror or the Standby Master will take over and the system will use this IP address.
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. The available codecs in default preference order are: • **G.711 A-Law** • **G.711 U-LAW** • **G.729** • **G.723.1** Note that the default order for G.711 codecs will vary to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition, it is supported on Primary Server, Secondary Server and Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo.

Table continues…

Field	Description
	The codecs available in this form 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 matches the codecs set in the system wide list. • **Custom** This option allows specific configuration of the codec preferences to be different from the system list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.
TDM | IP Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the system TDM interface to the IP connection. This field is not shown on Linux based platforms.
IP | TDM Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the IP connection to the system TDM interface. This field is not shown on Linux based platforms.
VoIP Silence Suppression	Default = Off. When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.
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.

Related Links

IP DECT Line on page 327
Line | IP DECT VoIP (9.0) on page 334

Line | IP DECT VoIP (9.0)

This form is used to configure the VoIP setting applied to calls on the IP DECT line.

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

Field	Description
Gateway IP Address	Default = Blank.

Table continues…

Field	Description
	Enter the IP address of the gateway device at the remote end. This address must not be shared by any other IP line (H.323, SIP, SES or IP DECT).
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. The available codecs in default preference order are: • **G.711 A-Law** • **G.711 U-LAW** • **G.729** • **G.723.1** Note that the default order for G.711 codecs will vary to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition, it is supported on Primary Server, Secondary Server and Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo. The codecs available in this form are set through the **System Codec** list (**System | System Codec**). The options are: • **System Default** This is the default setting. When selected, the codec list below matches the codecs set in the system wide list. • **Custom** This option allows specific configuration of the codec preferences to be different from the system list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.
TDM | IP Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the system TDM interface to the IP connection. This field is not shown on Linux based platforms.
IP | TDM Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the IP connection to the system TDM interface. This field is not shown on Linux based platforms.
VoIP Silence Suppression	Default = Off. When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.
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.

Table continues…

Field	Description
	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.

Related Links

Line | IP DECT VoIP on page 333

SIP Line

IP Office supports SIP voice calls through the addition of SIP lines to the system configuration. This approach allows users with non-SIP phones to make and receive SIP calls.

For information on SIP line specifications and a procedure for configuring a SIP line, see Configuring SIP Trunks on page 705.

Related Links

Line on page 272
Line | SIP Line on page 336
Line | SIP Transport on page 346
Line | SIP URI on page 349
Line | SIP VoIP on page 352
Line | SIP T38 Fax on page 358
Line | SIP Credentials on page 360
Line | SIP Advanced on page 360
Line | SIP Engineering on page 365

Line | SIP Line

These settings have changed in release 9.1. View the release 9.0 settings on page 340.

These settings are mergeable with the exception of the **Line Number** setting. Changing the **Line Number** setting requires a “merge with service disruption”. When the configuration file is sent to the system, the SIP trunk is restarted and all calls on the line are dropped.

Deleting a SIP line requires a “merge with service disruption”.

Field	Description
Line Number	Default = Automatically assigned. By default a value is assigned by the system. This value can be changed but it must be unique.

Table continues…

Field	Description
ITSP Domain Name	Default = Blank. This field is used to specify the default host part of the SIP URI in the From, To, and R-URI fields for outgoing calls. For example, in the SIP URI `name@example.com`, the host part of the URI is `example.com`. When empty, the default host is provided by the **Transport | ITSP Proxy Address** field value. If multiple addresses are defined in the **Transport | ITSP Proxy Address** field, then this field must be defined. For the user making the call, the user part of the From SIP URI is determined by the settings of the SIP URI channel record being used to route the call (see **SIP URI | Local URI**). This will use one of the following: • a specific name entered in Local URI field of the channel record. • or specify using the primary or secondary authentication name set for the line below. • or specify using the SIP Name set for the user making the call (**User | SIP | SIP Name**). For the destination of the call, the user part of the To and R-URI fields are determined by dial short codes of the form 9N/N"@example.com" where N is the user part of the SIP URI and "@example.com" is optional and can be used to override the host part of the To and R-URI.
URI	Default = SIP. When SIP or SIPS is selected in the drop-down box, the SIP URI format is used (for example, name@example.com). When **Tel** is selected in the drop-down box, the Tel URI format is used (for example, +1-425-555-4567). This affects the From field of outgoing calls. The To field for outgoing calls will always use the format specified by the short codes used for outgoing call routing. Recommendation: When SIP Secured URI is required, the URI Type should be set to SIPS. SIPS can be used only when Layer 4 Protocol is set to TLS.
Location	Default = Cloud. Specify a location to associate the line with a physical location. Associating a line with a location: • Allows emergency services to identify the source of an emergency call. • Allows you to configure call access control settings for the location. The drop down list contains all locations that have been defined in the **System | Location** form.
Prefix	Default = Blank. This prefix is removed from the called number on outgoing calls if present.
National Prefix	Default = 0. This prefix is added to calls identified as not being international.

Table continues…

Field	Description
International Prefix	Default = 00. This prefix is added to calls identified as not being national.
Country Code	Default = Blank. Set to match the local country code of the system location.
Name Priority	Default = System Default. For SIP trunks, the caller name displayed on an extension can either be that supplied by the trunk or one obtained by checking for a number match in the extension user's personal directory and the system directory. This setting determines which method is used by the line. The options are: • **System Default**: Use the system's **Default Name Priority** setting (**System | Telephony | Telephony**). • **Favour Trunk**: Display the name provided by the trunk. For example, the trunk may be configured to provide the calling number or the name of the caller. The system should display the caller information as it is provided by the trunk. If the trunk does not provide a name, the system uses the **Favour Directory** method. • **Favour Directory**: Search for a number match in the extension user's personal directory and then in the system directory. The first match is used and overrides the name provided by the SIP line. If no match is found, the name provided by the line, if any, is used.
Description	Default = Blank. Maximum 31 characters. Use this field to enter a description of this configuration.
Network Type	Default = Public. This option is available if **Restrict Network Interconnect** (**System | Telephony | Telephony**) is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
In Service	Default = On. When this field is not selected, the SIP trunk is unregistered and not available to incoming and outgoing calls.
Check OOS	Default = On. If enabled, the system will regularly check if the trunk is in service using the methods listed below. Checking that SIP trunks are in service ensures that outgoing call routing is not delayed waiting for response on a SIP trunk that is not currently usable. For UDP and TCP trunks, OPTIONS message are regularly sent. If no reply to an OPTIONS message is received the trunk is taken out of service.

Table continues…

Field	Description
	For TCP trunks, if the TCP connection is disconnected the trunk will be taken out of service. For trunks using DNS, if the IP address is not resolved or the DNS resolution has expired, the trunk is taken out of service.
Session Timers	
Refresh Method	Default = Auto. The options are: • **Auto** • **Reinvite** • **Update** When **Auto** is selected, if UPDATE is in the Allow: header from the far SIP endpoint, then it is used. Otherwise INVITE is used.
Timer (seconds)	Default = On Demand. Range = 90 to 64800 This field specifies the session expiry time. At the half way point of the expiry time, a session refresh message is sent. When set to **On Demand**, IP Office will not send a session refresh message but will respond to them.
Forwarding and Twinning	
Originator number	Default = Blank. This field can be used to set an originator number for forwarded and twinned calls when using any of the **Send Caller ID** options above other than **None**. If exported or imported as part of a trunk template, this setting is not supported by Basic Edition systems.
Send Caller ID	Default = None. Set the type of header for to use for the originating calling party information. The options are: • **Diversion Header**: Use the information from the Diversion Header. • **Remote Party ID**: Use the Remote Part ID. • **P Asserted ID**: Use the contact information from the P Asserted ID. • **None**: This option corresponds to the ISDN withheld setting. This setting is also used for forwarded calls. Note that the values on the **System | Twinning** tab override this if set. For incoming calls to a hunt group, the hunt group details will be provided and not the details of the answering agent. This setting is mergeable. The SIP line **Send Caller ID** setting takes priority.
Redirect and Transfer Redirection and blind transfer are configured separately. By default, they are disabled.	

Table continues…

Field	Description
A supervised transfer occurs when a consultation call is made and the REFER contains a Replaces: header indicating the CallID of another call leg which the REFERing agent has already initiated with the REFER target. **Note:** Do not change these settings unless directed to by the SIP service provider.	
Incoming Supervised REFER	Default = Auto. Determines if IP Office will accept a REFER being sent by the far end. The options are: • **Always**: Always accepted. • **Auto**: If the far end does not advertise REFER support in the Allow: header of the OPTIONS responses, then IP Office will reject a REFER from that endpoint. • **Never**: Never accepted.
Outgoing Supervised REFER	Default = Auto. Determines if IP Office will attempt to use the REFER mechanism to transfer a party to a call leg which IP Office has already initiated so that it can include the CallID in a Replaces: header. The options are: • **Always**: Always use REFER. • **Auto**: Use the Allow: header of the OPTIONS response to determine if the endpoint supports REFER. • **Never**: Never use REFER.
Send 302 Moved Temporarily	Default = Off. A SIP response code used for redirecting an unanswered incoming call. It is a response to the INVITE, and cannot be used after the 200 OK has been sent as a response to the INVITE.
Outgoing Blind REFER	Default = Off. When enabled, a user, voicemail system or IVR can transfer a call by sending a REFER to an endpoint that has not set up a second call. In this case, there is no Replaces: header because there is no CallID to replace the current one. This directs the far end to perform the transfer by initiating the new call and release the current call with IP Office.

Related Links

SIP Line on page 336
Line | SIP Line (Release 9.0) on page 340

Line | SIP Line (Release 9.0)

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

Field	Description
Line Number	Default = Automatically assigned.

Table continues…

Field	Description
	By default a value is assigned by the system. This value can be changed but it must be unique.
ITSP Domain Name	Default = Blank. This field is used to specify the default domain part of the SIP URI in the From, To and R-URI fields for outgoing calls. For example, in the SIP URI `name@example.com`, the domain part of the URI is `example.com`. When empty, the default domain is provided by the **Transport | ITSP Proxy Address** field value. If multiple addresses are defined in the **Transport | ITSP Proxy Address** field, then this field must be defined. For the user making the call, the user part of the From SIP URI is determined by the settings of the SIP URI channel record being used to route the call. This will use one of the following: • a specific name entered in Local URI field of the channel record. • or specify using the primary or secondary authentication name set for the line below. • or specify using the SIP Name set for the user making the call (**User | SIP | SIP Name**). For the destination of the call, the user part of the To and R-URI fields are determined by dial short codes of the form 9N/N"@example.com" where N is the user part of the SIP URI and "@example.com" is optional and can be used to override the domain in To and R-URI.
Prefix	Default = Blank. This prefix is removed from the called number on outgoing calls if present.
National Prefix	Default = 0. This prefix is added to calls identified as not being international.
Country Code	Default = Blank. Set to match the local country code of the system location.
International Prefix	Default = 00. This prefix is added to calls identified as not being national.
Send Caller ID	Default = None. Select which value the SIP line should use for the original calling party ID when routing twinned calls. The options are: • **Diversion Header**: Use the information from the Diversion Header. • **Remote Party ID**: Use the Remote Part ID. • **P Asserted ID**: Use the contact information from the P Asserted ID. • **None**: This option corresponds to the ISDN withheld setting. This setting is also used for forwarded calls. Note that the values on the **System | Twinning** tab override this if set. For incoming calls to a hunt group, the hunt

Table continues…

Field	Description
	group details will be provided and not the details of the answering agent. This setting is mergeable. The SIP line **Send Caller ID** setting takes priority.
Network Type	Default = Public. This option is available if **Restrict Network Interconnect** (**System | Telephony | Telephony**) is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Association Method	Default = By Source IP Address. This setting sets the method by which a SIP line is associated with an incoming SIP request. The match criteria used for each line can be varied. The search for a line match for an incoming request is done against each line in turn using each lines Association Method. The order of line matching uses the configured **Line Number** settings until a match occurs. If no match occurs the request is ignored. This method allows multiple SIP lines with the same address settings. This may be necessary for scenarios where it may be required to support multiple SIP lines to the same ITSP. For example when the same ITSP supports different call plans on separate lines or where all outgoing SIP lines are routed from the system via an additional on-site system. The options are: • **By Source IP Address**: This option uses the source IP address and port of the incoming request for association. The match is against the configured remote end of the SIP line, using either an IP address/port or the resolution of a fully qualified domain name. • **"From" header hostpart against ITSP domain**: This option uses the host part of the From header in the incoming SIP request for association. The match is against the **ITSP Domain Name** above. • **R-URI hostpart against ITSP domain**: This option uses the host part of the Request-URI header in the incoming SIP request for association. The match is against the **ITSP Domain Name** above. • **"To" header hostpart against ITSP domain**: This option uses the host part of the To header in the incoming SIP request for association. The match is against the **ITSP Domain Name** above. • **"From" header hostpart against DNS-resolved ITSP domain**: This option uses the host part of the FROM header in the incoming SIP request for association. The match is found by comparing the FROM header against a list of IP addresses resulting from resolution of the **ITSP Domain Name** above or, if set, the **ITSP Proxy Address** on the **Transport** tab.

Table continues…

Field	Description
	• **"Via" header hostpart against DNS-resolved ITSP domain**: This option uses the host part of the VIA header in the incoming SIP request for association. The match is found by comparing the VIA header against a list of IP addresses resulting from resolution of the **ITSP Domain Name** above or, if set, the **ITSP Proxy Address** on the **Transport** tab. • **"From" header hostpart against ITSP proxy**: This option uses the host part of the “From” header in the incoming SIP request for association. The match is against the **ITSP Proxy Address** on the **Transport** tab. • **"To" header hostpart against ITSP proxy**: This option uses the host part of the From header in the incoming SIP request for association. The match is against the **ITSP Proxy Address** on the **Transport** tab. • **R-URI hostpart against ITSP proxy**: This option uses the host part of the Request-URI in the incoming SIP request for association. The match is against the **ITSP Proxy Address** on the **Transport** tab.
REFER Support	Default = On. REFER is the method used by many SIP device, including SIP trunks, to transfer calls. These settings can be used to control whether REFER is used as the method to transfer calls on this SIP trunk to another call on the same trunk. If supported, once the transfer has been completed, the system is no longer involved in the call. If not supported, the transfer may still be completed but the call will continue to be routed via the system.
Incoming	Default = Auto Select whether REFER can or should be used when an attempt to transfer an incoming call on the trunk results in an outgoing call on another channel on the same trunk. The options are: • **Always**: Always use REFER for call transfers that use this trunk for both legs of the transfer. If REFER is not supported, the call transfer attempt is stopped. • **Auto**: Request to use REFER if possible for call transfers that use this trunk for both legs of the transfer. If REFER is not supported, transfer the call via the system as for the **Never** setting below. • **Never**: Do not use REFER for call transfers that use this trunk for both legs of the transfer. The transfer can be completed but will use 2 channels on the trunk.
Outgoing	Default = Auto Select whether REFER can or should be used when attempt to transfer an outgoing call on the trunk results in an incoming call on another channel on the same trunk. This uses system resources and may incur costs for the duration of the transferred call. The options available are the same as for the **Incoming** setting.
Method for Session Refresh	Default = Auto.

Table continues…

Field	Description
	The SIP UPDATE method (RFC 3311) allows a client to update parameters of a session (such as the set of media streams and their codecs) but has no impact on the state of a dialog. The options are: • **RE-INVITE** Re-Invite messages are sent for session refresh. • **UPDATE** UPDATE messages are sent for session refresh if the other end indicates support for UPDATE in the allow header. • **Auto** UPDATE messages are sent for session refresh if the other end indicates support for UPDATE in the allow header. If UPDATE is not supported, RE-INVITE messages are sent.
Session Timer	Default = On Demand. Range = 90 to 64800 This field specifies the session expiry time. At the half way point of the expiry time, a session refresh message is sent. Setting the field to **On Demand** disables the session timer.
Media Connection Preservation	Default = Disabled. When enabled, allows established calls to continue despite brief network failures. Call handling features are no longer available when a call is in a preserved state. Preservation on public SIP trunks is not supported until tested with a specific service provider.
In Service	Default = On. When this field is not selected, the SIP trunk is unregistered and not available to incoming and outgoing calls.
URI Type	Default = SIP. When SIP or SIPS is selected in the drop-down box, the SIP URI format is used (for example, name@example.com). When **Tel** is selected in the drop-down box, the Tel URI format is used (for example, +1-425-555-4567). This affects the From field of outgoing calls. The To field for outgoing calls will always use the format specified by the short codes used for outgoing call routing. Recommendation: When SIP Secured URI is required, the URI Type should be set to SIPS. SIPS can be used only when Layer 4 Protocol is set to TLS.
Check OOS	Default = On. If enabled, the system will regularly check if the trunk is in service using the methods listed below. Checking that SIP trunks are in service ensures that outgoing call routing is not delayed waiting for response on a SIP trunk that is not currently usable. For UDP and TCP trunks, OPTIONS message are regularly sent. If no reply to an OPTIONS message is received the trunk is taken out of service. For TCP trunks, if the TCP connection is disconnected the trunk will be taken out of service. For trunks using DNS, if the IP address is not resolved or the DNS resolution has expired, the trunk is taken out of service.
Call Routing Method	Default = Request URI.

Table continues…

Field	Description
	This field allows selection of which incoming SIP information should be used for incoming number matching by the system's incoming call routes. The options are to match either the **Request URI** or the **To Header** element provided with the incoming call.
Originator number for forwarded and twinning calls	Default = Blank. This field can be used to set a originator number for forwarded and twinned calls when using any of the **Send Caller ID** options above other than **None**. If exported or imported as part of a trunk template, this setting is not supported by Basic Edition Quick mode systems.
Name Priority	Default = System Default. For SIP trunks, the caller name displayed on an extension can either be that supplied by the trunk or one obtained by checking for a number match in the extension user's personal directory and the system directory. This setting determines which method is used by the line. The options are: • **System Default**: Use the system's **Default Name Priority** setting (**System | Telephony | Telephony**). • **Favour Trunk**: Display the name provided by the trunk. For example, the trunk may be configured to provide the calling number or the name of the caller. The system should display the caller information as it is provided by the trunk. If the trunk does not provide a name, the system uses the **Favour Directory** method. • **Favour Directory**: Search for a number match in the extension user's personal directory and then in the system directory. The first match is used and overrides the name provided by the SIP line. If no match is found, the name provided by the line, if any, is used.
Caller ID From Header	Default = Off. Incoming calls can include caller ID information in both the From field and in the PAI fields. When this option is selected, the caller ID information in the From field is used rather than that in the PAI fields.
Send From In Clear	Default = Off. When selected, the user ID of the caller is included in the From field. This applies even if the caller has selected to be or is configured to be anonymous, though their anonymous state is honored in other fields used to display the caller identity.
User-Agent and Server Headers	Default = Blank (Use system type and software level). The value set in this field is used as the User-Agent and Server value included in SIP request headers made by this line. If the field is blank, the type of IP Office system and its software level used. Setting a unique value can be useful in call diagnostics when the system has multiple SIP trunks.
Service Busy Response	Default = 486 - Busy Here (503 - Service Unavailable for the France2 locale). For calls that result in a busy response from IP Office, this setting determines the response code. The options are: • **486 - Busy Here**

Table continues…

Field	Description
	• **503 - Service Unavailable**
Action on CAC Location Limit	Default = Allow Voicemail When set to **Allow Voicmail**, the call is allowed to go to a user's voicemail when the user's location call limit has been reached. When set to **Reject Call**, the call is rejected with the failure response code configured in the **Service Busy Response** field.

Related Links

Line | SIP Line on page 336

Line | SIP Transport

Changing these settings requires a “merge with service disruption”. When the configuration file is sent to the system, the SIP trunk is restarted.

Note that **ITSP Proxy Address** and **Calls Route via Registrar** are mergeable.

Deleting a SIP line requires a “merge with service disruption”.

Behavior during Service unavailable

A proxy server is considered Active once the system has received a response to an INVITE, REGISTER or OPTIONS.

In the case of the proxy server responding with 503 - Service Unavailable, it should be considered Active - In Maintenance. In this case, the following should occur:

If the response 503 - Service Unavailable was in response to an INVITE request:

- If calls are tied to registrations (**Calls Route via Registrar** enabled) and there are other proxies available, the tied registrations should issue an Un-REGISTER and try to REGISTER with a different proxy. The call should fail with cause = Temporary Fail.
- If calls are not tied, the INVITE should be immediately tried to a different proxy.

If the response 503 - Service Unavailable was in response to a REGISTER request:

If there are other proxies available, this registration only should issue an Un-REGISTER and try to REGISTER with a different proxy.

If **Explicit DNS Server(s)** are configured, a DNS request should be sent out to see whether the proxy server has disappeared from those being offered.

An Active-InMaintenance proxy server should not be used for a new transactions (INVITE or REGISTER) until:

- There is a change in DNS responses indicating the proxy has become active.
- The configuration does not leave any better option available. In this case, there should be a throttle so that no more than 5 failures (without successes) in 1 minute should be allowed.
- A config merge has occurred where the proxy string is changed.
- 10 minutes has expired.

Behavior during Not Responding

A proxy server that is not-responding (UDP) is indicated when 3 requests are sent and no replies are received. This would normally occur during a single INVITE transaction.

Consideration should be given whether this is caused by a local network fault or is caused by the Proxy being out of service. Since it is likely to be local, no action should be taken unless traffic is received from an alternative proxy while this proxy is actually not responding. The state should be "Possibly non responding".

If explicit DNS servers are configured, a DNS request should be sent out to see whether this Proxy server has disappeared from those being offered.

If possible, an alternative proxy should be stimulated simultaneously with stimulating the suspect server.

The server should be considered non-responding if it is persistently nonresponding while other proxies are responding or if it is non-responding and has disappeared from the DNS advertisement.

While in the "possibly not responding" state, it would be better to send an INVITE to an alternative proxy while simultaneously sending any appropriate message to this proxy. This will help to resolve whether it is really not responding rather than there being local network problems. However, there is no requirement to blacklist the proxy.

Once in the "definitely not responding" state:

- If there are other proxies available: this registration only issues an Un-REGISTER, and try to REGISTER with a different proxy. Calls do not automatically clear.
- If a SIP message is received from it, the state should immediately go"Active".
- This proxy should be blacklisted unless there are no better options available. While blacklisted, only one transaction per 10 minutes is allowed.
- Even if not blacklisted, there should be a throttle so that no more than 5 failures (without successes) in 1 minute should be alowed.

Field	Description
ITSP Proxy Address	Default = Blank This is the SIP Proxy address used for outgoing SIP calls. The address can be specified in the following ways: • If left blank, the ITSP Domain Name is used and is resolved by DNS resolution in the same way as if a DNS address had been specified as below. • An IP address. • A list of up to 4 IP addresses, with each address separated by a comma or space. - The addresses can include an indication of the relative call weighting of each address compared to the others. This is done by adding a **w N** suffix to the address where **N** is the weighting value. For example, in the list 213.74.81.102w3 213.74.81.100w2, the weighting values assigns 1.5 times the weight of calls to the first address. The default weight if not specified is 1. A weight of 0 can be used to disable an address. Weight is only applied to outgoing calls.

Table continues…

Field	Description
	If there is more than one proxy defined, and no weight indication, then calls are only sent to the first in the list until there is a failure at which point the next proxy is used. - If the **Calls Route via Registrar** setting below is enabled, the weighting is applied to registrations rather than calls. • A DNS address, for example sbc.example.com. - The DNS response may return multiple proxy addresses (RFC 3263). If that is the case, the system will resolve the address to use based on priority, TTL and weighting information included with each address. - A load balancing suffix can be added to specify that multiple proxy results should be returned if possible, for example sbc.example.com(N). where **N** is the required number of addresses from 1 to 4. This field is mergeable. However, no more than 4 IP Addresses should be in use at any time. So, if the combined new and old address settings exceed 4, the new addresses are only phased into use as transactions in progress on the previous addresses are completed.
Network Configuration	
Layer 4 Protocol	Default = UDP. The options are: • **TCP** • **UDP** • **TLS** • **Auto** TLS connections support the following ciphers: • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA
Use Network Topology Info	Default = None. This field associates the SIP line with the **Network Topology** settings (**System | LAN1 | Network Topology**) settings of the LAN interface. It also applies the LAN interfaces **DiffServ Settings** (**System | LAN1 | VoIP**) to the outgoing traffic on the SIP line. If **None** is selected, STUN lookup is not applied and routing is determined by the system's routing tables. If no STUN server address is set for the interface, then the **Binding Refresh Time** (**System | LAN | Network Topology**) is ignored by SIP Lines when calculating the periodic OPTIONS timing unless the **Firewall/NAT Type** is set to **Open Internet**.

Table continues…

Field	Description
Send Port	When Network Configuration is set to TLS, the default setting is 5061. When Network Configuration is set to TCP or UDP, the default setting is 5060.
Listen Port	When Network Configuration is set to TLS, the default setting is 5061. When Network Configuration is set to TCP or UDP, the default setting is 5060.
Explicit DNS Server(s)	Default = 0.0.0.0 (Off) If specific DNS servers should be used for SIP trunk operation rather than the general DNS server specified or obtained for the system, the server addresses can be specified here. If exported or imported as part of a trunk template, this setting not supported by Basic Edition Quick mode systems.
Calls Route via Registrar	Default = On If selected, all calls are routed via the same proxy as used for registration. If multiple ITSP proxy addresses have been specified, there is no load balancing of registrations.
Separate Registrar	Default = Blank This field allows the SIP registrar address to be specified if it is different from that of the SIP proxy. The address can be specified as an IP address or DNS name.

Related Links

SIP Line on page 336

Line | SIP URI

Having setup the SIP trunk to the SIP ITSP, the SIP URI's registered with that ITSP are entered on this tab. A SIP URI (Uniform Resource Identifier) is similar to an internet email address and represents the source or destination for SIP connection. The URI consists of two parts, the user part (eg. name) and the host part (eg. example.com).

If the wildcard * is used in the SIP trunk's **Local URI**, **Contact** and **Display** fields, that SIP trunk will accept any incoming SIP call. The incoming call routing is still performed by the system incoming call routes based on matching the values received with the call or the URI's incoming group setting. For outgoing calls using this SIP URI, all valid short code CLI manipulations are used (transforming calling party number to ISDN will be ignored).

For the system, each SIP URI acts as a set of trunk channels. Outgoing calls can then be routed to the required URI by short codes that match that URI's **Outgoing Group** setting. Incoming calls can be routed by incoming call routes that match the URI's **Incoming Group** setting.

Note that the system only supports up to 150 URI records on a SIP line.

These settings are mergeable, with the exception of the **Registration** setting. Changing the **Registration** setting requires a “merge with service disruption”. When the configuration file is sent to the system, the SIP trunk is restarted and all calls on the line are dropped.

Deleting a SIP line requires a “merge with service disruption”.

Field	Description
Via	This field is for information only and cannot be edited. It shows the IP address of the system LAN interface with which the SIP trunk is associated.
Local URI	Default = Use Authentication Name This field sets the 'From' field for outgoing SIP calls using this URI. The value can either be entered manually or one of the following options can be selected: • **Use Credentials User Name**: Use the **User Name** from the **SIP Credentials** record being used for the call. • **Use Internal Data**: Use the **SIP Name** value from the **User | SIP** tab of the user making the call. The system can also use SIP URI information configured for a hunt group (**Hunt Group | SIP**) or for the voicemail (**System | Voicemail**). • **Use Credentials Authentication Name**: Use the **Authentication Name** from the **SIP Credentials** record being used for the call. • **Use Credentials Contact**: Use the **Contact** information from the **SIP Credentials** record being used for the call.
Contact	Default = Use Authentication Name This field sets the 'Contact' field for SIP calls using this URI. The value can either be entered manually or one of the following options can be selected: • **Use Credentials User Name**: Use the **User Name** from the **SIP Credentials** record being used for the call. • **Use Internal Data**: Use the **SIP Name** value from the **User | SIP** tab of the user making the call. The system can also use SIP URI information configured for a hunt group (**Hunt Group | SIP**) or for the voicemail (**System | Voicemail**). • **Use Credentials Authentication Name**: Use the **Authentication Name** from the **SIP Credentials** record being used for the call. • **Use Credentials Contact**: Use the **Contact** information from the **SIP Credentials** record being used for the call.
Display Name	Default = Use Authentication Name This field sets the 'Name' value for SIP calls using this URI. The value can either be entered manually or one of the following options can be selected: • **Use Credentials User Name**: Use the **User Name** from the **SIP Credentials** record being used for the call. • **Use Internal Data**: Use the **SIP Name** value from the **User | SIP** tab of the user making the call. The system can also use SIP URI information configured for a hunt group (**Hunt Group | SIP**) or for the voicemail (**System | Voicemail**). • **Use Credentials Authentication Name**: Use the **Authentication Name** from the **SIP Credentials** record being used for the call. • **Use Credentials Contact**: Use the **Contact** information from the **SIP Credentials** record being used for the call.
PAI	Default = None.

Table continues…

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>You can enable P-Asserted-Identity (PAI) headers to assert the identity of users in outgoing SIP requests or response messages. Use this setting to select the source of the user identity information or enter a value manually.
Note:
You can enter the wildcard character “*”. Entering this value populates the SIP PAI header with the caller information available to IP Office.
The options are:
• None: When selected, the P-Preferred-Identity header is used instead of the P-Asserted-Identity, in order to ensure compatibility with legacy networks.
• Use Credentials User Name: Use the User Name from the SIP Credentials record being used for the call.
• Use Internal Data: Use the SIP Name value from the User | SIP tab of the user making the call. The system can also use SIP URI information configured for a hunt group (Hunt Group | SIP) or for the voicemail (System | Voicemail).
• Use Credentials Authentication Name: Use the Authentication Name from the SIP Credentials record being used for the call.
• Use Credentials Contact: Use the Contact information from the SIP Credentials record being used for the call.</td></tr>
<tr><td>Registration</td><td>Default = Primary
This field is used to select from a list of the account credentials configured on the line's SIP Credentials tab.</td></tr>
<tr><td>Incoming Group ID</td><td>Default = 0, Range 0 to 99999.
The Incoming Group ID to which a line belongs is used to match it to incoming call routes in the system configuration. The matching incoming call route is then used to route incoming calls. The same ID can be used for multiple lines.</td></tr>
<tr><td>Outgoing Group ID</td><td>Default = 0, Range 0 to 99999.
Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID.
For Basic Edition and Standard Edition deployments, the same ID can be used for multiple lines.
In a Server Edition network, the Outgoing Group ID used on a system must also be unique within the network, ie. the same ID cannot be used in the configuration of any lines on another server system in the network.
<table>
<tr><th>Reserved Group ID numbers</th><th>Description</th></tr>
<tr><td>90000 - 99999</td><td>Reserved for system use (not enforced).</td></tr>
<tr><td>99999 and 99998</td><td>In a Server Edition network, reserved for the H.323 lines to the Primary Server and Secondary Server respectively.</td></tr>
</table></td></tr>
</table>

Table continues…

Field	Description	
	999901 to 99930	In a Server Edition network, reserved for the H.323 lines from the Primary Server to each expansion system in the network.
	0	In a Server Edition network, the ID 0 cannot be used.
	98888	For IP Office deployed in an Enterprise Branch environment, reserved for the SM line.
Max Calls per Channel	Default =10 This field sets the maximum number of simultaneous calls that can use the URI before the system returns busy to any further calls. For Outbound Contact Express deployments, the maximum value is 250.	

Related Links

SIP Line on page 336

Line | SIP VoIP

These settings have changed in release 9.1. To view the release 9.0 settings click here on page 355.

This form is used to configure the VoIP settings applied to calls on the SIP trunk.

These settings are mergeable. Deleting a SIP line requires a “merge with service disruption”.

Field	Description
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. The available codecs in default preference order are: • **G.711 A-Law** • **G.711 U-LAW** • **G.729** • **G.723.1** Note that the default order for G.711 codecs will vary to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition, it is supported on Primary Server, Secondary Server and Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo. The codecs available in this form are set through the **System Codec** list (**System | System Codec**). The options are: • **System Default** This is the default setting. When selected, the codec list below matches the codecs set in the system wide list. • **Custom** This option allows specific configuration of the codec preferences to be different from the system list. When **Custom** is selected, the list can be used to

Table continues…

Field	Description
	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.
DTMF Support	Default = RFC2833. This setting is used to select the method by which DTMF key presses are signalled to the remote end. The options are: • **In Band** • **RFC2833** • **Info**
Media Security	Default = Disable. These setting control whether SRTP is used for this line 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. • **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.

Table continues…

Field	Description
Advanced Media Security Options	Not displayed if **Media Security** is set to **Disabled**. The options are: • **Same as System**: Use the same 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 trunks between networked systems, the same setting should be set at both ends.
Re-Invite Supported	Default = Off. When enabled, Re-Invite can be used during a session to change the characteristics of the session. For example when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk. Requires the ITSP to also support **Re-Invite**.
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.
Allow Direct Media Path	Default = Off. This option is only available when **Re-Invite Supported** is enabled. The 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.
Force direct media with phones	Default = Off.

Table continues…

Field	Description
	The setting is only available when the trunk's **Re-invite Supported** and **Allow Direct Media Path** settings are enabled and its DTMF Support option is set to **RFC2833/ RFC4733**. It also requires the H.323 IP extension involved in the call to also have **Allow Direct Media Path** enabled. This feature is only supported with Avaya H.323 IP telephones. For calls where the Avaya H.323 IP extension using the trunk is doing so as a direct media call, this feature allows digits pressed on the extension to be detected and the call changed to an indirect media call so that RFC2833 DTMF can be sent. The call remains as an indirect media call for 15 seconds after the last digit before reverting back to being a direct media call.
PRACK/100rel Supported	Default = Off. When selected, supports Provisional Reliable Acknowledgement (PRACK) on SIP trunks. Enable this parameter when you want to ensure that provisional responses, such as announcement messages, have been delivered. Provisional responses provide information on the progress of the request that is in process. For example, while a cell phone call is being connected, there may be a delay while the cell phone is located; an announcement such as “please wait while we attempt to reach the subscriber” provides provisional information to the caller while the request is in process. PRACK, which is defined in RFC 3262, provides a mechanism to ensure the delivery of these provisional responses.
G.711 Fax ECAN	Default = Off (Grayed out for Server Edition Linux systems.) This setting is only available when **Fax Transport Support** is set to **G.711** or **T.38 Fallback**. When IP Office detects a fax call, the IP Office negotiates to G.711 (if not already in G.711) and reconfigures the connection with echo cancellation (ECAN) based on the 'G.711 Fax ECAN field. This can be used to avoid an ECAN mismatch with the SIP trunk service provider. Also for fax calls, the connection’s NLP is disabled, a fixed jitter buffer is set and silence suppression is disabled.

Related Links

SIP Line on page 336
Line | SIP VoIP (Release 9.0) on page 355

Line | SIP VoIP (Release 9.0)

This form is used to configure the VoIP settings applied to calls on the SIP trunk.

These settings are mergeable.

Field	Description
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. The available codecs in default preference order are: • **G.711 A-Law** • **G.711 U-LAW** • **G.729** • **G.723.1**

Table continues…

Field	Description
	Note that the default order for G.711 codecs will vary to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition, it is supported on Primary Server, Secondary Server and Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo. The codecs available in this form are set through the **System Codec** list (**System | System Codec**). The options are: • **System Default** This is the default setting. When selected, the codec list below matches the codecs set in the system wide list. • **Custom** This option allows specific configuration of the codec preferences to be different from the system list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.
Fax Transport Support:	Default = Off. This option is only available if **Re-Invite Supported** is selected. When enabled, the system performs fax tone detection on calls routed via the line and, if fax tone is detected, renegotiates the call codec as configured below. The SIP line provider must support the selected fax method and Re-Invite. The system must have available VCM resources using an IP500 VCM, IP500 VCM V2 or IP500 Combo base card. For systems in a network, fax relay is supported for fax calls between the systems.The options are: • **None** Select this option if fax is not supported by the line provider. • **G.711** G.711 is used for the sending and receiving of faxes. • **T38** T38 is used for the sending and receiving of faxes. • **T38 Fallback** When you enable this option, T38 is used for sending and receiving faxes on a SIP line. If the called destination does not support T38, the system will send a re-invite to change the transport method to G.711. This option is not supported by Linux based systems.
Location	Default = Cloud. Specify a location to associate the extension with a physical location. Associating an extension with a location: • Allows emergency services to identify the source of an emergency call. • Allows you to configure call access control settings for the location. The drop down list contains all locations that have been defined in the **System | Location** form.
Call Initiation Timeout	Default = 4 seconds. Range = 1 to 99 seconds. This option sets how long the system should wait for a response to its attempt to initiate a call before following the alternate routes set in an ARS form.
DTMF Support	Default = RFC2833.

Table continues…

Field	Description
	This setting is used to select the method by which DTMF key presses are signalled to the remote end. The options are: • **In Band** • **RFC2833** • **Info**
VoIP Silence Suppression	Default = Off When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.
Allow Direct Media Path	Default = Off. This setting is only supported on Server Edition systems. This option is only available when **Re-Invite Supported** is enabled. The 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.
Re-Invite Supported	Default = Off. When enabled, Re-Invite can be used during a session to change the characteristics of the session. For example when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk. Requires the ITSP to also support **Re-Invite**.
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.
PRACK/100rel Supported	Default = Off. When selected, supports Provisional Reliable Acknowledgement (PRACK) on SIP trunks. Enable this parameter when you want to ensure that provisional responses, such as announcement messages, have been delivered. Provisional responses provide information on the progress of the request that is in process. For example, while a cell phone call is being connected, there may be a delay while the cell phone is located; an announcement such as “please wait while we attempt to reach the subscriber” provides provisional information to the caller while the request is in

Table continues…

Field	Description
	process. PRACK, which is defined in RFC 3262, provides a mechanism to ensure the delivery of these provisional responses.
Force direct media with phones	Default = Off. The setting is only useable when the trunk's **Re-invite Supported** and **Allow Direct Media Path** settings are enabled and its DTMF Support option is set to **RFC2833/ RFC4733**. It also requires the H.323 IP extension involved in the call to also have **Allow Direct Media Path** enabled. This feature is only supported with Avaya H.323 IP telephones. For calls where the Avaya H.323 IP extension using the trunk is doing so as a direct media call, this feature allows digits presses on the extension to be detected and the call changed to an indirect media call so that RFC2833 DTMF can be sent. The call remains as an indirect media call for 15 seconds after the last digit before reverting back to being a direct media call.

Related Links

Line | SIP VoIP on page 352

Line | 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.

Changing these settings requires a “merge with service disruption”. When the configuration file is sent to the system, the SIP trunk is restarted and all calls on the line are dropped.

Deleting a SIP line requires a “merge with service disruption”.

Field	Description
Use Default Values	Default = On. If selected, all the fields are set to their default values and greyed out.
T38 Fax Version	Default = 3. During fax relay, the two gateways will negotiate to use the highest version which they both support. The options are: • **0** • **1** • **2** • **3**
Transport	Default = UDPTL (fixed). Only **UDPTL** is supported. **TCP** and **RTP** transport are not supported. For **UDPTL**, redundancy error correction is supported. Forward Error Correction (FEC) is not supported.

Table continues…

Field	Description
Redundancy Redundancy sends additional fax packets in order to increase the reliability. However increased redundancy increases the bandwidth required for the fax transport.	
Low Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for low speed V.21 T.30 fax transmissions.
High Speed	Default = 0 (No redundancy). Range = 0 to 5. Sets the number of redundant T38 fax packets that should be sent for V.17, V.27 and V.28 fax transmissions.
TCF Method	Default = Trans TCF. TCF = Training Check Frame.
Max Bit Rate (bps)	Default = 14400. Lower rates can be selected if the current rate is not supported by the fax equipment or is found to not be reliable.
EFlag Start Timer (msecs)	Default = 2600.
EFlag Stop Timer (msecs)	Default = 2300.
Tx Network Timeout (secs)	Default = 150.
Scan Line Fix-up	Default = On.
TFOP Enhancement	Default = On.
Disable T30 ECM	Default = Off. When selected, disabled the T.30 Error Correction Mode used for fax transmission.
Disable EFlags For First DIS	Default = Off.
Disable T30 MR Compression	Default = Off.
NSF Override	Default = Off. If selected, the NSF (Non-Standard Facility) information sent by the T38 device can be overridden using the values in the fields below. **Country Code**: Default = 0. **Vendor Code**: Default = 0.

Related Links

SIP Line on page 336

Line | SIP Credentials

Used to enter the ITSP username and password for the SIP account with the ITSP. If you have several SIP accounts going to the same ITSP IP address or domain name, you can enter up to 30 sets of ITSP account names and passwords on this tab.

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

Deleting a SIP line requires a “merge with service disruption”.

Use the **Add**, **Remove**, and **Edit** buttons to manage the set of credentials for the SIP trunk accounts. The settings for each account are listed below.

Field	Descriptions
Index	This number is assigned automatically and cannot be edited. If the **From** field on the SIP URI being used for the call is set to **Use Authentication Name** , the registration field of the SIP URI will indicate the index number of the SIP credentials to use for calls by that SIP URI.
User Name	This name must be unique and is used to identify the trunk. The name can include the domain if necessary.
Authentication Name	Default = Blank. This field can be blank but must be completed if a **Password** is also specified. This value is provided by the SIP ITSP. Depending on the settings on the Local URI tab associated with the SIP call, it may also be used as the user part of the SIP URI. The name can include the domain if necessary.
Contact	Default = Blank. This field is used to enter a contact and can include the domain if necessary.
Password	Default = Blank. This value is provided by the SIP ITSP. If a password is specified, the matching **Authentication Name** must also be set.
Expiry	Default = 60 minutes. This setting defines how often registration with the SIP ITSP is required following any previous registration.
Registration Required	Default = On. I If selected, the fields above above are used for registration when making calls. If exported or imported as part of a trunk template, this setting is not supported by Basic Edition Quick mode systems.

Related Links

SIP Line on page 336

Line | SIP Advanced

These settings are mergable, with the exception of the **Media Connection Preservation** setting. Changing the **Media Connection Preservation** setting requires a “merge with service disruption”. When the configuration file is sent to the system, the SIP trunk is restarted and all calls on the line are dropped.

Deleting a SIP line requires a “merge with service disruption”.

Field	Description
Addressing	
Association Method	Default = By Source IP Address. This setting sets the method by which a SIP line is associated with an incoming SIP request. The match criteria used for each line can be varied. The search for a line match for an incoming request is done against each line in turn using each lines Association Method. The order of line matching uses the configured **Line Number** settings until a match occurs. If no match occurs the request is ignored. This method allows multiple SIP lines with the same address settings. This may be necessary for scenarios where it may be required to support multiple SIP lines to the same ITSP. For example when the same ITSP supports different call plans on separate lines or where all outgoing SIP lines are routed from the system via an additional on-site system. The options are: • **By Source IP Address**: This option uses the source IP address and port of the incoming request for association. The match is against the configured remote end of the SIP line, using either an IP address/port or the resolution of a fully qualified domain name. • **"From" header hostpart against ITSP domain**: This option uses the host part of the From header in the incoming SIP request for association. The match is against the **ITSP Domain Name** above. • **R-URI hostpart against ITSP domain**: This option uses the host part of the Request-URI header in the incoming SIP request for association. The match is against the **ITSP Domain Name** above. • **"To" header hostpart against ITSP domain**: This option uses the host part of the To header in the incoming SIP request for association. The match is against the **ITSP Domain Name** above. • **"From" header hostpart against DNS-resolved ITSP domain**: This option uses the host part of the FROM header in the incoming SIP request for association. The match is found by comparing the FROM header against a list of IP addresses resulting from resolution of the **ITSP Domain Name** above or, if set, the **ITSP Proxy Address** on the **Transport** tab. • **"Via" header hostpart against DNS-resolved ITSP domain**: This option uses the host part of the VIA header in the incoming SIP request for association. The match is found by comparing the VIA header against a list of IP addresses resulting from resolution of the **ITSP Domain Name** above or, if set, the **ITSP Proxy Address** on the **Transport** tab. • **"From" header hostpart against ITSP proxy**: This option uses the host part of the “From” header in the incoming SIP request for association. The match is against the **ITSP Proxy Address** on the **Transport** tab. • **"To" header hostpart against ITSP proxy**: This option uses the host part of the From header in the incoming SIP request for association. The match is against the **ITSP Proxy Address** on the **Transport** tab.

Table continues…

Field	Description
	• **R-URI hostpart against ITSP proxy**: This option uses the host part of the Request-URI in the incoming SIP request for association. The match is against the **ITSP Proxy Address** on the **Transport** tab.
Call Routing Method	Default = Request URI. This field allows selection of which incoming SIP information should be used for incoming number matching by the system's incoming call routes. The options are to match either the **Request URI** or the **To Header** element provided with the incoming call.
Suppress DNS SRV Lookups	Default = Off. Controls whether to send SRV queries for this endpoint, or just NAPTR and A record queries.
Identity	
Use Phone Context	Default = Off. When set to On, signals SIP enabled PBXs that the call routing identifier is a telephone number.
Add user=phone	Default = Off. This setting is available when **Use Phone Context** is set to On.
Use + for International	Default = Off. When set to On, outgoing international calls use E.164/International format with a '+' followed by the country code and then the directory number.
Use PAI for Privacy	Default = Off. When set to On, if the caller ID is withheld, the SIP message From: header is made anonymous, and the caller's identity, for admission control, billing, and emergency services, is inserted into the P-Asserted-Identity header. This mechanism should only be used in a trusted network and must be stripped out of the SIP message before it is forwarded outside the trusted domain.
Use Domain for PAI	Default = Off. When set to Off, the DNS resolved IP address of the ITSP Proxy is used for the host part in the P-Asserted-Identity header. When set to On, the the Domain for PAI is used.
Swap From and PAI	Default = Off. When set to on, swaps the values in the From: and P-Asserted-Identity headers, as required by some networks.
Caller ID from From Header	Default = Off. Incoming calls can include caller ID information in both the From field and in the PAI fields. When this option is selected, the caller ID information in the From field is used rather than that in the PAI fields.
Send From In Clear	Default = Off.

Table continues…

Field	Description
	When selected, the user ID of the caller is included in the From field. This applies even if the caller has selected to be or is configured to be anonymous, though their anonymous state is honored in other fields used to display the caller identity.
Cache Auth Credentials	Default = On. When set to On, allows the credentials challenge and response from a registration transaction to be automatically inserted into later SIP messages without waiting for a subsequent challenge.
User-Agent and Server Headers	Default = Blank (Use system type and software level). The value set in this field is used as the User-Agent and Server value included in SIP request headers made by this line. If the field is blank, the type of IP Office system and its software level used. Setting a unique value can be useful in call diagnostics when the system has multiple SIP trunks.
Media	
Allow Empty INVITE	Default = Off. When set to On, allows 3pcc devices to initiate calls to IP Office by sending an INVITE without SDP.
Send Empty re-INVITE	Default = Off. This option is only available if **Re-Invite Supported** is selected on the VoIP tab. If set to On, when connecting a call between two endpoints, IP Office sends an INVITE without SDP in order to solicit the full media capabilities of both parties.
Allow To Tag Change	Default = Off. When set to On, allows the IP Office to change media parameters when connecting a call to a different party than that which was advertised in the media parameters of provisional responses, such as 183 Session Progress.
P-Early-Media Support	Default = None. When set to on, allows the service provider and IP Office to supply several early media responses, but indicate which should be used to supply media to the endpoint before the call is answered.
Send SilenceSupp=off	Default = Off. Used for the G711 codec. When checked, the silence suppression off attribute is sent in SDP on this trunk.
Force Early Direct Media	Default = Off. When set to On, allows the direct connection of early media streams to IP endpoints rather than anchoring it at the IP office.
Media Connection Preservation	Default = Disabled. When enabled, allows established calls to continue despite brief network failures. Call handling features are no longer available when a call is in a preserved state. Preservation on public SIP trunks is not supported until tested with a specific service provider.

Table continues…

Field	Description
Call Control	
Call Initiation Timeout (s)	Default = 4 seconds. Range = 1 to 99 seconds. Sets how long the system should wait for a response to its attempt to initiate a call before following the alternate routes set in an ARS form.
Call Queuing Timeout (m)	Default = 5 minutes. For incoming calls, how many minutes to wait before dropping a call that has been queued waiting for a free VCM resource, or has remained in the unanswered state. For an outgoing calls, how many minutes to wait for the call to be answered after receiving a provisional response.
Service Busy Response	Default = 486 - Busy Here (503 - Service Unavailable for the France2 locale). For calls that result in a busy response from IP Office, this setting determines the response code. The options are: • **486 - Busy Here** • **503 - Service Unavailable**
on No User Responding Send	Default = 408-Request Timeout. Specifies whether to send a SIP response 408-Request Timeout or 480 Temporarily Unavailable.
Action on CAC Location Limit	Default = Allow Voicemail When set to **Allow Voicemail**, the call is allowed to go to a user's voicemail when the user's location call limit has been reached. When set to **Reject Call**, the call is rejected with the failure response code configured in the **Service Busy Response** field.
Suppress Q.850 Reason Header	Default = Off. When SIP calls are released by sending BYE and CANCEL, a release reason header is added to the message.
Emulate NOTIFY for REFER	Default = Off. Use for SIP providers that do not send NOTIFY messages. During transfers, if the trunk is waiting for NOTIFY messages due to sending a REFER, and a BYE message is received on that call leg, the trunk will emulate a NOTIFY message with status 200 OK and pass it to the other end.
No REFER if using Diversion	Default = Off. When enabled, REFER is not sent on the trunk if the forwarding was done with 'Send Caller ID = Diversion Header'. Applies to Forwards and Twinning.

Related Links

SIP Line on page 336

Line | SIP Engineering

This page is used to enter values that apply special features to the SIP line. These are entered using the **Add**, **Edit** and **Remove** buttons.

These settings are mergeable. Deleting a SIP line requires a “merge with service disruption”.

Related Links

SIP Line on page 336

Line | SIP DECT Line

A SIP DECT line can be manually added. SIP DECT lines are used to manage D100 Base Station operation.

Related Links

Line on page 272
Line | SIP DECT Base on page 365
Line | SIP DECT VoIP on page 366

Line | SIP DECT Base

Currently, IP Office supports four D100 Base Stations.

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

Field	Description
Line Number	Default = Blank. A unique line number associated with the SIP DECT Base Station. **Associated Extensions** are other extensions that can log into the base station.
Base Name	Default = Blank. Maximum 16 characters. A name assigned to the base station. Each base station provisioned on the IP Office must have a unique name. The field cannot be blank. The format is an alphanumeric string with no special characters.
Base MAC Address	Default = Blank. The MAC Address of the base station. If only one base station is provisioned, the field can remain at the default value. If multiple base stations are provisioned, the MAC address for each base station must be entered.
Configure Base IP	
Configure Base IP	Default = Off. Set to **On** to configure IP address attributes for the base station. When enabled, the Configure Base IP settings are displayed.
DHCP Client	Default = On. When enabled, specifies that the base station operates as a DHCP client. When enabled, not other IP address attributes can be configured.

Table continues…

Field	Description
IP Address	Default = Blank. The IP address of the base station. The IP address must be on the same subnet as one of the LAN interfaces.
IP Mask	Default = Blank. IP address mask.
IP Gateway	Default = Blank. The default gateway address
Provisioning Server	Default = IP Office interface address. The server address from where the Base Station configuration files can be retrieved.
Description	Default = Blank. Maximum 31 characters. Use this field to enter a description of this configuration.

Related Links

Line | SIP DECT Line on page 365

Line | SIP DECT VoIP

This form is used to configure the VoIP setting applied to calls on the SIP DECT line.

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

Field	Description
IP Address	Default = Blank. The IP address of the SIP DECT extension.
Codec Selection	Default = Custom This field defines the codec or codecs offered during call setup. The codecs available to be used are set through the **System Codec** list (**System | System Codec**). The Custom option allows specific configuration of the codec preferences to be different from the system **Default Selection** list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs. The D100 Base Station supports only G711 codecs.
TDM | IP Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the system TDM interface to the IP connection. This field is not shown on Linux based platforms.
IP | TDM Gain	Default = Default (0dB). Range = -31dB to +31dB. Allows adjustment of the gain on audio from the IP connection to the system TDM interface. This field is not shown on Linux based platforms.
DTMF Support	Default =RFC2833 The D100 Base Station supports only RFC2833.

Table continues…

Field	Description
VoIP Silence Suppression	Default = Off When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.
Local Hold Music	Default = Off
Allow Direct Media Path	Default = On This settings controls whether IP calls must be routed via the system or can be routed alternately if possible within the network structure. • If enabled, IP calls can take routes other than through the system. This removes the need for a voice compression channel. Both ends of the calls must support Direct Media and be using the same protocol (H.323 or SIP). Enabling this option may cause some vendors problems with changing the media path mid call. • If disabled or not supported at on one end of the call, the call is routed via the system. RTP relay support allows calls between devices using the same audio codec to not require a voice compression channel.
RE-Invite Supported	Default = Off. When enabled, Re-Invite can be used during a session to change the characteristics of the session. For example when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk. Requires the ITSP to also support **Re-Invite**.

Related Links

Line | SIP DECT Line on page 365

Line | SM Line

This type of line is used to create a SIP connection between an IP Office and an Avaya Aura® Session Manager. The other end of the SIP connection must be configured on the Session Manager as a SIP Entity Link.

An SM Line can only be added to IP Office system Standard Mode or Server Edition configurations. It is typically used in IP Office Standard mode in Enterprise Branch deployments connected to the Avaya Aura® network. For more details about IP Office Enterprise Branch deployments refer to Deploying IP Office in an Avaya Aura® Branch Environment (18–603853).

An SM Line can also be used in IP Office Server Edition to connect to an Avaya Aura® Session Manager. Through the SM Line, IP Office Server Edition supports interoperability with Avaya Aura® Session Manager. It also supports interoperability, via the Avaya Aura® Session Manager, with Avaya Aura® Communication Manager systems and with CS 1000 systems. Note that IP Office Server Edition is not used as an enterprise branch product and does not support some of the IP Office enterprise branch functionality, such as management by Avaya Aura® System Manager, WebLM licensing, Centralized Users or voicemail over the SM Line.

If the Avaya Aura® network has multiple Avaya Aura® Session Managers to provide redundancy, two SM lines can be added, one configured for each Avaya Aura® Session Manager.

Related Links

Line on page 272
Line | Session Manager on page 368
Line | SM Line VoIP on page 370
SM Line T38 Fax on page 372

Line | Session Manager

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

Field	Description
Line Number	Default = Automatically assigned. This value is automatically assigned by the Enterprise Branch and should be unique for each line added to the configuration. • **Session Manager line prioritization**: Up to two Session Manager lines can be configured. The two Session Manager lines are prioritized based on the line number. The lower line number is considered the primary Session Manager line. For example, if the first Session Manager line is configured as line number 17 and the second Session Manager line is configured as line 18, then line number 17 is considered the primary Session Manager line. If you want to designate the second Session Manager line (line 18 in this example) as the primary Session Manager line, you must change one or both of the line numbers so that the second Session Manager line is configured with a lower number than the current primary line. • **Session Manager line redundancy**: Based on the priority of the Session Manager lines designated by the line number, the active line to which theIP Office> sends all calls will always be the highest priority Session Manager line in service. That is, if the primary Session Manager line is in service, it will be the active line for sending calls. If the connection to the primary Session Manager line is lost, causing the IP Office to switch to the secondary Session Manager line, then when the primary line comes back up later, the IP Office reverts back to the primary Session Manager line.
In Service	Default = Enabled This option can be used to administratively disable the SM Line. It does not reflect the dynamic state of the line. If an SM Line is administratively disabled it is not equivalent to being in the dynamic out of service state.
SM Domain Name	This should match a SIP domain defined in the Session Manager system's SIP Domains table. Unless there are reasons to do otherwise, all the Enterprise Branch systems in the Avaya Aura® network can share the same domain.
SM Address	Enter the IP address of the Session Manager the line should use in the Avaya Aura network. The same Session Manager should be used for the matching **Entity Link** record in the Avaya Aura® configuration.

Table continues…

Field	Description
Outgoing Group ID	Default = 98888 This value is not changeable. However note the value as it is used in Enterprise Branch short codes used to route calls to the Session Manager.
Prefix	Default = Blank This prefix will be added to any source number received with incoming calls.
Max Calls	Default = 10 Sets the number of simultaneous calls allowed between the Enterprise Branch and Session Manager using this connection. Each call will use one of the available licenses that are shared by all SIP trunks configured in the system. **Note:** You must configure the **Maximum SIP Sessions** setting on the **System | Telephony | Telephony** page.
Network Type	Default = Public. This option is available if **Restrict Network Interconnect** (**System | Telephony | Telephony**) is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Include location specific information	Default = Off. Enabled when **Network Type** is set to **Private**. Set to **On** if the PBX on the other end of the trunk is toll compliant.
URI Type	Default = SIP. When **SIP** or **SIPS** is selected in the drop-down box, the SIP URI format is used (for example, name@example.com). This affects the **From** field of outgoing calls. The **To** field for outgoing calls will always use the format specified by the short codes used for outgoing call routing. Recommendation: When SIP Secured URI is required, the URI Type should be set to **SIPS**. **SIPS** can be used only when Layer 4 Protocol is set to TLS.
Media Connection Preservation	Default = Enabled. When enabled, attempts to maintain established calls despite brief network failures. Call handling features are no longer available when a call is in a preserved state. When enabled, Media Connection Preservation applies to Avaya H.323 phones that support connection preservation.
Network Configuration TLS connections support the following ciphers: • TLS_RSA_WITH_AES_128_CBC_SHA	

Table continues…

Field	Description
• TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA	
Layer 4 Protocol	Default = TLS.
Send Port	When Network Configuration is set to TLS, the default setting is 5061. When Network Configuration is set to TCP, the default setting is 5060.
Listen Port	When Network Configuration is set to TLS, the default setting is 5061. When Network Configuration is set to TCP, the default setting is 5060.
Session Timer	Default = 1200. Range = 90 to 64800 This field specifies the session expiry time. At the half way point of the expiry time, a session refresh message is sent. Setting the field to **On Demand** disables the session timer. Communication Manager supports SIP session refresh via UPDATE in Communicaton Manger release 6.2 SP1 and later. If using an earlier release of Communication Manager, then the **Session Timer** parameter must be set to **On Demand**.
Description	Default = Blank. Maximum 31 characters. Use this field to enter a description of this configuration.

Related Links

Line | SM Line on page 367

Line | SM Line VoIP

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

Field	Description
Codec Selection	Default = System Default This field defines the codec or codecs offered during call setup. The available codecs in default preference order are: • **G.711 A-Law** • **G.711 U-LAW** • **G.729** • **G.723.1** Note that the default order for G.711 codecs will vary to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition, it is supported on Primary Server, Secondary Server and Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo.

Table continues…

Field	Description
	The codecs available in this form 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 matches the codecs set in the system wide list. • **Custom** This option allows specific configuration of the codec preferences to be different from the system list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.
Fax Transport Support	Default = 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.
Location	Default = Cloud. Specify a location to associate the extension with a physical location. Associating an extension with a location: • Allows emergency services to identify the source of an emergency call. • Allows you to configure call access control settings for the location. The drop down list contains all locations that have been defined in the **Location** form.
Call Initiation Timeout	Default = 4 seconds. Range = 1 to 99 seconds. This option sets how long the system should wait for a response to its attempt to initiate a call before following the alternate routes set in an ARS form.
DTMF Support	Default = RFC2833. This setting is used to select the method by which DTMF key presses are signalled to the remote end. The options are: • **In Band**

Table continues…

Field	Description
	• **RFC2833** • **Info**
VoIP Silence Suppression	Default = Off. When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.
Allow Direct Media Path	Default = On This settings controls whether IP calls must be routed via the system or can be routed 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 support the codec originally negotiated on the trunk. Requires the ITSP to also support **Re-Invite**.
Codec Lockdown	Default = Off. Supports RFC 3264 Section 10.2 when **RE-Invite Supported** is enabled. In response to a SIP offer with a list of codecs supported, some SIP user agents supply a SDP answer that also lists multiple codecs. This means that the user agent may switch to any of those codecs during the session without further negotiation. The system does not support multiple concurrent codecs for a session, so loss of speech path will occur if the codec is changed during the session. If codec lockdown is enabled, when the system receives an SDP answer with more than one codec from the list of offered codecs, it sends an extra re-INVITE using just a single codec from the list and resubmits a new SDP offer with just the single chosen codec.
Force direct media with phones	Default = Off.
G.711 Fax ECAN	Default = Off.

Related Links

Line | SM Line on page 367

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

Table continues…

Field	Description
TFOP Enhancement	Default = On.
Disable T30 ECM	Default = Off. When selected, disabled the T.30 Error Correction Mode used for fax transmission.
Disable EFlags For First DIS	Default = Off.
Disable T30 MR Compression	Default = Off.
NSF Override	Default = Off. If selected, the NSF (Non-Standard Facility) information sent by the T38 device can be overridden using the values in the fields below. **Country Code**: Default = 0. **Vendor Code**: Default = 0.

Related Links

Line | SM Line on page 367

Line | IP Office Line

This line type is used to connect two IP Office systems.

In previous releases, connecting two IP Office systems was achieved using H.323 Lines configured with **Supplementary Services** set to **IP Office SCN**. In the current release, the IP Office line type is used to connect IP Office systems. Separating out the IP Office line type from the H.323 line type allows for the logical grouping of features and functions available when connecting two IP Office systems, including IP Office systems connected through the cloud.

Note:

Setting an IP Office line with **Transport Type** = **Proprietary** and **Networking Level** = **SCN** will interwork with a previous release system configured with an H.323 SCN line.

Related Links

Line on page 272
Line | IP Office Line on page 374
Line | IP Office Line Short Codes on page 378
Line | IP Office Line VoIP on page 379

Line | IP Office Line

Field	Description
Line Number	Default = 0. Range = 1 to 349.

Table continues…

Field	Description
	Enter the line number that you wish. Note that this must be unique.
Transport Type	Default = Proprietary. The options are • **Proprietary**: The default connection type when connecting two IP Office systems in an SCN or Server Edition network. • **WebSocket Client / Websocket Server**: A WebSocket connection is an HTTP / HTTPS initiated TCP pipe through which Call signalling and Network Signaling is tunneled. This transport type is used to connect IP Office systems through the cloud. Selecting one of the WebSocket options enables the **Security** field and the **Password** fields.
Networking Level	Default = SCN. The options are • **None**: No supplementary services are supported. • **SCN**: This option is used to link IP Office system within a multi-site network. The systems within a multi-site network automatically exchange information about users and extensions, allowing remote users to be called without any additional configuration on the local system.
Security	Default = Unsecured. The Security field is available when **Transport Type** is set to **WebSocket Client** or **WebSocket Server**. The options are • **Unsecured** : The connection uses HTTP/TCP. • **Medium**: The connection uses HTTPS/TLS. • **High**: The connection uses HTTPS/TLS. The server certificate store must contain the client identity certificate.
Network Type	Default = Public. This option is available if **Restrict Network Interconnect** (**System | Telephony | Telephony**) is enabled. It allows the trunk to be set as either **Public** or **Private**. The system will return number busy indication to any attempt to connect a call on a **Private** trunk to a **Public** trunk or vice versa. This restriction includes transfers, forwarding and conference calls. Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.
Include location specific information	Default = Off. Enabled when **Network Type** is set to **Private**. Set to **On** if the PBX on the other end of the trunk is toll compliant.
Telephone Number	Default = Blank.

Table continues…

Field	Description
	Used to remember the telephone number of this line. For information only.
Prefix	Default = Blank. The prefix is used in the following ways: • **For incoming calls** The ISDN messaging tags indicates the call type (National, International or Unknown). If the call type is unknown, then the number in the Prefix field is added to the ICLID. • **For outgoing calls** The prefix is not stripped, therefore any prefixes not suitable for external line presentation should be stripped using short codes.
Outgoing Group ID	Default = 1. Range 0 to 99999. Short codes that specify a number to dial also specify the line group to be used. The system will then seize a line with a matching Outgoing Group ID. The same ID can be used for multiple lines. In a Server Edition network, the **Outgoing Group ID** used on a system must also be unique within the network, ie. the same ID cannot be used in the configuration of any lines on another server system in the network. The IDs 99999 and 99998 which are reserved for the H.323 lines to the Primary Server and Secondary Server respectively. The IDs 999901 to 99930 are reserved for the H.323 lines from the Primary Server to each expansion system in the network. The ID 0 cannot be used in a Server Edition network.
Number of Channels	Default = 20, Range 0 to 250. Defines the number of operational channels that are available on this line.
Outgoing Channels	Default = 20, Range 0 to 250. This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as Number of Channels field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls.
Gateway	
Address	Default = Blank. Enter the IP address of the gateway device at the remote end. This address must not be shared by any other IP line (H.323, SIP, SES or IP DECT).
Location	Default = Cloud. Specify a location to associate the extension with a physical location. Associating an extension with a location: • Allows emergency services to identify the source of an emergency call. • Allows you to configure call access control settings for the location. The drop down list contains all locations that have been defined in the **Location** form.
Password **Confirm Password**	Default = Blank. The **Password** field is enabled when **Transport Type** is set to **WebSocket Server** or **WebSocket Client**.

Table continues…

Field	Description
	WebSockets are bi-directional HTTP or HTTPS communication pipes initiated from a client to a server. They permit clients behind local a firewall to traverse the internet to a server by using well known ports and protocols. A matching password must be set at each end of the line.
Port	When **Transport Type** is set to **Proprietary**, the default port is 1720 and cannot be changed. When **Transport Type** is set to **WebSocket Client**, the default port is 80. The **Port** field is not available when **Transport Type** is set to **WebSocket Server**. The HTTP and HTTPS receive ports are defined at the system level in the security settings **System Details** tab.
SCN Backup Options These options are only available when the **Networking Level** option is set to **SCN**. The intention of this feature is to attempt to maintain a minimal level of operation while problems with the local system are resolved.	
Supports Fallback	Default = Off. The Supports Fallback fields are available when **Networking Level** is set to **SCN**. When enabled, all three backup options are set to **On**.
Backs up my IP Phones	Default = Off. This option is used for Avaya 1600, 4600, 5600 and 9600 Series phones registered with the system. When selected, it will share information about the registered phones and users on those phones with the other system. If the local system is no longer visible to the phones, the phones will reregister with the other system. The users who were currently on those phones will appear on the other system as if they had hot desked. Note that when the local system is restored to the network, the phones will not automatically re-register with it. A phone reset via either a phone power cycle or using the System Status Application is required. When phones have registered with the other system, they will show an **R** on their display. If using resilience backup to support Avaya IP phones, **Auto-create Extn** and **Auto-create User** should not be left enabled after initial configuration or any subsequent addition of new extensions and users. Leaving auto-create options enabled on a system that is a failover target may cause duplicate extension/user records on the multi-site network under multiple failure scenarios.
Backs up my Hunt Groups	Default = Off. When selected, any hunt groups the local system is advertising to the network are advertised from the other system when fallback is required. The trigger for this occurring is Avaya H.323 phones registered with the local system registering with the other system, ie. **Backs up my IP Phones** above must also be enabled. In a Server Edition network this option is only available on the H.323 trunk from the Primary Server to the Secondary Server. When used, the only hunt group members that will be available are as follows: • If the group was a distributed hunt group, those members who were remote members on other systems still visible within the network.

Table continues…

Field	Description
	• Any local members who have hot desked to another system still visible within the network. When the local system becomes visible to the other system again, the groups will return to be advertised from the local system.
Backs up my Voicemail	Default = Off. This option can be used if the local system is hosting the Voicemail Pro server being used by the network. If selected, when the local system is no longer visible to the voicemail server, the other system will act as host for the voicemail server. In a Server Edition network this option is only available on the H.323 trunk from the Primary Server to the Secondary Server. It is assumed as being on an is automatically set by the Resilience Administration tool. The option: • requires the other system to have licenses for the Voicemail Pro features that are required to operate during any fallback period. • requires Voicemail Pro 5.0+.
Backs up my IP DECT Phones	Default = Off. This option is only available when **Transport Type** is set to **Proprietary**. This option is used for Avaya IP DECT phones registered with the system. When selected, it will share information about the registered phones and users on those phones with the other system. If the local system is no longer visible to the phones, the phones will reregister with the other system. The users who were currently on those phones will appear on the other system as if they had hot desked. Note that when the local system is restored to the network, the phones will not automatically re-register with it. A phone reset via either a phone power cycle or using the System Status Application is required. When phones have registered with the other system, they will show an **R** on their display. **Note:** Only one IP Office Line can have this configuration parameter set to On.
Description	Default = Blank. Maximum 31 characters. Use this field to enter a description of this configuration.

Related Links

Line | IP Office Line on page 374

Line | IP Office Line Short Codes

Incoming calls on IP Office Lines are not routed using Incoming Call Route settings.

Short codes can be added and edited using the **Add**, **Remove** and **Edit** buttons. Alternatively you can right-click on the list of existing short code to add and edit short codes. These settings are not mergeable. Changes to these settings will require a reboot of the system.

Related Links

Line | IP Office Line on page 374

Line | IP Office Line VoIP

Field	Description
Code Selection	Default = System Default This field defines the codec or codecs offered during call setup. The available codecs in default preference order are: • **G.711 A-Law** • **G.711 U-LAW** • **G.729** • **G.723.1** Note that the default order for G.711 codecs will vary to match the system's default companding setting. **G.723.1** is not supported on Linux based systems. The **G.722 64K** codec is also supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 or IP500 Combo cards. For Server Edition, it is supported on Primary Server, Secondary Server and Expansion System (L) systems and on Expansion System (V2) systems fitted with IP500 VCM, IP500 VCM V2 or IP500 Combo. The codecs available in this form are set through the **System Codec** list (**System | System Codec**). The options are: • **System Default** This is the default setting. When selected, the codec list below matches the codecs set in the system wide list. • **Custom** This option allows specific configuration of the codec preferences to be different from the system list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.
Call Initiation Timeouts	Default = 4. Range = 1 to 99 seconds. This option sets how long the system should wait for a response to its attempt to initiate a call before following the alternate routes set in an ARS form.
Media Security	Default = Same as System. Secure RTP (SRTP) can be used between IP Offices to add additional security. These settings control whether SRTP is used for this line and the settings used for the SRTP. The options are: • **Same As System**: Use the same settings as the system setting configured on the **System | VoIP Security** tab. • **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.

Table continues…

Field	Description
	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.
Fax Transport Support	Default = Off This option is only supported on trunks with the **Networking Level** set to **SCN**. On IP Office Lines, fax relay is supported across multi-site network lines with **Fax Transport Support** selected. This will use 2 VCM channels in each of the systems. Fax relay is only supported on IP500 V2 systems with IP500 VCM, IP500 VCM V2 and or IP500 Combo cards. Fax relay is supported on Server Edition Linux servers.
Out Of Band DTMF	Default = On. Out of Band DTMF is set to on and cannot be changed.
Allow Direct Media Path	Default = On This settings controls whether IP calls must be routed via the system or can be routed 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.

Related Links

Line | IP Office Line on page 374

Control Unit | Control Unit

The **Control Unit** form gives details of the system and some devices connected to or within the system. This includes some modules within the control nit as well as external expansion modules.

For Server Edition systems, for the Primary Server, Secondary Server and Expansion System (L) it shows details for the physical server platform and details for the IP Office Media service being hosted on that server. For the Expansion System (V2) it shows details of the IP500 V2 control unit and the cards installed into the control unit.

The **New** and **Delete** actions on this form have special functions.

- **New** This action is used to added a WAN3 expansion module. If when a WAN3 is added to the system, the WAN3 is not recognized following a system reboot, New on this form can be used to scan for the WAN3 module.
- **Delete** This action can only be used with external expansion modules. This action can only be used with external expansion modules attached to a system. The action should used with caution as deleting a module will also delete any extensions or lines associated with the module being deleted. If the module is physically present, default records are automatically recreated following a reboot.

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

Field	Description
Device Number	This is automatically allocated by the system.
Unit Type	The name of the device.
Version	The version of software running on each unit.
Serial Number	This is the number the system uses to tie a physical Control Unit to a device configuration (device number). For the control unit this is the MAC address. For a device connected to an Expansion port, it is the Expansion port number plus 1.
Unit IP Address	This field shows the IP address for the LAN1.
Interconnect Number	For external expansion modules this is the control unit expansion port used for connection. For other devices this is 0.
Module Number	For external expansion modules this is the control unit expansion port used for connection. For internal devices in the control unit, **Control Unit** is displayed.

Table continues…

Field	Description
Operating Mode	This field is available when a DS16B or DS30B digital expansion module is selected as the control unit. Select the operating mode based on the type of telephones deployed. • **DS - 1400, 9500, 5400, 2400, T3, 4400 Series Phones** • **BST - T7000, M7000 Series Phones**

Related Links

Configuration Mode Field Descriptions on page 193

Extension

By default, each extension is normally associated with a user and uses that user's directory number and other setting. Users with a log in code can move between extensions by logging in and out, so the directory number is not a fixed property of the extension.

Non-IP Extensions

Physical extension ports are either integral to the control unit or added by the installation of an analog or digital phone expansion module. Extension records are automatically created for each physical extension port within the system. These ports cannot be added or deleted manually.For Server Edition, non-IP extensions are only supported on Expansion System (V2) units.

Standard Telephone

A standard extension.

Quiet Headset

Used for analog extension devices that are permanently off-hook.

:

IVR Port

Used for analog ports connected to devices that require a specific disconnect clear signal at the end of each call.

Paging Speaker

An analog extension port set to be used as a paging speaker connection.

FAX Machine

Indicates that the extension is connected to a FAX machine.

MOH Source

Indicates that the extension is being used as a music on hold source.

IP Extensions

These are used for IP phone devices and VoIP applications.

H.323 or SIP Extension

This icon indicates an IP extension. 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. Note that third-party IP phone devices require entry of an IP End-Points license.

IP DECT or 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

Configuration Mode Field Descriptions on page 193
Extension | Extn on page 383
Extension | Analog on page 386
Extension | VoIP on page 389
T38 Fax on page 400
Extension | IP DECT on page 401
Extension | SIP DECT Base on page 403

Extension | Extn

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.

Table continues…

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td></td><td colspan="2">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.

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.</td></tr>
<tr><td>Phone Password</td><td colspan="2">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.</td></tr>
<tr><td>Caller Display Type</td><td colspan="2">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.</td></tr>
<tr><td></td><td>Type</td><td>Description</td></tr>
<tr><td></td><td>Off</td><td>Disables caller display.</td></tr>
<tr><td></td><td>On</td><td>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.</td></tr>
<tr><td></td><td>UK</td><td>FSK before the first ring conforming to BT SIN 227. Name and number.</td></tr>
<tr><td></td><td>UK20</td><td>As per UK but with a maximum length of 20 characters. Name and number.</td></tr>
<tr><td></td><td>DTMFA</td><td>Caller ID in the DTMF pattern A<caller ID>C. Number only.</td></tr>
<tr><td></td><td>DTMFB</td><td>Caller ID in DTMF after call connection. Number only.</td></tr>
<tr><td></td><td>DTMFC</td><td>Caller ID in the DTMF pattern A<caller ID>#. Number only.</td></tr>
<tr><td></td><td>DTMFF</td><td>Sends the called number in DTMF after call connection. Number only. Used for fax servers. When calls are delivered via a hunt group it is recommended that hunt group queuing is not used. If hunt group queuing is being used, set the Queue Type to Assign Call on Agent Alert.</td></tr>
<tr><td></td><td>DTMFD</td><td>Caller ID in the DTMF pattern D<caller ID>C. Number only.</td></tr>
</table>

Table continues…

Field	Description	
	FSKA	Variant of UK used for BT Relate 1100 phones. Name and number.
	FSKB	ETSI specification with 0.25 second leading ring. Name and number.
	FSKC	ETSI specification with 1.2 second leading ring. Name and number.
	FSKD	Conforms to Belcore specification. Name and number.
Reset Volume after Calls	Default = Off. Resets the phone's handset volume after each call. This option is supported on Avaya 1400, 1600, 2400, 4400, 4600, 5400, 5600, 6400, 9500 and 9600 Series phones.	
Device Type	This field indicates, the last known type of phone connected to the extension port. • Analogue extension ports always report as **Analog Handset** since the presence or absence of actual analog phone cannot be detected. • Digital extension ports report the type of digital phone connected or **Unknown digital handset** if no phone is detected. • H.323 extensions report the type of IP phone registered or **Unknown H.323 handset** if no phone is currently registered as that extension. • SIP extensions report the type of SIP phone registered or **Unknown SIP device** if no SIP device is currently registered as that extension. 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	

Table continues…

Field	Description
	digital station (DS) port on the control unit. For an IP500 V2 control unit, **BD** and **BP** is also followed by the slot number. VoIP extensions report as **0**.
Port	This field indicates the port number on the **Module** indicated above. VoIP extensions report as **0**.
Disable Speakerphone	Default = Off (Speakerphone enabled). When selected, disables the fixed **SPEAKER** button if present on the phone using this extension port. Only supported on Avaya DS, TCM and H.323 IP phones. An audible beep is sounded when a disabled **SPEAKER** button is pressed. Incoming calls such as pages and intercom calls are still connected but the speech path is not audible until the user goes off-hook using the handset or headset. Similarly calls made or answered using other buttons on the phone are not audible unless the user goes off-hook using the handset or headset. Currently connected calls are not affected by changes to this setting.
Force Authorization	Default = On. This setting is used with SIP extension devices.

Related Links

Extension on page 382

Extension | Analog

This tab contains settings that are applicable to analog extensions. These extensions are provided by ports marked as **POT** or **PHONE** on control units and expansion modules.

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

Field	Description
Equipment Classification: Default = Standard Telephone. Only available for analog extension ports. Note that changes to this setting are mergeable.	
Quiet Headset	On extensions set to **Quiet Headset**, the audio path is disabled when the extension is idle. Ringing is presented in the audio path. Caller ID is not supported on the phone. This option can be used with analog extensions where the handset is replaced by a headset since in such a scenario audio is only desired when a call is connected. Since the audio path is disabled when idle, the **Quiet Headset** extension cannot dial digits to make calls. Therefore to make and answer calls this option is typically used with the user Offhook Station (User | Telephony | Call Settings) setting which allows the extension user to make and answer calls using applications.
Paging Speaker	Used for analog ports connected to a paging amplifier. This extension will present busy and cannot be called or be used to make calls. It can only be accessed using Dial Paging features.

Table continues…

Field	Description
	When using a UPAM connected to an analog extension port, the extension's Equipment Classification (Extension | Analog) should be set to **IVR Port** and not **Paging Speaker**.
Standard Telephone	Use for normal analog phones.
Door Phone 1/Door Phone 2	These two options are currently not used and so are grayed out.
IVR Port	Used for analog ports connected to devices that require a disconnect clear signal (ie. a break in the loop current) at the end of each call. When selected the **Disconnect Pulse Width** is used.
FAX Machine	If fax Relay is being used, this setting should be selected on any analog extension connected to an analog fax machine. This setting can also be used with SIP trunks.
MOH Source	If selected, the port can be used as a music on hold source in the Tones and Music settings. An extension set as a music on hold source cannot make or receive calls. The audio input can be monitored through the extension music on hold controls. A suitable interface device is required to provide the audio input to the extension port. It must look to the system like an off-hook analog phone. For example a transformer with a 600 Ohm winding (such as a Bogen WMT1A) or a dedicated MoH device with a 600Ohm output designed for connection to a PBX extension port which is providing loop current can be used.
Flash Hook Pulse Width The following options are only available for analog extension ports. They define the length of loop break that will be considered a time break recall (TBR) signal.	
Use System Defaults	Default = Selected (On) Use the default values appropriate to the system's locale.
Minimum Width	Range = 0 to 2540 milliseconds. Minimum hook flash length used if **Use System Defaults** is not selected. Shorter breaks are ignored a glitches.
Maximum Width	Range = 0 to 2550 milliseconds. Maximum hook flash length used if **Use System Defaults** is not selected. Longer breaks are treated as clearing.
Disconnect Pulse Width	Default = 0ms. Range = 0 to 2550ms This setting is used with analog extensions where the **Equipment Classification** above has been set to **IVR Port**. It sets the length of loop current break used to indicate call clearing.
Message Waiting Lamp Indication Type	Default = None Allows the selection of the message waiting indication (MWI) mode for analog and IP DECT extensions. For control unit and Phone V1 module analog extensions, the options are: • **101V** • **51V Stepped**

Table continues…

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td></td><td colspan="2">• 81V
• Bellcore FSK
• Line Reversal A
• Line Reversal B
• None
• On
For Phone V2 external module extensions and IP500 Phone base cards, the additional option 101V is available.
For IP500 V2 systems, if the option Restrict Analog Extension Ringer Voltage is selected (System | Telephony | Telephony), the MWI options are restricted to:
• Line Reversal A
• Line Reversal B
• None
Any extensions set to another option are forced to Line Reversal A.
On defaults the message waiting indication as follows using the system locale.</td></tr>
<tr><td></td><td>Locale</td><td>'On' =</td></tr>
<tr><td></td><td>Argentina, Australia, Brazil, Canada, Chile, China, Colombia, Japan, Korea, Mexico, New Zealand, Peru, Russia, Saudi Arabia, South Africa, Spain, United States, Venezuela</td><td>51V Stepped</td></tr>
<tr><td></td><td>Bahrain, Belgium, Denmark, Egypt, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, Italy, India, Kuwait, Morocco, Netherlands, Norway, Oman, Pakistan, Poland, Portugal, Qatar, Singapore, Sweden, Switzerland, Taiwan, Turkey, United Arab Emirates, United Kingdom</td><td>On = 101V on Phone V2 modules and IP500 Phone cards, otherwise 81V.</td></tr>
<tr><td>Hook Persistency:</td><td colspan="2">Default = 100ms. Range = 50 to 255ms.
Defines the time frame (in milliseconds) in which the system will wait before determining that the phone is off-hook.</td></tr>
</table>

Related Links

Extension on page 382

Extension | VoIP

This tab is only available for H.323 and SIP extensions. The settings available will vary depending on the extension type.

Related Links

Extension on page 382
H.323 Extension VoIP on page 389
SIP Extension VoIP on page 394

H.323 Extension VoIP

These settings have changed in release 9.1. View the 9.0 settings on page 392.

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 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.

Table continues…

Field	Description
	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). • **Authentication**: Default = RTP and RTCP This setting allows selection of which parts of the media session should be protected using authentication. • **Replay Protection SRTP Window Size**: Default = 64. Currently not adjustable. • **Crypto Suites**: Default = SRTP_AES_CM_128_SHA1_80. There is also the option to select SRTP_AES_CM_128_SHA1_32.

Table continues…

Field	Description
VoIP Silence Suppression	Default = Off When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods. This feature is not used on IP lines using **G.711** between systems. On trunk's between networked systems, the same setting should be set at both ends.
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 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**

Table continues…

Field	Description
	• **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

Extension | VoIP on page 389
H.323 Extension VoIP (9.0) on page 392

H.323 Extension VoIP (9.0)

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 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).

Table continues…

Field	Description
	• **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.
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

Table continues…

Field	Description
	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 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

H.323 Extension VoIP on page 389

SIP Extension VoIP

These settings have changed in release 9.1. View the 9.0 settings on page 398.

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.

Table continues…

Field	Description
	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.
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.

Table continues…

Field	Description
	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. • **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

Table continues…

Field	Description
	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 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

Extension | VoIP on page 389
Extension SIP VoIP (9.0) on page 398

Extension SIP VoIP (9.0)

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. It is not supported on any systems that include any IP400 VCM cards. The codecs available to be used are set through the **System Codec** list (System | System Codec). The options are: • **System Default**: This is the default setting. When selected, the codec list below show matches the codecs set in the system wide **Default Selection** list (System | Codecs). • **Custom**: This option allows specific configuration of the codec preferences to be different from the system **Default Selection** list. When **Custom** is selected, the list can be used to select which codecs are in the **Unused** list and in the **Selected** list and to change the order of the selected codecs.
Fax Transport Support:	Default = Off. This option is only available if **Re-Invite Supported** is selected. When enabled, the system performs fax tone detection on calls routed via the line and, if fax tone is detected, renegotiates the call codec as configured below. The SIP line provider must support the selected fax method and Re-Invite. The system must have available VCM resources using an IP500 VCM, IP500 VCM V2 or IP500 Combo base card. For systems in a network, fax relay is supported for fax calls between the systems. The options are: • **None**: Select this option if fax is not supported by the line provider. • **G.711**: G.711 is used for the sending and receiving of faxes. • **T38**: T38 is used for the sending and receiving of faxes. • **T38 Fallback**: When you enable this option, T38 is used for sending and receiving faxes on a SIP line. If the called destination does not support T38, the system will

Table continues…

Field	Description
	send a re-invite to change the transport method to G.711. This option is not supported by 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**.
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 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

Table continues…

Field	Description
	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

SIP Extension VoIP on page 394

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

Table continues…

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

Related Links

Extension on page 382

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 not mergeable. Changes to these settings will require 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	
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

Extension on page 382

Extension | SIP DECT Base

This tab is displayed for SIP DECT extensions.

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

Field	Description
DECT Line ID	Use the drop-down list to select the SIP DECT Line from the system to the base station.

Related Links

Extension on page 382

User

Users are the people who use the system. They do not necessary have to be an extension user, for example users are used for RAS dial in data access. In addition, more users can be created than there are extensions, with users logging in to an extension when they want to receive calls.

By default, a user is automatically created to match each extension. They are numbered from 201 upwards and the first 16 are placed in the hunt group Main (200), which is the default destination for incoming calls.

 **Standard User:** A standard user.

 **Centralized User**: A centralized user.

 **No User**: Used to apply settings for extensions which currently have no associated user.

 **Remote Manager**: Used as the default settings for dial in user connections.

 **Hot Desking User:** Users with a Login Code can move between extensions by logging in and off.

When a User is Deleted?

When a user is deleted, any calls in progress continue until completed. The ownership of the call is shown as the NoUser user. Merging the deletion of a user causes all references to that deleted user to be removed from the system.

Changing a User's Extension

Changing a user's extension number automatically logs the user in on the matching base extension if available and the user doesn't have Forced Login enabled. If **Forced Login** is enabled, then the user remains on the current extension being used until they log out and log in at the new extension.

Note that changing a user's extension number affects the user's ability to collect Voicemail messages from their own extension. Each user's extension is set up as a "trusted location" under the Source Numbers tab of the User configuration form. This "trusted location" allows the user to dial *17 to collect Voicemail from his own extension. Therefore if the extension number is changed so must the "trusted location".

The following related configuration items are automatically updated when a user extension is changed:

- User, Coverage and Bridged Appearance buttons associated with the user.
- Hunt group membership (disabled membership state is maintained).
- Forwards and Follow Me's set to the user as the destination.
- Incoming call routes to this destination.
- Dial in source numbers for access to the user's own voicemail.
- Direct call pickup buttons are updated.
- The extension number of an associated extension is updated.

Server Edition User Management

In a Server Edition network, individual users are still added to the configuration of a particular server. Typically they are added to the configuration of the server that hosts the user's physical extension or supports their main place of work. That server is treated as the host system for the user. However, once a user is added to the configuration of a particular system, their settings can also be accessed and edited under the **Users** grouping at the top of the navigation pane of Manager.

Related Links

Configuration Mode Field Descriptions on page 193
User | User on page 405
User | Voicemail on page 411
User | DND on page 415
User | Short Codes on page 416
User | Source Numbers on page 417
User | Telephony on page 420
User | Forwarding on page 429
User | Dial In on page 432
User | Voice Recording on page 432
User | Button Programming on page 434
User | Menu Programming on page 434
User | Mobility on page 437
User | Hunt Group Memberships on page 440
User | Announcements on page 440

User | 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. 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

Table continues…

Field	Description
	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. 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

Table continues…

Field	Description
	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. • 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
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 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, remote workers are supported for users licensed and configured for the **Power User** user profile.
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.

System Type	Standard Mode	Server Edition

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, remote workers are supported for users licensed and configured for the **Power User** user profile. 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. 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.

Table continues…

Field	Description
	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**.
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).

Table continues…

Field	Description
	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

User on page 403

User | 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, 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. • **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).
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.

Table continues…

Field	Description
	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. • **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

Table continues…

Field	Description
	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**. 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.

Table continues…

Field	Description
	• **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

User on page 403

User | DND

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

User on page 403

User | 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

User on page 403

User | 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.
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**.
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/

Table continues…

Value	Description
	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 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

User on page 403

User | Telephony

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

Related Links

User on page 403
Call Settings on page 420
Supervisor Settings on page 422
Multi-line Options on page 426
Call Log on page 427
TUI on page 428

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.
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.

Table continues…

Field	Description
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.
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

Table continues…

Field	Description
	(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

User | Telephony on page 420

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.
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

Table continues…

Field	Description
	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. 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

Table continues…

Field	Description
	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 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

User | Telephony on page 420

Multi-line 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. The ring used for a call alerting on a call coverage or bridged appearance button will vary according to whether the user is currently connected to a call or not. • If not currently on a call, the **Coverage Ring** setting is used. • If currently on a call, the quieter of the **Coverage Ring** and **Attention Ring** settings is used.

Attention Ring Setting	**Coverage Ring Setting**		
	Ring	**Abbreviated**	**Off**
Ring	Ring	Abbreviated	Off
Abbreviated	Abbreviated	Abbreviated	Off

Attention Ring	Default = Abbreviated Ring. This field selects the type of ringing that should be used for calls alerting on appearance buttons when the user already has a connected call on one of their appearance buttons. **Ring** selects normal ringing. **Abbreviated Ring** selects a single

Table continues…

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

Related Links

User | Telephony on page 420

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). 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

User | Telephony on page 420

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

Table continues…

Field	Description
	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

User | Telephony on page 420

User | 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.
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

Table continues…

Field	Description
	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. 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

User on page 403

User | 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.
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

User on page 403

User | Voice 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. • **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

Table continues…

Field	Description
	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

User on page 403

User | 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.
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

User on page 403

User | Menu Programming

These menus control a range of options that are specific to different types of phones. The functions become accessible when the user logs in on the appropriate type of phone.

Related Links

User on page 403
T3 Telephony on page 435

Huntgroup on page 435
4400/6400 on page 436

T3 Telephony

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

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.

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

Field	Description
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.
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

User | Menu Programming on page 434

Huntgroup

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.

Field	Description
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

Table continues…

Field	Description
	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

User | Menu Programming on page 434

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.

Field	Description
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

User | Menu Programming on page 434

User | 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.

Table continues…

Field	Description
	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.
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.

Table continues…

Field	Description
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. - 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

User on page 403

User | Hunt Group Memberships

This tab displays the hunt group of which the user has been made a member. The tick boxes indicate whether the user's membership of each of those groups is currently enabled or disabled.

Related Links

User on page 403

User | 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 9999 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 9999 seconds. This setting sets the wait between the 1st and the 2nd announcement.
Repeat last announcement	Default = On. If selected, the last announcement played to the caller is repeated until they are answered or hang-up.
Wait before repeat	Default = 20 seconds. Range = 0 to 9999 seconds. If **Repeat last announcement** is selected, this setting sets is applied between each repeat of the last announcement.

Related Links

User on page 403

User | 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

User on page 403

User | 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

User on page 403

User | Web Self Administration

Use this page to enable self administration for users.

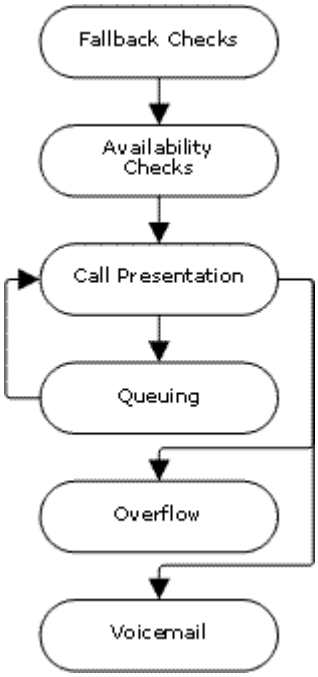
Field	Description
Self Adminstration	Default = Off. When enabled, users can log in to the <XYZ> interface. Configuration settings are grouped under the following categories. • **User** • **Voicemail** • **DND** • **Forwarding** • **Mobility** • **Personal Directory** • **Button Programming**
Visible	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

User on page 403

Group

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 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

Configuration Mode Field Descriptions on page 193

Group | Group on page 447

Group | Group

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 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

Table continues…

Field	Description
	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.
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).

Table continues…

Field	Description
	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 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).

Table continues…

Field	Description
	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 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.

Table continues…

Field	Description
	• 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

Group on page 445
User List Select Members window on page 451

User List Select Members window

The hunt group **Select Members** form is used to add and remove users from the hunt group. For hunt group's with a **Ring Mode** of **Sequential** or **Rotary** it is also used to set the order of use for the members of the hunt group.

The filters section at the top of the form can be used to filter the users shown. Note for hunt groups set as a **CCR Agent Group**, only users set as **CCR Agent** are shown.

The controls and data on the form vary depending on the hunt group's **Ring Mode** setting and on whether the system is in a multi-site network.

To sort either table, click on the column header that should be used for the sort the table. Sort changes the order of display only, it does not change the actual order of hunt group membership.

For **Sequential** and **Rotary** hunt groups, an **Order** column is shown. To change the order position of a hunt group member, select the member and then use the ↑ up and down ↓ arrow buttons.

During the actions below, the Shift and Ctrl keys can be used as normal to select multiple users. Note that the list of members has been sorted, the sort is updated after adding or moving members.

- **Add Before** Using the Shift and/or Ctrl keys, select the users you want to add and then on the right select the existing member that you want to add them before.
- **Add After** Using the Shift and/or Ctrl keys, select the users you want to add and then on the left select the existing member after which you want them added.
- **Append** Add the selected users on the left to the hunt group members on the right as the last member in the group order.
- **Remove** Remove the selected users on the right from the list of hunt group members.
- ↑ ↓ Move the selected member on the right up or down the membership order of the group.

Related Links

Group | Group on page 447

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 Limit	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

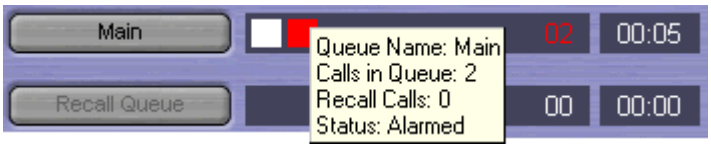
Table continues…

Field	Description
	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. 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

Table continues…

Field	Description
	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:
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

Group on page 445

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.

Table continues…

Field	Description
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. 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

Group on page 445

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**.

- **Fallback Group**: When in **Out of Service**, if an **Out of Service Fallback Group** has been set, calls are redirected to that group. When in **Night Service**, if a **Night Service Fallback Group** has been set, calls are redirected to that group.
- **Voicemail**: If no fallback group has been set but voicemail is enabled for the group, calls are redirected to voicemail.
- **Busy Tone**: If no fallback group 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.

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 time profile can be associated with the hunt group. When outside the time profile, the hunt group is automatically place 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
Time Profile	Default = <None> (No automatic night service)

Table continues…

Field	Description
	This field allows selection of a previously created Time Profile. That profile then specifies the times at which it should use the manually selected Service Mode settings. Outside the period defined in the time profile, the hunt group behaves as if set to Night Service mode. Note that when a hunt group is in Night Service due to it associated time profile, this is not reflected by the Service Mode on this tab. Note also that the manual controls for changing a hunt group's service mode cannot be used to take a hunt group out of time profile night service.
Night Service Destination	Default = <None> (Voicemail or Busy Tone) This field sets the alternate hunt group destination for calls when this hunt group is in Night Service mode. 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 hunt group destination for calls when this hunt group is in Out of Service mode. 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

Hunt Group Fallback				
Manager	Hunt group fallback selection is done through the **Group | Fallback** tab. A time profile if required is set through the **Time Profile | Time Profile** tab.			
Controls	The following short code features/button programming actions can be used: 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.			
	Feature/Action	**Short Code**	**Default**	**Button**
	Set Hunt Group Night Service	Yes	*20*N#	Yes — Toggles

Table continues…

Hunt Group Fallback				
	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	Ues
SoftConsole	There are no specific controls for the operation of hunt group fallback.			
Voicemail	There are no specific controls for the operation of hunt group fallback.			

Related Links

Group on page 445

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,

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.
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

Table continues…

Field	Description
	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. • **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

Table continues…

Field	Description
	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

Group on page 445

Group | Voice Recording

This tab is used to configure automatic recording of external calls handled by hunt group members. The recording of internal calls as well 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.

A destination mailbox other than the hunt group's own mailbox can be specified as the destination for recordings.

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

Field	Description
Record Inbound	Default = None Select whether automatic recording of incoming calls is enabled. The options are: • **None**: Do not automatically record calls. • **On**: Record the call if possible. If not possible to record, allow the call to continue. • **Mandatory**: Record the call if possible. If not possible to record, block the call and return busy tone.

Table continues…

Field	Description
	• **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.
Auto Record Calls	Default = External. This setting allows selection of whether **External** or **External & Internal** calls are subject to automatic call recording.

Related Links

Group on page 445

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 9999 seconds.

Table continues…

Field	Description
	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 9999 seconds. This setting sets the wait between the 1st and the 2nd announcement. If **Synchronize Calls** is selected, the actual wait may differ, see below.
Repeat last announcement	Default = On. If selected, the last announcement played to the caller is repeated until they are answered or hang-up.
Wait before repeat	Default = 20 seconds. Range = 0 to 9999 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.

Table continues…

Field	Description
	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

Group on page 445

Hunt Group | SIP

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

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

These settings 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

Group on page 445

Short Code

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

Warning:

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

These settings 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

Configuration Mode Field Descriptions on page 193

Service

Services are used to configure the settings required when a user or device on the LAN needs to connect to a off-switch data service such as the Internet or another network. Services can be used when making data connections via trunk or WAN interfaces.

Once a service is created, it can be used as the destination for an IP Route record. One service can also be set as the **Default Service**. That service will then be used for any data traffic received by the system for which no IP Route is specified.

The system supports the following types of service:

- **Normal Service** This type of service should be selected when for example, connecting to an ISP.
- **WAN Service** This type of service is used when creating a WAN link. A User and RAS Service will also be created with the same name. These three records are automatically linked and each open the same form. Note however, that this type of Service cannot be used if the Encrypted Password option is checked. In this case the RAS Service name must match the Account Name. Therefore either create each record manually or create an Intranet Service.
- **Intranet Service** This type of service can be selected to automatically create a User with the same name at the same time. These two records are linked and will each open the same form. The User's password is entered in the Incoming Password field at the bottom on the Service tab. An Intranet Services shares the same configuration tabs as those available to the WAN Service.
- **SSL VPN Service** 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.

For full details on how to configure and administer SSL VPN services, refer to the *Avaya IP Office SSL VPN Solutions Guide*.

Related Links

Configuration Mode Field Descriptions on page 193
Normal, WAN or Intranet Services on page 470
SSL VPN Service on page 478

Normal, WAN or Intranet Services

Related Links

Service on page 469
Service | Service on page 470
Service | Bandwidth on page 471
Service | IP on page 473
Service | Autoconnect on page 474
Service | Quota on page 474
Service | PPP on page 475
Service | Fallback on page 477
Service | Dial In on page 478

Service | Service

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
Service Name	The name of the service. It is recommended that only alphanumeric characters be used.
Account Name	The user name that is used to authenticate the connection. This is provided by the ISP or remote system.
Password	Default = Blank Enter the password that is used to authenticate the connection. This is provided by the ISP or remote system.
Telephone Number	Default = Blank If the connection is to be made via ISDN enter the telephone number to be dialed. This is provided by the ISP or remote system.
Firewall Profile	Default = Internet01 if present, otherwise <None> From the list box select the Firewall Profile that is used to allow/disallow protocols through this Service.
Encrypted Password	Default = Off When enabled the password is authenticated via CHAP (this must also be supported at the remote end). If disabled, PAP is used as the authentication method.
Default Route	Default = Off When enabled this Service is the default route for data packets unless a blank IP Route has been defined in the system IP Routes. A green arrow appears to the left of the Service in the Configuration Tree. Only one Service can be the default route. If disabled, a route must be created under IP Route.
Incoming Password	Default = Blank Shown on WAN and Intranet services. Enter the password that will be used to authenticate the connection from the remote Control Unit. (If this field has

Table continues…

Field	Description
	appeared because you have created a Service and User of the same name, this is the password you entered in the User's Password field).

Related Links

Normal, WAN or Intranet Services on page 470

Service | Bandwidth

These options give the ability to make ISDN calls between sites only when there is data to be sent or sufficient data to warrant an additional call. The calls are made automatically without the users being aware of when calls begin or end. Using ISDN it is possible to establish a data call and be passing data in less that a second.

Note:

The system will check **Minimum Call Time** first, then **Idle Period**, then the **Active Idle Period**.

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

Field	Description
Minimum No of Channels	Default = 1. Range = 1 to 30. Defines the number of channels used to connect for an outgoing connection. The initial channel must be established and stable, before further calls are made.
Maximum No of Channels	Default = 1. Range = 1 to 30. Defines the maximum number of channels to can be used. This field should contain a value equal to or greater than the Minimum Channels field.
Extra BW Threshold	Default = 50%. Range = 0 to 100%. Defines the utilization threshold at which extra channels are connected. The value entered is a %. The % utilization is calculated over the total number of channels in use at any time, which may be one, two etc. For example, if **Minimum Channels** set to 1, **Maximum Channels** set to 2 and **Extra Bandwidth** set to 50 - once 50% of first channel has been used the second channel is connected.
Reduce BW Threshold	Default = 10%. Range = 0 to 100%. Defines the utilization threshold at which additional channels are disconnected. The value entered is a %. Additional calls are only dropped when the % utilization, calculated over the total number of channels in use, falls below the % value set for a time period defined by the Service-Idle Time. The last call (calls - if Minimum Calls is greater than 1) to the Service is only dropped if the % utilization falls to 0, for a time period defined by the Service-Idle Time. Only used when 2 or more channels are set above. For example, if Minimum Channels set to 1, Maximum Channels set to 2 and Reduce Bandwidth is set to 10 - once the usage of the 2 channels drops to 10% the number of channels used is 1.

Table continues…

Field	Description
Callback Telephone Number	Default = Blank The number that is given to the remote service, via BAP, which the remote Control Unit then dials to allow the bandwidth to be increased. Incoming Call routing and RAS Services must be appropriately configured.
Idle Period (secs)	Default = 10 seconds. Range = 0 to 999999 seconds. The time period, in seconds, required to expire after the line has gone idle. At this point the call is considered inactive and is completely closed. For example, the 'Idle Period' is set to X seconds. X seconds before the 'Active Idle Period' timeouts the Control Unit checks the packets being transmitted/received, if there is nothing then at the end of the 'Active Idle Period' the session is closed & the line is dropped. If there are some packets being transmitted or received then the line stays up. After the 'Active Idle Period' has timed out the system performs the same check every X seconds, until there are no packets being transferred and the session is closed and the line dropped.
Active Idle Period (secs):	Default = 180 seconds. Range = 0 to 999999 seconds. Sets the time period during which time the line has gone idle but there are still active sessions in progress (for example an FTP is in process, but not actually passing data at the moment). Only after this timeout will call be dropped. For example, you are downloading a file from your PC and for some reason the other end has stopped responding, (the remote site may have a problem etc.) the line is idle, not down, no data is being transmitted/ received but the file download session is still active. After the set time period of being in this state the line will drop and the sessions close. You may receive a remote server timeout error on your PC in the Browser/FTP client you were using.
Minimum Call Time (secs):	Default = 60 seconds. Range = 0 to 999999 seconds. Sets the minimum time that a call is held up after initial connection. This is useful if you pay a minimum call charge every time a call is made, no matter the actual length of the call. The minimum call time should be set to match that provided by the line provider.
Extra Bandwidth Mode	Default = Incoming Outgoing Defines the mode of operation used to increases bandwidth to the initial call to the remote Service. The options are: • **Outgoing Only** Bandwidth is added by making outgoing calls. • **Incoming Only** Bandwidth is added by the remote service calling back on the BACP number (assuming that BACP is successfully negotiated). • **Outgoing Incoming** Uses both methods but bandwidth is first added using outgoing calls. • **Incoming Outgoing** Uses both methods but bandwidth is first added using incoming BACP calls.

Related Links

Normal, WAN or Intranet Services on page 470

Service | IP

The fields in this tab are used to configure network addressing for the services you are running. Depending on how your network is configured, the use of Network Address Translation (NAT) may be required.

Usability

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

Field	Description
IP Address	Default = 0.0.0.0 (address assigned by ISP) An address should only be entered here if a specific IP address and mask have been provided by the Service Provider. Note that if the address is in a different domain from the system then NAT is automatically enabled
IP Mask	Default = 0.0.0.0 (use NAT) Enter the IP Mask associated with the IP Address if an address is entered.
Primary Transfer IP Address	Default = 0.0.0.0 (No transfer) This address acts as a primary address for incoming IP traffic. All incoming IP packets without a session are translated to this address. This would normally be set to the local mail or web server address. For control units supporting a LAN1 and LAN2, the primary transfer address for each LAN can be set through the **System | LAN1** and **System | LAN2** tabs.
RIP Mode	Default = None Routing Information Protocol (RIP) is a method by which network routers can exchange information about device locations and routes. RIP can be used within small networks to allow dynamic route configuration as opposed to static configuration using. The options are: • **None** The LAN does not listen to or send RIP messages. • **Listen Only (Passive)** Listen to RIP-1 and RIP-2 messages in order to learn RIP routes on the network. • **RIP1** Listen to RIP-1 and RIP-2 messages and send RIP-1 responses as a sub-network broadcast. • **RIP2 Broadcast (RIP1 Compatibility)** Listen to RIP-1 and RIP-2 messages and send RIP-2 responses as a sub-network broadcast. • **RIP2 Multicast** Listen to RIP-1 and RIP-2 messages and send RIP-2 responses to the RIP-2 multicast address.
Request DNS	Default = Off. When selected, DNS information is obtained from the service provider. To use this, the DNS Server addresses set in the system configuration (System | DNS) should be blank. The PC making the DNS request should have the system set as its DNS Server. For DHCP clients the system will provide its own address as the DNS server.

Table continues…

Field	Description
Forward Multicast Messages	Default = On. By default this option is on. Multicasting allows WAN bandwidth to be maximized through the reduction of traffic that needs to be passed between sites.

Related Links

Normal, WAN or Intranet Services on page 470

Service | Autoconnect

Fields in this tab enable you to set up automatic connections to the specified Service.

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

Field	Description
Auto Connect Interval (mins):	Default = 0 (disabled). Range = 0 to 99999 minutes. This field defines how often this Service will automatically be called ("polled"). For example setting 60 means the system will call this Service every hour in the absence of any normally generated call (this timer is reset for every call; therefore if the service is already connected, then no additional calls are made). This is ideal for SMTP Mail polling from Internet Service Providers.
Auto Connect Time Profile	Default = <None> Allows the selection of any configured Time Profiles. The selected profile controls the time period during which automatic connections to the service are made. It does NOT mean that connection to that service is barred outside of these hours. For example, if a time profile called "Working Hours" is selected, where the profile is defined to be 9:00AM to 6:00PM Monday to Friday, then automatic connection to the service will not be made unless its within the defined profile. If there is an existing connection to the service at 9:00AM, then the connection will continue. If there is no connection, then an automatic connection will be made at 9:00AM.

Related Links

Normal, WAN or Intranet Services on page 470

Service | Quota

Quotas are associated with outgoing calls, they place a time limit on calls to a particular IP Service. This avoids excessive call charges when perhaps something changes on your network and call frequency increases unintentionally.

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

Field	Description
Quota Time (mins)	Default = 240 minutes. Range = 0 to 99999 minutes. Defines the number of minutes used in the quota. When the quota time is used up no further data can be passed to this service. This feature is useful to stop things like an internet game keeping a call to your ISP open for a long period.

Table continues…

Field	Description
	Warning: Setting a value here without selecting a Quota period below will stop all further calls after the Quota Time has expired.
Quota:	Default = Daily. Range = None, Daily, Weekly or Monthly Sets the period during which the quota is applied. For example, if the **Quota Time** is 60 minutes and the **Quota** is set to **Daily**, then the maximum total connect time during any day is 60 minutes. Any time beyond this will cause the system to close the service and prevent any further calls to this service. To disable quotas select **None** and set a **Quota Time** of zero. **Note:** The ClearQuota feature can be used to create short codes to refresh the quota time.

Related Links

Normal, WAN or Intranet Services on page 470

Service | PPP

Fields in this tab enable you to configure Point to Point Protocol (PPP) in relation to this particular service. PPP is a protocol for communication between two computers using a Serial interface.

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

Field	Description
Chap Challenge Interval (secs)	Default = 0 (disabled). Range = 0 to 99999 seconds. The period between CHAP challenges. Blank or 0 disables repeated challenges. Some software such as Windows 95 DUN does not support repeated CHAP challenges.
Bi-Directional Chap	Default =Off.
Header Compression	Default = None selected Enables the negotiation and use of IP Header Compression. Supported modes are IPHC and VJ. IPHC should be used on WAN links.
PPP Compression Mode	Default = MPPC Enables the negotiate and use of compression. Do not use on VoIP WAN links. The options are: • **Disable** Do not use or attempt to use compression. • **StacLZS** Attempt to use STAC compression (Mode 3, sequence check mode). • **MPPC** Attempt to use MPPC compression. Useful for NT Servers.
PPP Callback Mode	Default = Disabled. The options are: • **Disable** Callback is not enabled

Table continues…

Field	Description
	• **LCP** (Link Control Protocol) After authentication the incoming call is dropped and an outgoing call to the number configured in the Service is made to re-establish the link. • **Callback CP** (Microsoft's Callback Control Protocol) After acceptance from both ends the incoming call is dropped and an outgoing call to the number configured in the Service is made to re-establish the link. • **Extended CBCP** (Extended Callback Control Protocol) Similar to Callback CP except the Microsoft application at the remote end prompts for a telephone number. An outgoing call is then made to that number to re-establish the link.
PPP Access Mode	Default = Digital64 Sets the protocol, line speed and connection request type used when making outgoing calls. Incoming calls are automatically handled (see RAS services). The options are: • **Digital64** Protocol set to Sync PPP, rate 64000 bps, call presented to local exchange as a "Data Call". • **Digital56** As above but rate 56000 bps. • **Voice56** As above but call is presented to local exchange as a "Voice Call". • **V120** Protocol set to Async PPP, rate V.120, call presented to local exchange as a "Data Call". This mode runs at up to 64K per channel but has a higher Protocol overhead than pure 64K operation. Used for some bulletin board systems as it allows the destination end to run at a different asynchronous speed to the calling end. • **V110** Protocol is set to Async PPP, rate V.110. This runs at 9600 bps, call is presented to local exchange as a "Data Call". It is ideal for some bulletin boards. • **Modem** Allows Asynchronous PPP to run over an auto-adapting Modem to a service provider (requires a Modem2 card in the main unit)
Data Pkt. Size	Default = 0. Range = 0 to 2048. Sets the size limit for the Maximum Transmissible Unit.
BACP	Default = Off. Enables the negotiation and use of BACP/BCP protocols. These are used to control the addition of B channels to increase bandwidth.
Incoming traffic does not keep link up	Default = On. When enabled, the link is not kept up for incoming traffic only.
Multilink/QoS	Default = Off. Enables the negotiation and use of Multilink protocol (MPPC) on links into this Service. Multilink must be enabled if there is more than one channel that is allowed to be Bundled/ Multilinked to this RAS Service.

Related Links

Normal, WAN or Intranet Services on page 470

Service | Fallback

These options allow you to set up a fallback for the Service. For example, you may wish to connect to your ISP during working hours and at other times take advantage of varying call charges from an alternative carrier. You could therefore set up one Service to connect during peak times and another to act as fallback during the cheaper period.

You need to create an additional Service to be used during the cheaper period and select this service from the Fallback Service list box (open the Service form and select the Fallback tab).

If the original Service is to be used during specific hours and the Fallback Service to be used outside of these hours, a Time Profile can be created. Select this Time Profile from the Time Profile list box. At the set time the original Service goes into Fallback and the Fallback Service is used.

A Service can also be put into Fallback manually using short codes, for example:

Put the service "Internet" into fallback:

- **Short Code**: *85
- **Telephone Number**: "Internet"
- **Line Group ID**: 0
- **Feature**: SetHuntGroupNightService

Take the service "Internet" out of fallback:

- **Short Code**: *86
- **Telephone Number**: "Internet"
- **Line Group ID**: 0
- **Feature**: ClearHuntGroupNightService

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

Field	Description
In Fallback	Default = Off. This option indicates whether the Service is in Fallback or not. A service can be set into fallback using this setting. Alternatively a service can be set into fallback using a time profile or short codes.
Time profile	Default = <None> (No automatic fallback) Select the time profile you wish to use for the service. The time profile should be set up for the hours that you wish this service to be operational, out of these hours the Fallback Service is used.
Fallback Service	Default = <None> Select the service that is used when this service is in fallback.

Related Links

Normal, WAN or Intranet Services on page 470

Service | Dial In

About this task

Only available for WAN and Intranet Services. This tab is used to define a WAN connection.

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

To define a WAN connection

Procedure

1. Select Add.
2. Enter WANif the service is being routed via a WAN port on a WAN3 expansion module.

Related Links

Normal, WAN or Intranet Services on page 470

SSL VPN Service

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.

Related Links

Service on page 469
Service on page 478
Session on page 479
NAPT on page 480
Fallback on page 480

Service

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
Service Name	Enter a name for the SSL VPN service.

Table continues…

Field	Description
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.

Related Links

SSL VPN Service on page 478

Session

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

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.

Related Links

SSL VPN Service on page 478

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.

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

The SSL VPN restarts after a setting change.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Application</td><td>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:
<table>
<tr><th>Application</th><th>Protocol</th><th>External and Internal Port Number</th></tr>
<tr><td>Custom</td><td>TCP</td><td>0</td></tr>
<tr><td>VMPro</td><td>TCP</td><td>50791</td></tr>
<tr><td>OneXPortal</td><td>TCP</td><td>8080</td></tr>
<tr><td>SSH</td><td>TCP</td><td>22</td></tr>
<tr><td>TELNET</td><td>TCP</td><td>23</td></tr>
<tr><td>RDP</td><td>TCP</td><td>3389</td></tr>
<tr><td>WebControl</td><td>TCP</td><td>7070</td></tr>
</table></td></tr>
<tr><td>Protocol</td><td>Default = TCP

The protocol used by the application. The options are TCP and UDP.</td></tr>
<tr><td>External Port Number</td><td>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.</td></tr>
<tr><td>Internal IP address</td><td>Default = Blank.

The IP address of the LAN device in the customer network.</td></tr>
<tr><td>Internal Port Number</td><td>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.</td></tr>
</table>

Related Links

SSL VPN Service on page 478

Fallback

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

Field	Description
In Fallback	Default = Off. This setting is used to indicate whether the SSL VPN service is in use or not. • To configure the service without establishing an SSL VPN connection, or to disable an SSL VPN connection, select this option. • To enable the service and establish an SSL VPN connection, de-select this option. • The **Set Hunt Group Night Service** and **Clear Hunt Group Night Service** short code and button features can be used to switch an SSL VPN service off or on respectively. The service is indicated by setting the service name as the telephone number or action data. Do not use quotation marks.

Related Links

SSL VPN Service on page 478

RAS | RAS

A Remote Access Server (RAS) is a piece of computer hardware which sits on a corporate LAN and into which employees dial on the public switched telephone network to get access to their email and to software and data on the corporate LAN.

This form is used to create a RAS service that the system offers Dial In users. A RAS service is needed when configuring modem dial in access, digital (ISDN) dial in access and a WAN link. Some systems may only require one RAS service since the incoming call type can be automatically sensed.

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

Field	Description
Name	A textual name for this service. If **Encrypted Password** below is used, this name must match the **Account Name** entered in the Service form.
Extension	Enter an extension number if this service is to be accessed internally.
COM Port	For future use.
TA Enable	Default = Off Select to enable or disable - if enabled RAS will pass the call onto a TA port for external handling.
Encrypted Password	Default = Off

Table continues…

Field	Description
	This option is used to define whether Dial In users are asked to use PAP or CHAP during their initial log in to the RAS Service. If the Encrypted Password box is checked then Dial In users are sent a CHAP challenge, if the box is unchecked PAP is used as the Dial In Authorization method.

Related Links

[Configuration Mode Field Descriptions](#) on page 193
[RAS | PPP](#) on page 482

RAS | PPP

PPP (Point-to-Point Protocol) is a Protocol for communication between two computers using a Serial interface, typically a personal computer connected by phone line to a server.

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

Field	Description
CHAP Challenge Interval (secs)	Default = 0 (disabled). Range = 0 to 99999 seconds. The period between successive CHAP challenges. Blank or 0 disables repeated challenges. Some software, for example Windows 95 DUN, does not support repeated CHAP challenges.
Header Compression	Default = Off Enables the negotiation and use of IP Header Compression as per RFC2507, RFC2508 and RFC2509.
PPP Compression Mode	Default = MPPC This option is used to negotiate compression (or not) using CCP. If set to MPPC or StacLZS the system will try to negotiate this mode with the remote Control Unit. If set to Disable CCP is not negotiated. The options are: • **Disable** Do not use or attempt to use compression. • **StacLZS** Attempt to use and negotiate STAC compression (the standard, Mode 3) • **MPPC** Attempt to use and negotiate MPPC (Microsoft) compression. Useful for dialing into NT Servers.
PPP Callback Mode	Default = Disable The options are: • **Disable**: Callback is not enabled • **LCP**: (Link Control Protocol) After authentication the incoming call is dropped and an outgoing call to the number configured in the Service will be made to reestablish the link. • **Callback CP**: (Microsoft's Callback Control Protocol) After acceptance from both ends the incoming call is dropped and an outgoing call to the number configured in the Service is made to reestablish the link.

Table continues…

Field	Description
	• **Extended CBCP**: (Extended Callback Control Protocol) Similar to Callback CP however the Microsoft application at the remote end will prompt for a telephone number. An outgoing call will then be made to that number to reestablish the link.
Data Pkt. Size	Default = 0. Range = 0 to 2048. This is the number of data bytes contained in a Data Packet.
BACP	Default = Off Allows negotiation of the BACP/BCP protocols. These are used to control the addition of additional B channels to simultaneously improve data throughput.
Multilink	Default = Off When enabled the system attempts to negotiate the use of the Multilink protocol (MPPC) on the link(s) into this Service. Multilink must be enabled if the more than one channel is allowed to be Bundled/Multilinked to this RAS Service.

Related Links

RAS | RAS on page 481

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

Table continues…

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

Configuration Mode Field Descriptions on page 193
Incoming Call Route | Standard on page 486
Incoming Call Route | Voice Recording on page 489
Incoming Call Route | Destinations on page 490

Incoming Call Route | Standard

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 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.

Table continues…

Field	Description
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. • 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.

Table continues…

Field	Description
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 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

Incoming Call Route on page 483

Incoming Call Route | Voice 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. • **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

Incoming Call Route on page 483

Incoming Call Route | Destinations

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

Incoming Call Route on page 483

WAN Port

These records are used to configure the operation of system WAN ports and services.

WAN services can be run over a T1 PRI trunk connection. This requires creation of a virtual WAN port. For full details refer to Using a Dedicated T1/PRI ISP Link.

Related Links

Configuration Mode Field Descriptions on page 193
WAN Port | WAN Port on page 492
WAN Port | Frame Relay on page 493
WAN Port | DLCIs on page 494
WAN Port | Advanced on page 495

WAN Port | WAN Port

Use this form to configure the leased line connected to the WAN port on the Control Unit. Normally this connection is automatically detected by the control unit. If a WAN Port is not displayed, connect the WAN cable, reboot the Control Unit and receive the configuration. The WAN Port configuration form should now be added.

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

Field	Description
Name	The physical ID of the Extension port,. This parameter is not configurable; it is allocated by the system.
Speed	The operational speed of this port. For example for a 128K connection, enter 128000. This should be set to the actual speed of the leased line as this value is used in the calculation of bandwidth utilization. If set incorrectly, additional calls may be made to increase Bandwidth erroneously.
Mode	Default = SyncPPP Select the protocol required. The options are: • **SyncPPP** For a data link. • **SyncFrameRelay** For a link supporting Frame Relay.

Table continues…

Field	Description
RAS Name	If the **Mode** is **SyncPPP**, selects the RAS service to associate with the port. If the **Mode** is **SyncFrameRelay**, the RAS Name is set through the DLCIs tab.

Related Links

WAN Port on page 492

WAN Port | Frame Relay

This tab is only available for Frame Relay records. These show **SyncFrameRelay** as the **Mode** on the WAN Port tab.

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

Field	Description
Frame Management Type	This must match the management type expected by the network provider. Selecting **AutoLearn** allows the system to automatically determine the management type based on the first few management frames received. If a fixed option is required the following options are supported: • **Q933 AnnexA 0393** • **Ansi AnnexD** • **FRFLMI** • **None**
Frame Learn Mode	This parameter allows the DLCIs that exist on the given WAN port to be provisioned in a number of different ways. • **None** No automatic learning of DLCIs. DLCIs must be entered and configured manually. • **Mgmt** Use LMI to learn what DLCIs are available on this WAN. • **Network** Listen for DLCIs arriving at the network. This presumes that a network provider will only send DLCIs that are configured for this particular WAN port. • **NetworkMgmt** Do both management and network listening to perform DLCI learning and creation.
Max Frame Length	Maximum frame size that is allowed to traverse the frame relay network.
Fragmentation Method	The options are: • **RFC1490** • **RFC1490+FRF12**

Related Links

WAN Port on page 492

WAN Port | DLCIs

This tab is only available for Frame Relay records. These show **SyncFrameRelay** as the **Mode** on the WAN Port tab. The tab lists the DLCIs created for the connection. These can be edited using the **Add**, **Edit** and **Remove** buttons.

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

Field	Description
Frame Link Type	Default = PPP Data transfer encapsulation method. Set to the same value at both ends of the PVC (Permanent Virtual Channel). The options are: • **None** • **PPP** Using PPP offers features such as out of sequence traffic reception, compression and link level connection management. • **RFC 1490** RFC 1490 encapsulation offers performance and ease of configuration and more inter-working with third party CPE. • **RFC1490 + FRF12** Alternate encapsulation to PPP for VoIP over Frame Relay. When selected all parameters on the Service | PPP tab being used are overridden.
DLCI	Default = 100 This is the Data Link Connection Identifier, a unique number assigned to a PVC end point that has local significance only. Identifies a particular PVC endpoint within a user's physical access channel in a frame relay.
RAS Name	Select the RAS Service you wish to use.
Tc	Default = 10 This is the Time Constant in milliseconds. This is used for measurement of data traffic rates. The Tc used by the system can be shorter than that used by the network provider.
CIR	(Committed Information Rate) Default = 64000 bps This is the Committed Information Rate setting. It is the maximum data rate that the WAN network provider has agreed to transfer. The committed burst size (Bc) can be calculated from the set Tc and CIR as Bc = CIR x Tc. For links carrying VoIP traffic, the Bc should be sufficient to carry a full VoIP packet including all its required headers. See the example below.
EIR	(Excess Information Rate) Default = 0 bps This is the maximum amount of data in excess of the CIR that a frame relay network may attempt to transfer during the given time interval. This traffic is normally marked as De (discard eligible). Delivery of De packets depends on the network provider and is not guaranteed and therefore they are not suitable for UDP and VoIP traffic. The excess burst size (Be) can be calculated as Be = EIR x Tc.

Example: Adjusting the Tc Setting

G.729 VoIP creates a 20 byte packet every 20ms. Adding typical WAN PPP headers results in a 33 byte packet every 20ms.

For a Committed Information Rate (CIR) of 14Kbps, with the Time Constant (Tc) set to 10ms; we can calculate the Committed Burst size:

Bc = CIR x Tc = 14,000 x 0.01 = 140 bits = 17.5 bytes.

Using 10ms as the Tc, a full G.729 VoIP packet (33 bytes) cannot be sent without exceeding the Bc. The most likely result is lost packets and jitter.

If the Tc is increased to 20ms:

Bc = CIR x Tc = 14,000 x 0.02 = 280 bits = 35 bytes.

The Bc is now sufficient to carry a full G.729 VoIP packet.

Notes:

1. Backup over Frame Relay is not supported when the Frame Link Type is set to RFC1490.
2. When multiple DLCIs are configured, the WAN link LED is switched off if any of those DLCIs is made inactive, regardless of the state of the other DLCIs. Note also that the WAN link LED is switched on following a reboot even if one of the DLCIs is inactive. Therefore when multiple DLCIs are used, the WAN link LED cannot be used to determine the current state of all DLCIs.
3. When the Frame Link Type is set to RFC1490, the WAN link LED is switched on when the WAN cable is attached regardless other whether being connected to a frame relay network.

Related Links

WAN Port on page 492

WAN Port | Advanced

The settings on this tab are used for Frame Relay connections.

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

Field	Description
Address Length	The address length used by the frame relay network. The network provider will indicate if lengths other than two bytes are to be used.
N391	Full Status Polling Counter Polling cycles count used by the CPE and the network provider equipment when bidirectional procedures are in operation. This is a count of the number of link integrity verification polls (T391) that are performed (that is Status Inquiry messages) prior to a Full Status Inquiry message being issued.
N392	Error Threshold Counter Error counter used by both the CPE and network provider equipment. This value is incremented for every LMI error that occurs on the given WAN interface. The DLCIs attached to the given WAN interface are disabled if the number of LMI errors exceeds this value when N393 events have occurred. If the given WAN interface is in an error condition then that error condition is cleared when N392 consecutive clear events occur.
N393	Monitored Events Counter

Table continues…

Field	Description
	Events counter measure used by both the CPE and network provider equipment. This counter is used to count the total number of management events that have occurred in order to measure error thresholds and clearing thresholds.
T391	Link Integrity Verification Polling Timer The link integrity verification polling timer normally applies to the user equipment and to the network equipment when bidirectional procedures are in operation. It is the time between transmissions of Status Inquiry messages.
T392	Polling Verification Timer The polling verification timer only applies to the user equipment when bidirectional procedures are in operation. It is the timeout value within which to receive a Status Inquiry message from the network in response to transmitting a Status message. If the timeout lapses an error is recorded (N392 incremented).

Related Links

WAN Port on page 492

Directory

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	5000	5000	5000
Server Edition	**Primary Server**	2500	5000	–	5000

Table continues…

	System	Number of Directory Records			Total Number of Directory Records
		Configuration	LDAP Import	HTTP Import	
	Secondary Server	–	–	5000	5000
	Expansion System (L)	–	–	5000	5000
	Expansion System (V2)	–	–	5000	5000

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

Configuration Mode Field Descriptions on page 193
Directory | Directory Record on page 498

Directory | 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.
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 496

Time Profile

For additional configuration information, see Time Profile on page 544.

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 31 characters This name is used to select the time profile from within other tabs.
Override	

Table continues…

Field	Description
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.
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

Configuration Mode Field Descriptions on page 193

Firewall Profile

The system can act as a firewall, allowing only specific types of data traffic to start a session across the firewall and controlling in which direction such sessions can be started.

The system supports Static NAT address translation by a firewall profiles. If the Firewall Profile contains any Static NAT records, all packets received by the firewall must match one of those static NAT records to not be blocked.

If Network Address Translation (NAT) is used with the firewall (which it typically is), then you must also configure a **Primary Incoming Translation Address** (see IP tab of the Service configuration form) if you wish sessions to be started into your site (typically for SMTP) from the Internet.

On Server Edition Linux systems, to ensure that the firewall starts after a reboot, you must enable the **Activate** setting in the Web Control menus. See the document Using the Server Edition Web Control Menus.

System firewall profiles can be applied in the following areas of operation.

System:

A firewall profile can be selected to be applied to traffic between LAN1 and LAN2.

User:

Users can be used as the destination of incoming RAS calls. For those users a firewall profile can be selected on the user's Dial In tab.

Service:

Services are used as the destination for IP routes connection to off-switch data services such as the internet. A Firewall Profile can be selected for use with a service.

Related Links

Configuration Mode Field Descriptions on page 193
Firewall | Standard on page 501
Firewall | Custom on page 503
Static NAT on page 505

Firewall | Standard

By default, any protocol not listed in the standard firewall list is dropped unless a custom firewall entry is configured for that protocol.

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 31 characters Enter the name to identify this profile.		
Protocol Control	For each of the listed protocols, the options **Drop**, **In** (Incoming traffic can start a session), **Out** (Outgoing traffic can start a session) and **Both Directions** can be selected. Once a session is started, return traffic for that session is also able to cross the firewall.		
	Protocol	**Default**	**Description**
	TELNET	Out	Remote terminal log in.
	FTP	Out	File Transfer Protocol.
	SMTP	Out	Simple Mail Transfer Protocol.
	TIME	Out	Time update protocol.
	DNS	Out	Domain Name System.
	GOPHER	Drop	Internet menu system.
	FINGER	Drop	Remote user information protocol.
	RSVP	Drop	Resource Reservation Protocol.
	HTTP/S	Bothway	Hypertext Transfer Protocol.
	POP3	Out	Post Office Protocol.
	NNTP	Out	Network News Transfer Protocol.
	SNMP	Drop	Simple Network Management Protocol.
	IRC	Out	Internet Relay Chat.
	PPTP	Drop	Point to Point Tunneling Protocol.
	IGMP	Drop	Internet Group Membership Protocol.
Service Control	For each of the listed services, the options **Drop**, **In**, **Out** and **Both Directions** can be selected. Once a session is started, return traffic for that session is also able to cross the firewall.		
	Protocol	**Default**	**Description**
	SSI	In	System Status Application access.
	SEC	Drop	TCP security settings access.
	CFG	Drop	TCP configuration settings access.
	TSPI	In	TSPI service access.

Table continues…

Field	Description		
	WS	Drop	IP Office web management services.

Related Links

Firewall Profile on page 501

Firewall | Custom

The tab lists custom firewall settings added to the firewall profile. The Add, Edit and Remove controls can be used to amend the settings in the list.

Example Custom Firewall Records

Dropping NetBIOS searches on an ISPs DNS:

We suggest that the following filter is always added to the firewall facing the Internet to avoid costly but otherwise typically pointless requests from Windows machines making DNS searches on the DNS server at your ISP.

Direction: Drop

IP Protocol: 6 (TCP)

Match Offset: 20

Match Length: 4

Match Data: 00890035

Match Mask: FFFFFFFF

Browsing Non-Standard Port Numbers:

The radio button for HTTP permits ports 80 and 443 through the firewall. Some hosts use non-standard ports for HTTP traffic, for example 8080, 8000, 8001, 8002, etc. You can add individual filters for these ports as you find them.

You wish to access a web page but you cannot because it uses TCP port 8000 instead of the more usual port 80, use the entry below.

Direction: Out

IP Protocol: 6 (TCP)

Match Offset: 22

Match Length: 2

Match Data: 1F40

Match Mask: FFFF

A more general additional entry given below allows all TCP ports out.

Direction: Out

IP Protocol: 6 (TCP)

Match Offset: 0

Match Length: 0

Match Data: 00000000000000000000000000000000

Match Mask: 00000000000000000000000000000000

Routing All Internet Traffic through a WinProxy:

If you wish to put WinProxy in front of all Internet traffic via the Control Unit. The following firewall allows only the WinProxy server to contact the Internet : -

1. Create a new Firewall profile and select **Drop** for all protocols
2. Under Custom create a new Firewall Entry
3. In Notes enter the name of the server allowed. Then use the default settings except in Local IP Address enter the IP address of the WinProxy Server, in Local IP Mask enter 255.255.255.255 and in Direction select Both Directions.

Stopping PINGs:

You wish to stop pings - this is ICMP Filtering. Using the data below can create a firewall filter that performs the following; Trap Pings; Trap Ping Replies; Trap Both.

Trap Pings: Protocol = 1, offset = 20, data = 08, mask = FF

Trap Ping Replies: Protocol = 1, offset = 20, data = 00, mask = FF

Trap Both: Protocol = 1, offset = 20, data = 00, mask = F7, Traps Both.

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

Field	Description
Notes	For information only. Enter text to remind you of the purpose of the custom firewall record.
Remote IP Address	The IP address of the system at the far end of the link. Blank allows all IP addresses.
Remote IP Mask	The mask to use when checking the Remote IP Address. When left blank no mask is set, equivalent to 255.255.255.255 - allow all.
Local IP Address	The address of devices local to this network (pre-translated). Blank allows all IP addresses.
Local IP Mask	The mask to use when checking the Local IP Address. When left blank no mask is set, equivalent to 255.255.255.255 - allow all.
IP Protocol	The value entered here corresponds to the IP Protocol which is to be processed by this Firewall profile: 1 for ICMP, 6 for TCP, 17 for UDP or 47 for GRE. This information can be obtained from the "pcol" parameter in a Monitor trace.
Match Offset	The offset into the packet (0 = first byte of IP packet) where checking commences for either a specific port number, a range of port numbers, or data.
Match Length	The number of bytes to check in the packet, from the Match Offset point, that are checked against the Match Data and Match Mask settings.
Match Data	The values the data must equal once masked with the Match Mask. This information can be obtained from "TCP Dst" parameter in a Monitor trace (the firewall uses hex so a port number of 80 is 50 in hex)

Table continues…

Field	Description	
Match Mask	This is the byte pattern, which is logically ANDed with the data in the packet from the offset point. The result of this process is then compared against the contents of the "Match Data" field.	
Direction	The direction that data may take if matching this filter.	
	Drop	All matching traffic is dropped.
	In	Incoming traffic can start a session.
	Out	Outgoing traffic can start a session.
	Both Directions	Both incoming and outgoing traffic can start sessions.

Related Links

Firewall Profile on page 501

Static NAT

The **Static NAT** table allows the firewall to perform address translation between selected internal and external IP addresses. Up to 64 internal and external IP address pairs can be added to the Static NAT section of a Firewall Profile.

This feature is intended for incoming maintenance access using applications such as PC-Anywhere, Manager and the Voicemail Pro Client. The address translation is used for destinations such a Voicemail Pro server or the system's own LAN1 address.

- If there are any records in the **Static NAT** settings of a Firewall Profile, each packet attempting to pass through the firewall must match one of the static NAT pairs or else the packet will be dropped.
- The destination address of incoming packets is checked for a matching **External IP Address**. If a match is found, the target destination address is changed to the corresponding **Internal IP Address**.
- The source address of outgoing packets is checked for a matching **Internal IP Address**. If a match is found, the source address is changed to the corresponding **External IP Address**.
- Even when a static NAT address match occurs, the other settings on the Firewall Profile Standard and Custom tabs are still applied and may block the packet.

Related Links

Firewall Profile on page 501

IP Route

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.

Related Links

Configuration Mode Field Descriptions on page 193
IP Route | IP Route on page 506
RIP Dynamic Routing on page 507

IP Route | IP Route

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.
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 505

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

IP Route on page 505

Account Code

Account codes are commonly used to control cost allocation and out-going call restriction. The account code used on a call is included in the call information output by the system's call log. Incoming calls can also trigger account codes automatically by matching the Caller ID stored with the account code.

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

Once a call has been completed using an account code, the account code information is removed from the user's call information. This means that redial functions will not re-enter the account code. The maximum recommended number of accounts codes is 1000.

Related Links

Configuration Mode Field Descriptions on page 193

Account Code | Account Code

This tab is used to define an individual account code.

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	Descriptions
Account Code	Enter the account code required. It can also include wildcards; **?** matches a single digit and ***** matches any digits.
Caller ID	A caller ID can be entered and used to automatically assign an account code to calls made to or received from caller ID.

Account Code | Voice Recording

This tab is used to activate the automatic recording of external calls when the account code is entered at the start of the call. For pre-Release 4.0 systems the tab also provided settings for recording on calls automatically assigned by caller ID matching when the call is received.

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

Note the following:

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

The destination mailbox for the recording can be specified.

Configuration Settings

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

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

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

License

ADI

The license keys are unique 32-character codes based on the feature being activated and a unique identified used by the system.

The feature key dongle is the unique identifier for IP500 v2 systems. Its serial number is shown in the **Dongle Serial Number** field (**System | System**) in the configuration. The feature key dongle takes the form of a card (smart media or SD card respectively) inserted into the control unit. The card is a mandatory item for these systems even if they use no licensed features. The serial number is printed on the feature key dongle and prefixed with **SN** (**FK** for IP500 V2 SD card dongles).

For Linux based systems, the System Identification value of the system is the unique identifier. The **System Identification** value (**System | System**) is a 'fingerprint' value generated from the server hardware (the server and the server hard disk). This means that licenses are tied to a particular system and cannot be used on another system.

For more information on IP Office licensing requirements, see *Avaya IP Office Platform™ Solution Description*.

Importing License Keys

It is recommended that licenses are cut and pasted electronically. This removes the chances of errors due to mistyping and misinterpretation of characters fonts. Where multiple licenses need to be added, the CSV import option can be used (**File | Import/Export | Import**). Licenses imported this way may be listed as invalid until the configuration is saved and then reloaded.

WebLM

WebLM is a web-based application for managing licenses. To establish communication between IP Office and the WebLM server, you must configure the remote server profile on the **License | Remote Server** tab.

For more information on managing licenses on Enterprise Branch systems, see *Deploying IP Office in an Avaya Aura Branch Environment*.

PLDS

IP Office systems can use the Avaya Product Licensing and Delivery System (PLDS) to manage license files. PLDS is an online, web-based tool for managing license entitlements and electronic delivery of software and related license files. PLDS provides customers, Avaya Partners, distributors, and Avaya Associates with easy-to-use tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads.

PLDS Nodal license files are machine specific and you must specify the host ID in the PLDS Host ID field on the **License | License** tab.

PLDS WebLM license files are not machine specific. The WebLM server manages the license file for multiple IP Office systems. For PLDS WebLM license files, the host ID is the WebLM server MAC address.

For IP500 v2 systems, the PLDS host ID is made of the two digits "11" followed by the 10 digit feature key serial number printed on the IP Office SD card. For Linux based systems the PLDS host ID is derived from the system identification. If the system identification changes the PLDS host ID will also change

Related Links

Configuration Mode Field Descriptions on page 193
License | License on page 511
License | Remote Server on page 513

License | License

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

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>License Mode:</td><td>Identifies the status of the system licenses. The two license configuration types are nodal and WebLM. Nodal licenses are licenses that are present on the system. WebLM licenses means licenses obtained from the WebLM server.

The options are:
• Normal Mode Normal nodal licensing mode. In this mode, WebLM is not configured and only nodal licensing is allowed.
• Server Error This mode occurs when transitioning to WebLM licensing. WebLM has been configured but the server is not available.
• Configuration Error This mode occurs when transitioning to WebLM licensing. WebLM has been configured and the server is available, but there are not enough licenses available to license all of the configured features. Only nodal licenses are valid.
• WebLM Normal Mode WebLM has been configured and there are enough licenses available to license all of the configured features.
• WebLM Error Mode Action is required to correct the License Mode. Refer to the License Status column and the Error List section at the bottom of the screen to determine why the system is in License Error Mode. A 30-day grace period provides access to the capacities and features of the installed license when the system is in License Error Mode.
• WebLM Restricted Mode When the system is in License Error Mode, if the problem is not resolved with the 30-day grace period, the system will enter License Restricted Mode. When in this mode, configuration changes are blocked, except for fixing the licensing errors. Features that require a license do not function.
<table>
<tr><th>Type</th><th>Mode</th><th>WebLM Configured</th><th>Virtual License and Grace Period (30 days)</th></tr>
<tr><td>Nodal</td><td>Normal</td><td>No</td><td>No</td></tr>
<tr><td>Nodal</td><td>Server Error</td><td>Yes</td><td>No</td></tr>
<tr><td>Nodal</td><td>Configuration Error</td><td>Yes</td><td>No</td></tr>
<tr><td>WebLM</td><td>Normal</td><td>Yes</td><td>No</td></tr>
<tr><td>WebLM</td><td>Error</td><td>Yes</td><td>Yes</td></tr>
<tr><td>WebLM</td><td>Restricted</td><td>Yes</td><td>No</td></tr>
</table></td></tr>
<tr><td>Licensed Version</td><td>Indicates the software version the system is currently licensed for.</td></tr>
<tr><td>Serial Number (ADI)</td><td>The key to use to generate ADI licenses for the system. For IP500 V2 systems, it is the SD card serial number. For Linux systems, it is the system ID.</td></tr>
<tr><td>PLDS Host ID</td><td>The ID used when generating PLDS nodal license files. Not used with WebLM licensing.</td></tr>
<tr><td>PLDS File Status</td><td>If a PLDS nodal license file is loaded, this field indicates if the file is valid or not.</td></tr>
<tr><td>Select Licensing</td><td>Indicates that the system has a valid Select license.</td></tr>
<tr><td>Feature</td><td>Identifies the licenses installed on the system.</td></tr>
</table>

Table continues…

Field	Description
Key	This is the license key string supplied. It is a unique value based on the feature being licensed and the either the system's **Dongle Serial Number** or **System Identification** depending on the type of system (**System | System**).
Instance	For information only. Some licenses enable a number of port, channels or users. When that is the case, the number of such is indicated here. Multiple licenses for the same feature are usually cumulative.
Status	For information only. This field indicates the current validation status of the license key. • **Unknown** This status is shown for licenses that have just been added to the configuration shown in Manager. Once the configuration has been sent back to the system and then reloaded, the status will change to one of those below. • **Valid** The license has is valid. • **Invalid** The license was not recognized. It did not match the **Dongle Serial Number** or the **System Identification** number of the system. • **Dormant** The license is valid but is conditional on some other pre-requisite licenses. • **Obsolete** The license is valid but is one no longer used by the level of software running on the system.
Expiry Date	For information only. Licenses can be set to expire within a set period from their issue. The expiry date is shown here.
Source	The source of the license file. The options are: • **ADI Nodal** ADI licenses added locally to the system. • **PLDS Nodal** PLDS licenses added locally to the system. • **WebLM** Licenses obtained from the WebLM server. • **Virtual** Licenses created by the system.

Related Links

License on page 510

License | Remote Server

The Remote Server tab is used for:

- IP500 V2 systems in a Enterprise Branch deployments using WebLM licensing
- Server Edition systems to specify the centralized (Primary) licensing server.

These settings are not mergeable on IP500 V2 systems. Mergeable on Server Edition systems.

Field	Description
License Server IP Address	Default = 127.0.0.1

Table continues…

Field	Description
	This field is displayed on a Server Edition Primary Server. It is the IP address of the WebLM server.
Remote Server Configuration (Only visible on standalone IP500 v2 systems.)	
Enable Remote Server	Default = Off. Check this box if you are going to use WebLM to manage licenses. When enabled, the **Reserved Licenses** fields for are available.
Domain Name (URL)	Default = Blank. For Enterprise Branch deployments, the domain name of the WebLM server or the domain name of System Manager if the system is under System Manager control. For Server Edition deployments, the domain name of the Primary Server. The interface will allow configuration of the FQDN or IP address prefixed with http:// or https://.
URN	Default = WebLM/License Server. The name of the WebLM server or the name of the Server Edition Primary Server.
Port Number	Default = 52233. The port number of the WebLM server or the port number of the Server Edition Primary Server.
Reserved Licenses	Available on IP500 V2 systems when a licensing server is enabled. Used for obtaining WebLM licenses for the items listed. The value entered specifies the number of licenses to obtain from the WebLM server.

Related Links

License on page 510

Tunnel

Tunneling allows additional security to be applied to IP data traffic. This is useful when sites across an unsecure network such as the public internet. The system supports two methods of tunneling, L2TP and IPSec. Once a tunnel is created, it can be used as the destination for selected IP traffic in the IP Route table.

The use of tunnels is not supported by Linux based systems. On other systems, two types of tunneling are supported.

L2TP:

Layer 2 Tunneling Protocol PPP (Point to Point Protocol) authentication normally takes place between directly connected routing devices. For example when connecting to the internet, authentication is between the customer router and the internet service provider's equipment. L2TP allows additional authentication to be performed between the routers at each end of the connection regardless of any intermediate network routers. The use of L2TP does not require a license.

IPSec:

IPSec allows data between two locations to be secured using various methods of sender authentication and or data encryption. The use of IPSec requires entry of an IPSec Tunneling license into the system at each end.

Related Links

Configuration Mode Field Descriptions on page 193
L2TP Tunnel on page 515
IP Security Tunnel on page 517

L2TP Tunnel

Related Links

Tunnel on page 514
Tunnel | Tunnel (L2TP) on page 515
Tunnel | L2TP on page 516
Tunnel | PPP (L2TP) on page 517

Tunnel | Tunnel (L2TP)

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
Name	Default = Blank. A unique name for the tunnel. Once the tunnel is created, the name can be selected as a destination in the IP Route table.
Local Configuration The account name and password is used to set the PPP authentication parameters.	
Local Account Name	The local user name used in outgoing authentication.
Local Account Password/ Confirm Password	The local user password. Used during authentication.

Table continues…

Field	Description
Local IP Address	The source IP address to use when originating an L2TP tunnel. By default (un-configured), the system uses the IP address of the interface on which the tunnel is to be established as the source address of tunnel.
Remote Configuration The account name and password is used to set the PPP authentication parameters.	
Remote Account Name	The remote user name that is expected for the authentication of the peer.
Remote Account Password/ Confirm Password	The password for the remote user. Used during authentication.
Remote IP Address	The IP address of the remote L2TP peer or the local VPN line IP address or the WAN IP address.
Minimum Call Time (Mins)	Default = 60 minutes. Range = 1 to 999. The minimum time that the tunnel will remain active.
Forward Multicast Messages	Default = On Allow the tunnel to carry multicast messages when enabled.
Encrypted Password	Default = Off When enabled, the CHAP protocol is used to authenticate the incoming peer.

Related Links

L2TP Tunnel on page 515

Tunnel | L2TP

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

Field	Description
Shared Secret/ Confirm Password	User setting used for authentication. Must be matched at both ends of the tunnel. This password is separate from the PPP authentication parameters defined on the L2TP|Tunnel tab.
Total Control Retransmission Interval	Default = 0. Range = 0 to 65535. Time delay before retransmission.
Receive Window Size	Default = 4. Range = 0 to 65535. The number of unacknowledged packets allowed.
Sequence numbers on Data Channel	Default = On When on, adds sequence numbers to L2TP packets.

Table continues…

Field	Description
Add checksum on UDP packets	Default = On. When on, uses checksums to verify L2TP packets.
Use Hiding	Default = Off When on, encrypts the tunnel's control channel.

Related Links

L2TP Tunnel on page 515

Tunnel | PPP (L2TP)

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

Field	Description
CHAP Challenge Interval (secs)	Default = 0 (Disabled). Range = 0 to 99999 seconds. Sets the period between CHAP challenges. Blank or 0 disables repeated challenges. Some software (such as Windows 95 DUN) does not support repeated challenges.
Header Compression	Default = None Select header compression. Options are: IPHC and/or VJ.
PPP Compression Mode	Default = MPPC Select the compression mode for the tunnel connection. Options are: Disable, StacLZS or MPPC.
Multilink/QoS	Default = Off Enable the use of Multilink protocol (MPPC) on the link.
Incoming traffic does not keep link up	Default = On When enabled, the link is not kept up when the only traffic is incoming traffic.
LCP Echo Timeout (secs)	Default = 6. Range = 0 to 99999 seconds. When a PPP link is established, it is normal for each end to send echo packets to verify that the link is still connected. This field defines the time between LCP echo packets. Four missed responses in a row will cause the link to terminate.

Related Links

L2TP Tunnel on page 515

IP Security Tunnel

Related Links

Tunnel on page 514
Tunnel | Main (IPSec) on page 518
Tunnel | IKE Policies (IPSec) on page 518
Tunnel | IPSec Policies on page 519

Tunnel | Main (IPSec)

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
Name	Default = Blank. A unique name for the tunnel. Once the tunnel is created, the name can be selected as a destination for traffic in the IP Route table.
Local Configuration The IP Address and IP Mask are used in conjunction with each other to configure and set the conditions for this Security Association (SA) with regard to inbound and outbound IP packets.	
IP Address	The IP address or sub-net for the start of the tunnel.
IP Mask	The IP mask for the above address.
Tunnel Endpoint IP Address	The local IP address to be used to establish the SA to the remote peer. If left un-configured, the system will use the IP address of the local interface on which the tunnel is to be configured.
Remote Configuration The IP Address and IP Mask are used in conjunction with each other to configure and set the conditions for this Security Association (SA) with regard to inbound and outbound IP packets.	
IP Address	The IP address or sub-net for the end of the tunnel.
IP Mask	The IP mask for the above address.
Tunnel Endpoint IP Address	The IP address of the peer to which a SA must be established before the specified local and remote addresses can be forwarded.

Related Links

IP Security Tunnel on page 517

Tunnel | IKE Policies (IPSec)

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

Field	Description
Shared Secret/ Confirm Password	The password used for authentication. This must be matched at both ends of the tunnel.
Exchange Type	Default = ID Prot Aggressive provides faster security setup but does not hide the ID's of the communicating devices. **ID Prot** is slower but hides the ID's of the communicating devices.
Encryption	Default = DES CBC

Table continues…

Field	Description
	Select the encryption method used by the tunnel. The options are: • **DES CBC** • **3DES** • **Any**
Authentication	Default = MD5 The method of password authentication. Options are: • **MD5** • **SHA** • **Any**
DH Group	Default = Group 1
Life Type	Default = KBytes Sets whether **Life** (below) is measured in seconds or kilobytes.
Life	Range = 0 to 99999999. Determines the period of time or the number of bytes after which the SA key is refreshed or re-calculated.

Related Links

IP Security Tunnel on page 517

Tunnel | IPSec Policies

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

Field	Description
Protocol	Default = ESP The options are: • **ESP** (Encapsulated Security Payload) • **AH** (Authentication Header, no encryption)
Encryption	**Default = DES** Select the encryption method used by the tunnel. The options are: • **DES CBC** • **3DES** • **Any**
Authentication	Default = HMAC MD5 The method of password authentication. Options are: • **HMAC MD5** • **HMAC SHA**

Table continues…

Field	Description
	• **Any**
Life Type	Default = KBytes Sets whether Life (below) is measured in seconds or kilobytes.
Life	Determines the period of time or the number of bytes after which the SA key is refreshed or re-calculated.

Related Links

IP Security Tunnel on page 517

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

Configuration Mode Field Descriptions on page 193
Auto Attendant | Auto Attendant on page 521
Auto Attendant | Actions on page 523

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. 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

Table continues…

Field	Description
	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

Auto Attendant on page 520

Auto Attendant | Actions

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

These settings 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.	
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

Table continues…

Field	Description
	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 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

Auto Attendant on page 520

Authorization Codes

These settings have changed in release 9.1. View the release 9.0 settings. on page 525

Note:

In release 9.1, authorization codes can no longer be associated with User Rights. If an authorization code was configured in relationship with User Rights in an earlier release configuration, this authorization code will be lost during upgrade. The administrator must re-configure the authorization code, after upgrade. The authorization code must be associated with a user.

Authorization codes are enabled by default.

Each authorization code is associated with a particular user. The user can then dial numbers which are set to trigger forced authorization code entry. Once a code is entered, the short code settings of the user with which the code is associated are used to completed the call.

This can be used to allow authorized users to make otherwise restricted calls from any extension without first having to log in to that extension and then log out after the call. Valid/invalid authorization code entry can be recorded in the SMDR output.

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

Field	Description
Authorization Code	Range = Up to 12 digits. The digits used for the authorization code. Each code must be unique. Wildcards are not usable with authorization codes.
User	This field is used to select a user with which the authorization code is associated. The authorization code can then be used to authorize calls made by that user.

Related Links

Configuration Mode Field Descriptions on page 193
Authorization Codes | Authorization Codes (9.0) on page 525

Authorization Codes | Authorization Codes (9.0)

Authorization codes are not shown by default. Manager must be modified in order to support authorization codes.

Each authorization code is associated with a particular user. The user can then dial numbers which are set to trigger forced authorization code entry. Once a code is entered, the short code settings of the user with which the code is associated are used to completed the call.

This can be used to allow authorized users to make otherwise restricted calls from any extension without first having to log in to that extension and then log out after the call. Authorization code usage can be recorded in its SMDR output, including valid/invalid code entry and the code used.

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

Field	Description
Authorization Code	Range = Up to 12 digits. The digits used for the authorization code. Each code must be unique. Wildcards are not usable with authorization codes.
User Rights	This field is used to select the user right with which the authorization code is associated. The authorization code can then be used to authorize calls made by users currently associated with that set of user rights.
User	This field is used to select a user with which the authorization code is associated. The authorization code can then be used to authorize calls made by that user.

Related Links

Authorization Codes on page 524

User Rights

User Rights act as templates for selected user settings. The settings of a user rights template are applied to all users associated with that template. The use of a template can also be controlled by a time profile to set when the template is used for a particular user.

Related Links

Configuration Mode Field Descriptions on page 193

User Rights | User

This tab is used to set and lock various user settings.

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

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

Field	Description
Name	The name for the user rights . This must be set in order to allow the user rights to be selected within the User Rights drop down list on the User | User tab of individual users.
Application Servers Group	Default = Off. Set to On if the IP Office system is deployed in an IP Office Contact Center solution or an Avaya Contact Center Select solution. Only one user rights record can be configured to be the Application Servers Group. If it is set on any one group then the control is disabled on all other groups.
Locale	Default = Blank Sets and locks the language used for voicemail prompts to the user, assuming the language is available on the voicemail server. On a digital extension it also controls the display language used for messages from the system to the phone. See Supported Country and Locale Settings.
Priority	Default = 5, Range 1 (Lowest) to 5 (Highest) Sets and locks the user's priority setting for least cost routing.
Do Not Disturb	Default = Off Sets and locks the user's DND status setting.

User Rights | Short Codes

This tab is used to set and lock the user's short code set. The tab operates in the same way as the **User | Short Codes** tab. User and User Rights short codes are only applied to numbers dialed by that user. For example they are not applied to calls forwarded via the user.

Warning:

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

Usability

Mergeable: ✓ 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.

Configuration Settings

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

User Rights | Button Programming

This tab is used to set and lock the user's programmable button set. When locked, the user cannot use **Admin** or **Admin1** buttons on their phone to override any button set by their user rights.

Buttons not set through the user rights can be set through the user's own settings. When **Apply user rights value** is selected, the tab operates in the same manner as the User | Button Programming tab.

Usability

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

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

Adding Blank Buttons

There are scenarios where users are able to program their own buttons but you may want to force certain buttons to be blank. This can be done through the user's associated **User Rights** as follows:

1. Assign the action **Emulation | Inspect** to the button. This action has no specific function. Enter some spaces as the button label.
2. When pressed by the user, this button will not perform any action. However it cannot be overridden by the user.

User Rights | Telephony

This tab allows various user telephony settings to be set and locked. These match settings found on the User | Telephony tab.

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.

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
No Answer Time	Default = Blank (Use system setting). Range = 6 to 99999 seconds. Sets how long a call rings the user before following forwarded on no answer if set or going to voicemail. Leave blank to use the system default setting.
Transfer return Time (secs)	Default = Blank (Off), Range 1 to 99999 seconds. Sets the delay after which any call transferred by the user, which remains unanswered, should return to the user if possible.
Wrap up Time (secs)	Default = 2 seconds, Range 0 to 99999 seconds.

Table continues…

Field	Description
	Specifies the amount of time after ending one call before another call can ring. You may wish to increase this in a "call center" environment where users may need time to log call details before taking the next call. It is recommended that this option is not set to less than the default of 2 seconds. 0 is used for immediate ringing.
Call waiting on/ Enable call waiting	Default = Off For users on phones without appearance buttons, if the user is on a call and a second call arrives for them, an audio tone can be given in the speech path to indicate a waiting call (the call waiting tone varies according to locale). The waiting caller hears ringing rather than receiving busy. There can only be one waiting call, any further calls receive normal busy treatment. If the call waiting is not answered within the no answer time, it follows forward on no answer or goes to voicemail as appropriate. User call waiting is not used for users on phones with multiple call appearance buttons. Call waiting can also be applied to hunt group calls, see **Hunt Group | Hunt Group | Call Waiting**.
Busy on held/ Enable busy on Held	Default = Off If on, when the user has a call on hold, new calls receive busy tone (ringing for incoming analog call) or are diverted to voicemail if enabled, rather than ringing the user. Note this overrides call waiting when the user has a call on hold.

Supervisor Settings

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

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

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

Field	Description
Can Intrude	Default = Off Check this option if the User can interrupt other user's calls. This setting and the setting below are used to control the use of the following short code and button features: • Call Intrude • Call Listen • Call Steal • Dial Inclusion
Cannot be Intruded	Default = On If checked, this user's calls cannot be interrupted or acquired. In addition to the features listed above, this setting also affects whether other users can use their appearance buttons to bridge into a call to which this user has been the longest present user.
Force Login	Default = Off

Table continues…

Field	Description
	If checked, the user must log in using their Login Code to use an extension. For example, if Force Login is ticked for User A and user B has logged into A's phone, after B logs off A must log back. If Force Login was not ticked, A would be automatically logged back in.
Force Account Code	Default = Off If checked, the user must enter a valid account code to make an external call.
Inhibit Off-Switch Forward/Transfer	: Default = Off When enabled, this setting stops the user from transferring or forwarding calls externally. Note that all user can be barred from forwarding or transferring calls externally by the **System | Telephony | Telephony | Inhibit Off-Switch Forward/Transfers** setting.
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. ⚠ **Caution:** This setting should not be enabled/disabled for a user by using User Rights associated with a Time Profile. Do so will cause invalid data to be recorded in the Customer Call Reporter applications database. The number of simultaneous logged in CCR Agents supported by the system is controlled by licenses entered into the configuration. If all CCR Agent licenses on a system have been used, additional agents are prevented from logging in.
After Call Work Time:	Default = System Default. Range = 10 to 999 seconds. CCR Agents (see above) can be automatically put into **After Call Work** (ACW) state after ending a hunt group call. During ACW state, hunt group calls are not presented to the user. If set to **System Default**, the value set in Default After Call Work (**System | CCR**) is used.
Automatic After Call Work	Default = Off. For CCR Agents with **Automatic After Call Work** enabled, this value sets the duration of the ACW period.
Outgoing Call Bar	Default = Off When set, bars the user from making external calls.
Coverage Group	Default = <None>. If a group is selected, the system will not use voicemail to answer the users unanswered calls. Instead the call will continue ringing until either answered or the caller disconnects. For external calls, after the users no answer time, the call is also presented to the users who are members of the selected Coverage Group. For further details refer to Coverage Groups.

Multi-line 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.

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
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.

Call Log

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

On Avaya phones with a fixed **Call Log** or **History** button (1400, 1600, 9500 and 9600 Series), that button can be used to display the user's centralized call log. The centralized call log is also used for M-Series and T-Series phone. The user can use the call log to make calls or to store as a personal speed dial. They can also edit the call log to remove records. The same call log is also used if the user logs into one-X Portal for IP Office.

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

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

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

Field	Description
Centralized Call Log	Default = System Default (On)  This setting allows the use of centralized call logging to be enabled or disabled on a per user basis. The default is to match the system setting Default Centralized Call Log On (**System | Telephony | Call Log**). The other options are **On** or **Off** for the individual user. If off is selected, the call log shown on the users phone is the local call log stored by the phone.
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.

Table continues…

Field	Description
Groups	Default = System Default (On).  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.

User Rights | 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.

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.

User Rights | Twinning

This tab is used to set and lock the following settings relating to the use of mobile twinning. Use of mobile twinning requires entry of a mobile twinning license. This tab is no longer available for Release 4.2+.

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
Mobile Dial Delay	Sets and locks the dial delay applied to calls eligible for mobile twinning.
Hunt group calls eligible for mobile twinning	Sets whether mobile twinning is applied to hunt group calls.
Forwarded calls eligible for mobile twinning	Sets whether mobile twinning is applied to forwarded calls.

User Rights | User Rights Membership

The tabs display the users associated with the user rights and allows these to be changed.

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

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

Field	Description
Members of this User Rights	This tab indicates those users associated with the user rights. If the user has an associated Working hours time profile, their association to the user rights applies only during the periods defined by the time profile. If the user does not have an associated Working hours time profile, they are associated with the user rights at all times.
Members when out of service	This tab indicates those users associated with the user rights outside the time periods defined by their Working hours time profile. The Members when out of service tab is not populated unless there are time profiles available within the configuration.

User Rights | Voicemail

The tabs display the users associated with the user rights and allows these to be changed.

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

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

Field	Description
Voicemail On	Default = On When on, the mailbox is used by the system to answer the user's unanswered calls or calls when the user's extension returns busy. Note that selecting off does not disable use of the user's mailbox. Messages can still be forward to their mailbox and recordings can be placed in it. The mailbox can also still be accessed to collect messages.
Voicemail Ringback	Default = Off When enabled and a new message has been received, the voicemail server calls the user's extension to attempt to deliver the message each time the telephone is put down. Voicemail will not ring the extension more than once every 30 seconds.
DTMF Breakout When a caller is directed to voicemail to leave a message, they can be given the option to be transferred to a different extension. The greeting message needs to be recorded telling the caller the options available. The extension numbers that they can be transferred to are entered in the fields below. These system default values can be set for these numbers and are used unless a different number is set within these user settings. The Park & Page feature is supported when the system voicemail type is configured as **Embedded Voicemail** or **Voicemail Pro**. Park & Page is also supported on systems where Avaya Aura Messaging, Modular Messaging over SIP, or CallPilot (for Enterprise Branch with CS 1000 deployments) is configured as the central voice mail system and the local Embedded Voicemail or Voicemail Pro provides auto attendant operation. The Park & Page feature allows a call to be parked while a page is made to a hunt group or extension. This feature can be configured for Breakout DTMF 0, Breakout DTMF 2, or Breakout DTMF 3.	

Table continues…

Field	Description
Reception/ Breakout (DTMF 0)	The number to which a caller is transferred if they press 0while listening to the mailbox greeting rather than leaving a message (***0** on Embedded Voicemail in IP Office mode). For voicemail systems set to Intuity emulation mode, the mailbox owner can also access this option when collecting their messages by dialing ***0**. If the mailbox has been reached through a Voicemail Pro call flow containing a **Leave Mail** action, the option provided when **0** is pressed are: • For IP Office mode, the call follows the **Leave Mail** action's **Failure** or **Success** results connections depending on whether the caller pressed **0** before or after the record tone. • For Intuity mode, pressing **0** always follows the **Reception/Breakout (DTMF 0)** setting. When Park & Page is selected for a DTFM breakout, the following drop-down boxes appear: • **Paging Number –** displays a list of hunt groups and users (extensions). Select a hunt group or extension to configure this option. • **Retries –** the range is 0 to 5. The default setting is 0. • **Retry Timeout –** provided in the format M:SS (minute:seconds). The range can be set in 15-second increments. The minimum setting is 15 seconds and the maximum setting is 5 minutes. The default setting is 15 seconds
Breakout (DTMF 2)	The number to which a caller is transferred if they press 2while listening to the mailbox greeting rather than leaving a message (***2** on Embedded Voicemail in IP Office mode)
Breakout (DTMF 3)	The number to which a caller is transferred if they press 3while listening to the mailbox greeting rather than leaving a message (***3** on Embedded Voicemail in IP Office mode).

User Rights | Forwarding

The tabs display the users associated with the user rights and allows these to be changed.

These settings are mergeable.

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

Field	Description
Block Forwarding	
Enable Block Forwarding	Default = Off. When enabled, call forwarding is blocked. For information on call forwarding, see Forwarding Calls. The following actions are blocked: • Follow me • Forward unconditional

Table continues…

Field	Description
	• Forward on busy • Forward on no answer • Call Coverage • Hot Desking The following actions are not blocked: • Do not disturb • Voicemail • Twinning

ARS

ARS (Alternate Route Selection) replaces LCR (Least Cost Routing) used by previous releases of IP Office. It also replaces the need to keep outgoing call routing short codes in the system short codes.

Related Links

Configuration Mode Field Descriptions on page 193

ARS

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	This value is automatically assigned and cannot be edited.
Route Name	Default = Blank. Range = Up to 15 characters. The name is used for reference and is displayed in other areas when selecting which ARS to use.
Dial Delay Time	Default = System. Range = 1 to 30 seconds.

Table continues…

Field	Description
	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. 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.

Table continues…

Field	Description
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.
100	Invalid IE Contents.
101	Msg Not Compatible.

Table continues…

Code	Cause Code
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.

Location

These settings have changed in release 9.1. View the release 9.0 settings on page 541.

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.

Table continues…

Field	Description
	The subnet mask for this IP address.
Emergency ARS	Default = None. The ARS (Alternate Route Selection) that defines how emergency calls from this location are routed. The drop down list contains all available ARS entries using the format **ARS Route ID: Route Name**. For example **50: Main**.
Parent Location for CAC	Default = None. The options are: • **None** The default setting. • **Cloud** The parent location is an internet address external to the IP Office network. When set to **Cloud**, the **Call Admission Control** (CAC) settings are disabled. Calls to this location from other configured locations are counted as external, yet no CAC limits are applied to the location itself.
Call Admission Control The CAC settings, when not unlimited, restrict the number of calls into and out of the location, The following Call Admission Control settings can be configured.	
Total Maximum Calls	Default = Unlimited. Range = 1 - 99, Unlimited. Limit of all calls to or from other configured locations and the cloud.
External Maximum Calls	Default = Unlimited. Range = 1 - 99, Unlimited. Limit of calls to or from the cloud in this location.
Internal Maximum Calls	Default = Unlimited. Range = 1 - 99, Unlimited. Limit of calls to or from other configured locations in this location.
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	Default is based on the currently selected time zone.

Table continues…

Field	Description
(Start Date — End Date (DST Offset))	Click **Edit** to configure the time and date for DST clock corrections. In the Daylight Time Settings window, you can configure the following information: • **DST Offset**: the number of hours to shift for DST. • **Clock Forward/Back**: Select **Go Forward** to set the date when the clock will move forward. Select **Go Backwards** to set the date when the clock will move backward. • **Local Time To Go Forward**: The time of day to move the clock forward or backward. • **Date for Clock Forward/Back**: Set the year, month and day for moving the clock forwards and backwards. Once you click **OK**, the forward and back dates, plus the DST offset, are displayed using the format **(Start Date — End Date (DST Offset))**.
Fallback System	Default = No override. The drop down list contains all configured IP Office Lines and the associated IP Office system. The group of extensions associated with this location can fallback to the alternate system selected.

Related Links

Configuration Mode Field Descriptions on page 193
Location (9.0) on page 541

Location (9.0)

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.

Table continues…

Field	Description
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**.
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.

Related Links

Location on page 539

Chapter 12: Configure general system settings

System Date and Time

The control unit contains a battery backed clock which is used to maintain system time during normal operation and when mains power is removed.

For files stored on memory cards the system uses the UTC time. For other activities such as call logs, SMDR records, time display on phones; the local time (UTC + any offsets) is used.

The time can be set in a number of ways list below. The method used is set through the **Time Server IP Address** or **Time Setting Config Source** settings on the System | System form.

Simple Network Time Protocol (SNTP - RFC4330) SNTP can be used to make time requests to a list of NTP servers. The response is just a UTC time value, therefore the system has to be configured with the required offset for the local time value and also optional daylight savings values. The time request is sent when the system is started and every hour afterwards.

Voicemail Pro/Manager (TIME RFC868) Both the Voicemail Pro service and the Manager application can act as RF868 time servers, obtaining the time for the PC on which they are running. Use of other RFC868 server sources is not supported. In response to a request from a system, they will provide both the UTC time and local PC time. The time request is sent when the system is started and every 8 hours afterwards.

Warning:

When the Voicemail Pro server is running on the same server as the IP Office, for example a Unified Communication Module or Primary Server, it should not be used at the time source for the IP Office. Either SNTP or manual time setting must be used.

- If you are running Manager when the Voicemail Server starts, then Voicemail does not start as a time server. It is therefore recommended that you have no copy of Manager running when you start or restart the Voicemail Server.
- By default a broadcast address is used. A specific address for the time server that should be used can be set if required.
- When using a time server located in a different time zone from the system, there are two mechanisms for applying an offset to the time. If Manager is acting as the time server, the time offset can be specified through the **Time Offset** of the BOOTP record for the system. Alternatively, the offset can specified in the system configuration using Time Offset (System | System).

Manual Time Control The use of time requests using either of the above methods can be disabled. In that case the time and date used by the system is set manually using a system phone. See Manually Setting the System Time below.

Automatic time updates can be disabled by setting the System | System | Time Setting Config Source to **None**. If automatic time updates are being used, the manual controls below are overridden and only allow display of the time and date information received from the server.

Manually Setting the System Time

For systems without access to a time server, a number of methods to manually set the system time exist. In both cases the user's login code, if set, is used to restrict access to the time and date settings.

1400, 1600, 9500 and 9600 Phones

Phones in these series (excluding the 1403/1603 models) can set the system time and date when the extension user is configured with System Phone Rights. The user is able to access menu options to set the time, date and time offset by selecting **Features | Phone User | System Administration**.

Other Phones

The following method is only supported on these phones: 2410, 2420, 4412, 4424, 4612, 4624, 4610, 4620, 4621, 5410, 5420, 5610, 5620, 5621, 6412, 6424. The phone needs to be configured with a **Self Admin 2** button.

Time Profile

Time Profiles are used by different services to change their operation when required. In most areas where time profiles can be used, not setting a time profile is taken as meaning 24-hour operation.

Time profiles consist of recurring weekly patterns of days and times when the time profile is in effect.

Time profiles can include time periods on specified calendar days when the time profile is in effect. Calendar records can be entered for the current and following calendar year.

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

Time profiles are used by the following record types.

Hunt Group:

A time profile can be used to determine when a hunt group is put into night service mode. Calls then go to an alternate Night Service Fallback group if set, otherwise to voicemail if available or busy tone if not.

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

For automatic voice recording, a time profile can be used to set when voice recording is used.

User:

- Users being used for Dial In data services such as RAS can have an associated time profile that defines when they can be used for that service.
- Users can be associated with a working hours and an out of hours user rights. A time profile can then be used to determine which user rights is used at any moment.
- For automatic voice recording, a time profile can be used to set when that voice recording is used.
- For mobile twinning, a time profile can be used to define when twinning should be used.

Incoming Call Route:

Incoming call routes can also use time profiles to specify when calls should be recorded. Multiple time profiles can be associate with an incoming call route, each profile specifying a destination and fall back destination.

ARS:

ARS forms use time profile to determine when the ARS form should be used or calls rerouted to an out of hours route.

Account Code:

Account Codes can use automatic voice recording triggered by calls with particular account codes. A time profile can be used to set when this function is used.

Auto Attendant :

Embedded voicemail auto attendants can use time profiles to control the different greetings played to callers.

Service:

- A Service can use time profiles in the following ways:
- A time profile can be used to set when a data service is available. Outside its time profile, the service is either not available or uses an alternate fallback service if set.
- For services using auto connect, a time profile can be used to set when that function is used. See Service | Autoconnect.

Server Edition Time Profile Management

For systems in a Server Edition system, any time profiles are shared by all systems in the network.

Related Links

Overriding a Time Profile on page 545

Overriding a Time Profile

You can manually override a time profile. The override settings allow you to mix timed and manual settings.

The override options are as follows:

- **Set Time Profile Active Until Next Timed Inactive**

  Use for time profiles with multiple intervals. Make the time profile active until the next inactive interval.

- **Set Time Profile Inactive Until Next Timed Active**

  Use for time profiles with multiple intervals. Make the time profile inactive until the next active interval.

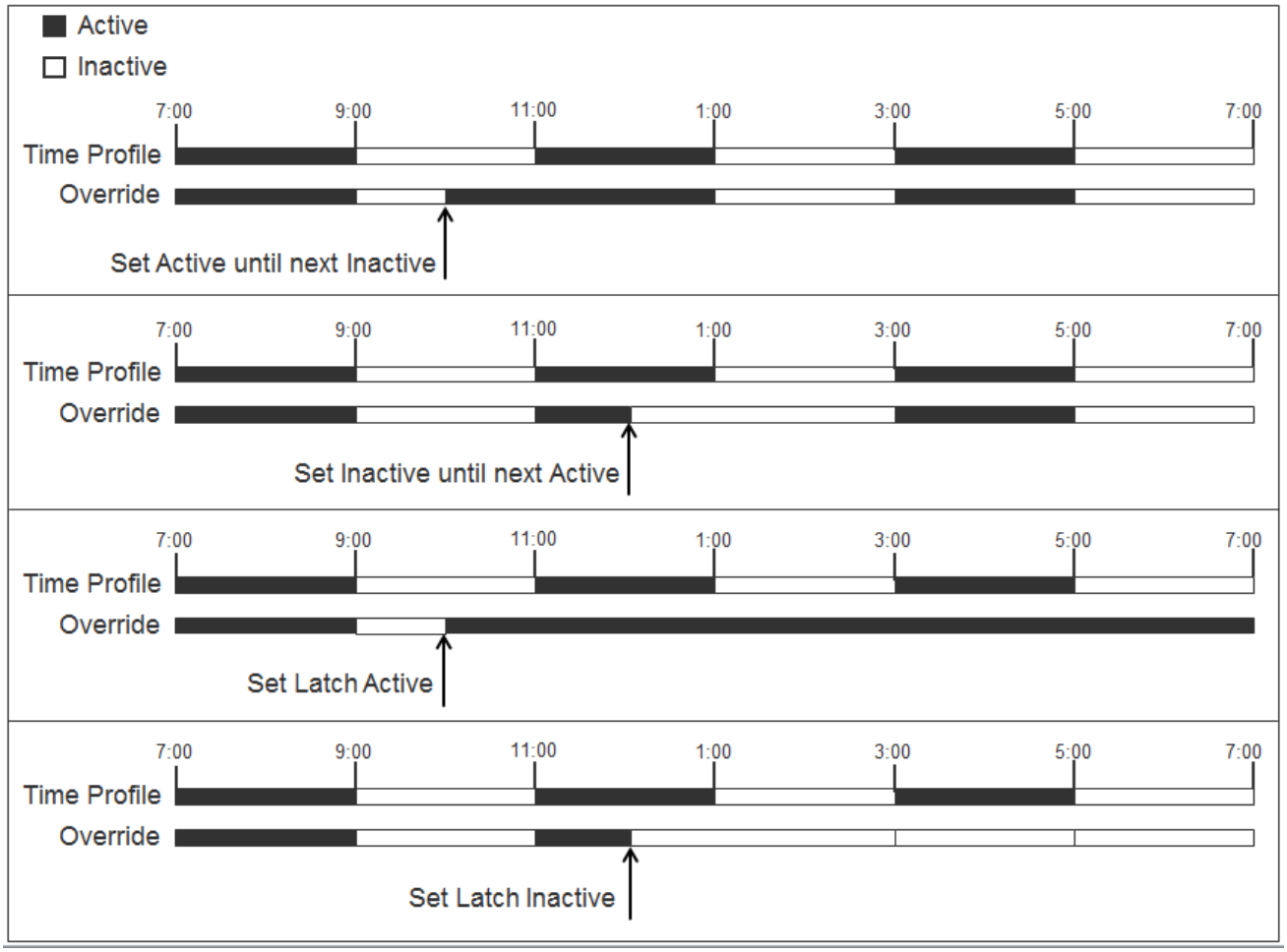
- **Set Time Profile Latch Active**

  Set the time profile to active. Timed inactive periods are overridden and remain active.

- **Set Time Profile Latch Inactive**

  Set the time profile to inactive. Timed active periods are overridden and remain active.

The illustration below provides an example of each override setting.



A time profile can be overridden using the following methods.

- Using the **Override** settings on the Time Profile configuration page.

- Configure short codes for the time profile. See the description for the “Set Time Profile” short code in *Avaya IP Office™ Platform Short Code and Button Action Reference*.
- Configure the Time Profile button action for the time profile. See the description for the “Time Profile” button in *Avaya IP Office Platform™ Short Code and Button Action Reference*.

Related Links

Time Profile on page 544

Working with Templates

The system supports the use of trunk templates. You can use SIP trunk templates to create new SIP trunks. You can use analog trunk templates to update the settings of existing analogue trunks. Avaya service providers can create templates from existing trunks.

Tested SIP Trunk Templates

The SIP trunk services from selected SIP providers are tested as part of the Avaya DevConnect program. The results of such testing are published as Avaya Application Notes available from the Avaya DevConnect web site (https://devconnect.avaya.com).

Standard Mode and Basic Edition SIP Trunk Templates

SIP trunk templates can be used with IP Office systems running all Standard and Basic modes. However, it is important to understand that some trunk parameters used by Standard mode systems are not used by Basic mode systems and vice versa.

The configuration parameters available depend on the mode that you use. When you export a template, Manager displays a warning message if you have configured parameters that are not supported in Basic mode. The warning message provides information about which parameters are not available.

Server Edition Templates

When running in Server Edition mode, Manager supports a number of template options. The settings for the following types of configuration items can be saved as template files. New records of those types can then also be created from a template file.

- User
- Extension (H.323, SIP, IP DECT)
- Hunt Group
- Service
- Tunnel
- Firewall Profile
- Time Profile
- IP Route
- ARS
- Line (H.323, SIP, IP DECT)

These template options are in addition to the existing trunk template options for SIP and analog trunks. The access to the controls detailed below is not affected by the Manager **Enable Template Options** setting.

Saving Template files

Non-Server Edition Systems: Manager in non-Server Edition mode exports templates to a local folder on the PC on which Manager is being run. Templates are stored in a specific Manager sub-folder `\Templates`.

Server Edition Systems: Templates exported from a Server Edition system are saved by default on the Primary Server. This means they are available to other administrators regardless of from which PC they are using Manager.

Related Links

Enabling Template Support on page 548
Importing Trunk Templates on page 548
Creating a Trunk Template on page 549
Creating a New SIP Trunk from a Template on page 549
Applying a Template to an Analog Trunk on page 550
Creating Server Edition Templates on page 550
Creating a New Server Edition Record from a Template on page 551

Enabling Template Support

By default, template support is not enabled.

Procedure

1. Select **File | Preferences**.
2. Select the **Visual Preferences** tab.
3. Select the **Enable Template Options** checkbox.
4. Click **OK**.

Related Links

Working with Templates on page 547

Importing Trunk Templates

For Standard Mode and Basic Edition systems, before you can use templates from another source, they must be placed in the Manager `\Templates` directory. Use this procedure to import a template from another source.

Procedure

1. Select **Tools | Import Templates in Manager**.

2. Browse to the current folder containing the templates that you want to import and select that folder.
3. Click **OK**.
4. Any template files in the folder will be copied to the correct Manager sub-folder.

Related Links

Working with Templates on page 547

Creating a Trunk Template

You can create a trunk template from an existing trunk.

Procedure

1. Select the trunk on which you want to base your template. In the group pane, right click on one of the following options.
   - If you are creating a SIP trunk template, select **Create SIP Trunk Template**.
   - If you are creating an analogue trunk template, select **Generate Analogue Trunk Template**.
2. The trunk settings are displayed in a window. Adjust the trunk settings if required
3. For SIP trunks, click **Create**. For analogue trunks, click **Export**.

Related Links

Working with Templates on page 547

Creating a New SIP Trunk from a Template

A SIP trunk template can be used to create a new SIP trunk record in the system configuration.

Procedure

1. In the navigation or group pane, right click on the any existing line.
2. Click the **New** icon and select **New SIP Trunk from Template**.
3. The template selection menu is displayed.
4. Use the **Locale** and **Service Provider** drop-downs to select the required template.

   If **Display All** is selected, the **Locale** selection changes to **All Locales**.
5. Click on **Create New SIP Trunk**.

Related Links

Working with Templates on page 547

Applying a Template to an Analog Trunk

You can apply an analogue trunk template to existing analogue trunks.

Note:

You must reboot the system for any changes to be applied.

Procedure

1. In the group pane, right click on the analogue trunk and select **Copy Setting from Template**.
2. The template and trunk selection menu is displayed.
3. In the Template Type Selection window, use the **Locale** and **Service Provider** drop-downs to select the required template.

   If **Display All** is selected, the **Locale** selection changes to **All Locales**.
4. Select the trunks to which you want the template to be applied.
5. Click on **Copy Settings**.

Related Links

Working with Templates on page 547

Creating Server Edition Templates

You can save a record shown in the details pane as a template.

Each template file is given a file extension that indicates the template type. For example .usr for a user and .lne for a line. By default the export dialog offers to save a template in the Manager `\manager_files\template` sub-folder (typically `C:\Program Files\Avaya\IP Office \Manager\manager_files\template`). It is recommended that you use this folder as Manager automatically lists the available templates in that folder when creating a new record from a template.

About this task

Procedure

1. Locate and display in the details pane the record that you want to use as a template.
2. Perform one of the following options.
   - In the group pane, right-click on the record and select **Export as Template (Binary)**.
   - In the details pane, click on the  icon in the top-right.

Note:

You cannot use the details pane for **Tunnel** and **Service** records. You must use the group pane.

3. Use the **Save As** window to name and save the template file.

   The file extension indicates the type of template.

Result

Once templates are available, they can be used to create new records in the configuration. Up to a maximum of 50 new entries can be created from a template at any time.

Related Links

Working with Templates on page 547

Creating a New Server Edition Record from a Template

You can use a template to create a new record of the same type as that currently shown.

Procedure

1. Locate and display in the details pane the type of record that you want to create .
2. Perform one of the following options.
   - In the group pane, right-click on the type of record that you want to create and select **New from Template (Binary)**.
   - In the details pane, click on the icon and select **New from Template (Binary)**.

     Note:

     The details pane cannot be used with **Tunnel** and **Service** records.
3. The names of the available templates of the correct type for the record being created and available in Manager's template folder are listed.

   Alternatively, the **Open from file** option can be used to browse to a template file stored in another location.
4. You may be prompted for the number of new configuration entries to create using the selected template.

   In this case, up to 50 new configuration entries can be created at a time.
5. Some template settings may match existing records and will cause immediate validation errors or warnings.

   Correct the fields showing error or warning icons and click **OK**.

Related Links

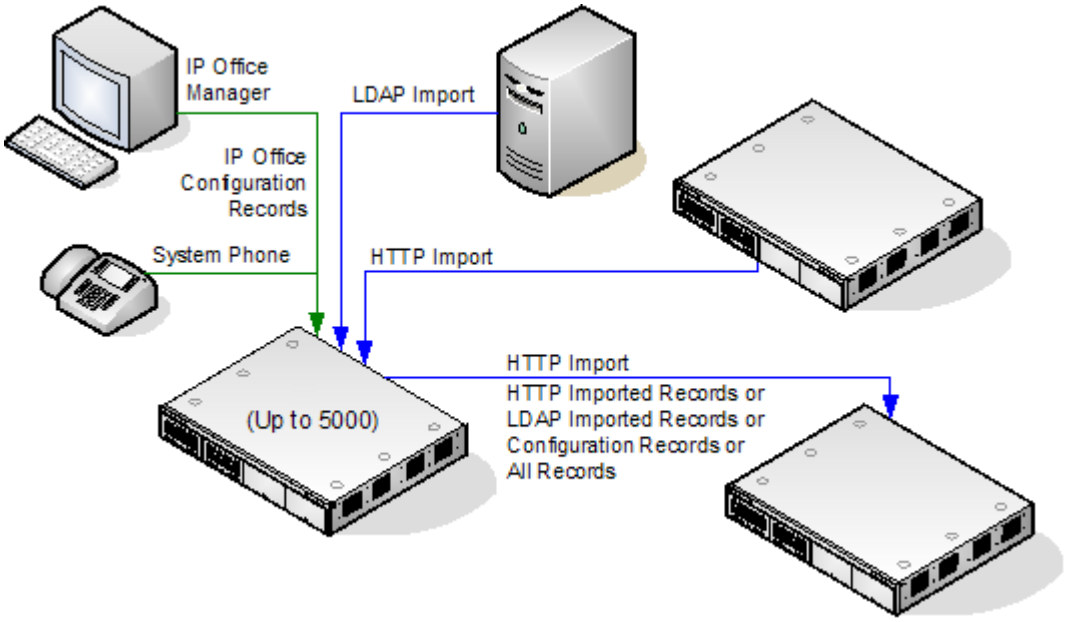
Working with Templates on page 547

Centralized System Directory

Directory services can be used to import directory records (names and numbers) from external sources. These sets of records are regularly re-imported. For systems, the directory records can come from the following sources:

- **LDAP Import** The system can import up to 5000 LDAP records for use within directories shown by user phones and applications. LDAP import is configured through the System | Directory Services | LDAP form. The LDAP used is LDAP Version 2.
- **HTTP Import** Systems are able to import the directory records from another system using HTTP. HTTP import is configured through the System | Directory Services | HTTP form by specifying an IP address or multi-site network connection. The records imported can be any or all of the following record types held by the system from which the records are being imported: LDAP imported records, HTTP imported records, configuration records.
- **System Directory Records (Configuration records)** Up to 2500 records can be entered directly into the system configuration through the Directory menu. System directory records override matching LDAP/HTTP imported records.

Phones with a **CONTACTS** button and System Phone Rights privileges, can add, delete and edit the system directory records of the system at which they are logged in. They cannot edit LDAP or HTTP imported records.



	System	Number of Directory Records			Total Number of Directory Records
		Configuration	LDAP Import	HTTP Import	
Standalone Systems	**IP500 V2**	2500	5000	5000	5000

Table continues…

	System	Number of Directory Records			Total Number of Directory Records
		Configuration	LDAP Import	HTTP Import	
Server Edition	**Primary Server**	2500	5000	–	5000
	Secondary Server	–	–	5000	5000
	Expansion System (L)	–	–	5000	5000
	Expansion System (V2)	–	–	5000	5000

Server Edition Directory Operation

In a Server Edition network, all system directory records are entered into the configuration of the Primary Server. Any LDAP importation is also done by the Primary Server. All other systems are configured by default to import the central directory from the Primary Server.

Use of Directory Records

Directory records are used for two types of functions, directory dialing and caller name matching.

Directory Dialing:

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

The **Dir** function groups directory records shown to the phone user into the following categories. Depending on the phone, the user may be able to select the category currently displayed. In some scenarios, the categories displayed may be limited to those supported for the function being performed by the user:

- **External** Directory records from the system configuration. This includes HTTP and LDAP imported records.
- **Groups** Groups on the system. If the system is in a multi-site network, it will also include groups on other systems in the network. 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 Special Characters

The following characters are supported in directory records. They are supported in both system configuration records and in imported records.

- **? = Any Digit** Directory records containing a **?** are only used for name matching against the dialed or received digits on outgoing or incoming. They are not included in the directory of numbers to dial available to users through their phones or applications. The wildcard can be used in any position but typically would be used at the end of the number.

  In the following example, any calls where the dialed or received number is 10 digits long and starts 732555 will have the display name Homdel associated with them.

  - **Name**: Holmdel
  - **Number**: 9732555????

- **(and) brackets = Optional Digits** These brackets are frequently used to enclose an optional portion of a number, typically the area code. Only one pair of brackets are supported in a number. Records containing digits inside ( ) brackets are used for both name matching or user dialling. When used for name matching, the dialed or received digits are compared to the directory number with and without the ( ) enclosed digits. When used for dialling from a phone or application directory, the full string is dialed with the ( ) brackets removed.

  The following example is a local number. When dialed by users they are likely to dial just the local number. However on incoming calls, for the CLI the telephony provider includes the full area code. Using the ( ) to enclose the area code digits, it is possible for the single directory record to be used for both incoming and outgoing calls.

  - **Name**: Raj Garden
  - **Number**: 9(01707)373386

- **Space and - Characters** Directory records can also contain spaces and - characters. These will be ignored during name matching and dialing from the directory.

Imported Records

Imported directory records are temporary until the next import refresh. They are not added to the system's configuration. They cannot be viewed or edited using Manager or edited by a system phone user. The temporary records are lost if the system is restarted. However the system will

request a new set of imported directory records after a system restart. The temporary records are lost if a configuration containing Directory changes is merged. The system will then import a new set of temporary records without waiting for the **Resync Interval**. If an configuration record is edited by a system phone user to match the name or number of a temporary record, the matching temporary record is discarded.

Importation Rules

When a set of directory records is imported by HTTP or LDAP, the following rules are applied to the new records:

- Imported records with a blank name or number are discarded.
- Imported records that match the name or number of any existing record are discarded.
- When the total number of directory records has reached the system limit, any further imported records are discarded.

	System	Number of Directory Records			Total Number of Directory Records
		Configuration	LDAP Import	HTTP Import	
Standalone Systems	**IP500 V2**	2500	5000	5000	5000
Server Edition	**Primary Server**	2500	5000	–	5000
	Secondary Server	–	–	5000	5000
	Expansion System (L)	–	–	5000	5000
	Expansion System (V2)	–	–	5000	5000

Advice of Charge

The system supports advice of charge (AOC) on outgoing calls to ISDN exchanges that provide AOC information. It supports AOC during a call (AOC-D) and at the end of a call (AOC-E). This information is included in the SMDR output.

AOC is only supported on outgoing ISDN exchange calls. It is not supported on incoming calls, reverse charge calls, QSIG and non-ISDN calls. Provision of AOC signalling will need to be requested from the ISDN service provider and a charge may be made for this service.

For users, display of AOC information is only supported on T3 phones and T3 IP phones.

The user who makes an outgoing call is assigned its charges whilst they are connected to the call, have the call on hold or have the call parked.

If AOC-D is not available, then all indicated by AOC-E are assigned to the user who dialed the call.

If AOC-D is available:

- If the call is transferred (using transfer, unpark or any other method) to another user, any call charges from the time of transfer are assigned to the new user.
- If the call is manually transferred off-switch, the call charges remain assigned to the user who transferred the call.
- If the call is automatically forwarded off switch, subsequent call charges are assigned to the forwarding user.
- AOC-D information will only be shown whilst the call is connected. It will not be shown when a call is parked or held.
- Call charges are updated every 5 seconds.

For conference calls all call charges for any outgoing calls that are included in the conference are assigned to the user who setup the conference, even if that user has subsequently left the conference.

Enabling AOC Operation

1. **Set the System Currency** The Default Currency (System | Telephony | Telephony) setting is by default set to match the system locale. Note that changing the currency clears all call costs stored by the system except those already logged through SMDR.
2. **Set the Call Cost per Charge Unit for the Line** AOC can be indicated by the ISDN exchange in charge units rather than actual cost. The cost per unit is determined by the system using the **Call Cost per Charge Unit** setting which needs to be set for each line. The values are 1/10,000th of a currency unit. For example if the call cost per unit is £1.07, a value of 10700 should be set on the line.
3. **Applying a Call Cost Markup** It may be a requirement that the cost applied to a user's calls has a mark-up (multiplier) applied to it. This can be done using the Call Cost Markup (User | Telephony | Call Settings) setting. The field is in units of 1/100th, for example an entry of 100 is a markup factor of 1.
4. **Enable User AOC Display** By default users do not see call charges. The **Display Charges** setting is used to switch this option on or off. Note that the display of AOC information is only supported on T3 phones.

AOC Short Codes

A number of short code features exist that can be used with AOC. These features can only be used with T3 phones.

AOC Previous Call Displays the call costs of the user's previous call if AOC information was provided with that call.

AOC Total Display the cumulative total cost of the user's calls for which AOC information is available.

AOC Reset Total Set the cumulative total (units and cost) for the user's calls back to zero.

Emergency Call

Manager expects that the configuration of each system should contain at least one short code that is set to use the **Dial Emergency** feature. If no such short code is present in the configuration then Manager will display an error warning. The importance of the **Dial Emergency** feature is that it overrides all external call barring that may have been applied to the user whose dialing has been matched to the short code. You must still ensure that no other short code or extension match occurs that would prevent the dialing of an emergency number being matched to the short code.

The short code (or codes) can be added as a system short code or as an ARS record short code. If the **Dial Emergency** short code is added at the solution level, that short code is automatically replicated into the configuration of all servers in the network and must be suitable for dialing by users on all systems. Separate **Dial Emergency** short codes can be added to the configuration of an individual system. Those short codes will only be useable by users currently hosted on the system including users who have hot desked onto an extension supported by the system.

Determining the Caller's Location

It is the installers responsibility to ensure that a **Dial Emergency** short code or codes are useable by all users. It is also their responsibility to ensure that either:

the trunks via which the resulting call may be routed are matched to the physical location to which emergency service will be despatched

or

the outgoing calling line ID number sent with the call matches the physical location from which the user is dialing.

Hot Desking Users

In addition to the location requirements above, you must also remember that for users who hot desk, from the networks perspective the user's location is that of the system hosting the extension onto which the user is currently hot desked. If that is an IP extension then that location is not necessarily the same as the physical location of the server.

Emergency call setup

Routing of emergency calls is based on a call resolving to a Dial Emergency short code. Based on the location value for the extension making the call, routing is performed as configured in the Emergency ARS. Emergency calls have maximum priority and are not delayed in any way.

Configuring emergency call routing

Create a Dial Emergency system short code. See Dial Emergency.

Note that the **Line Group ID** value in the Dial Emergency short code is the fallback route. If the system cannot find a location or an Emergency ARS, it will try to use the **Line Group ID** to route the call.

1. Create an ARS containing a Dial short code or a Dial Emergency short code. See ARS.
2. Create a Location and set the **Emergency ARS** to the ARS created in step 2. See Location.

3. Open the **Extn** tab for an extension that will use the location defined in step 3 and set the **Location** value to the location defined in step 3. Note that once you define a location, you must set a system **Location** value on the System | System page.

For non-IP based extensions, the system location value is used as the default. For IP based extensions, the location value is set to Automatic. An attempt is made to match the extension's IP address to the subnet configured in the location. If the match is cannot be made, the location value defaults to the system location value.

From the extension used in step 3, dial the Dial Emergency short code. IP Office checks the location value and determines the emergency ARS set for the location. Once the emergency ARS is found, IP Office will try to match the Telephone Number in the Dial Emergency short code to a short code in the ARS and use it to make the emergency call.

Fax Relay

Group 3 Fax is the common standard for fax transmission over analog and digital (TDM) phone lines. However, the sending of fax calls over IP lines is not normally possible or proves unreliable due to the distortion caused during encoding of the audio signal. However some SIP line providers support fax using specific codecs.

For a system with an IP500 VCM. IP500 VCM V2 or IP500 Combo cards, **T38** or **G.711** can be selected for fax over SIP lines. T38 Fax Relay is a public set of protocols that allow fax calls to be reliable transported over IP connections that have a T38 Fax gateway at each end. **T38** is not supported by Linux based systems.

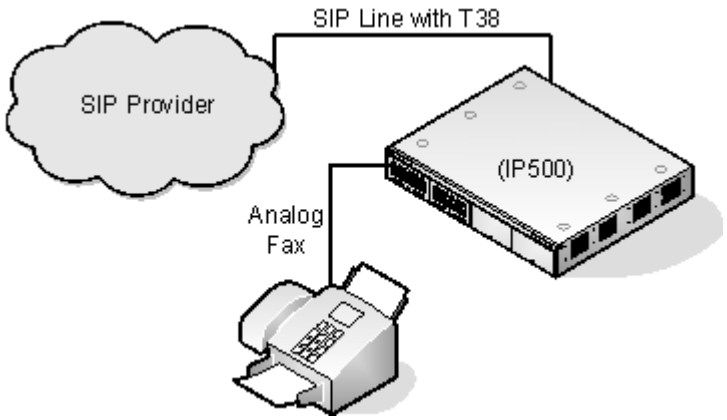
T38 Fallback can also be selected. On outgoing fax calls, if the called destination does not support T38, a re-invite it sent for fax transport using **G.711**.

Fax support is enabled using the SIP line's **Fax Transport Support** setting. Within a multi-site network, **Fax Transport Support** can also be enabled on the H.323 IP lines between the systems. This allows fax calls at one system to be sent to another system.

Both system SIP extensions and system SIP lines can be configured for T38. They can then be used as the point at which fax calls are sent and or received. Each fax call uses a VCM channel. The SIP line or extension must support Re-Invite. In addition, the existing system Fax Transport Support can still be used to transport the faxes over a multi-site network. That includes faxes being made or received via a SIP line or extension. The conversion from T38 or G.711 to multi-site network or vice versa requires two VCM channels.

Scenario 1

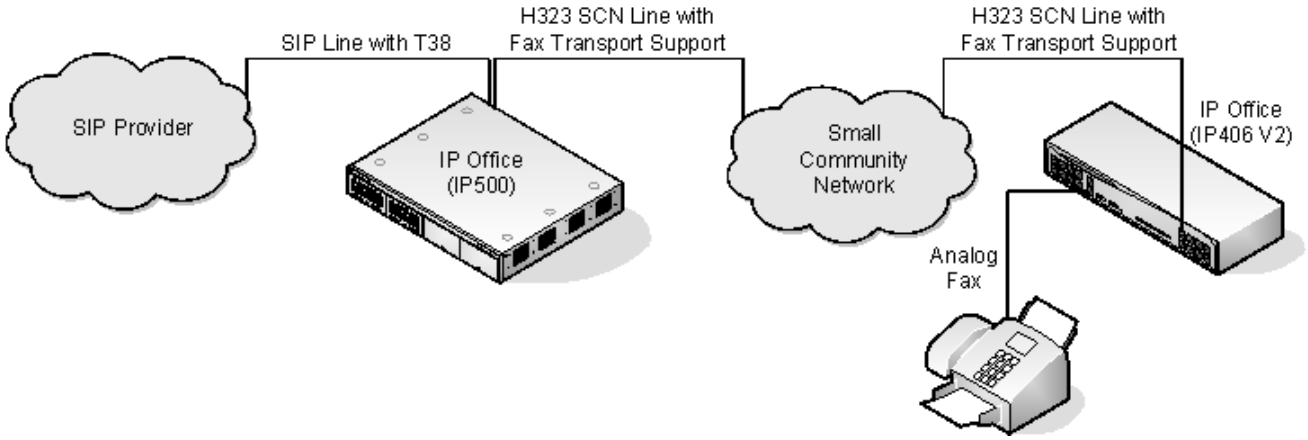
In this scenario, the SIP provider supports T38. By configuring the system's SIP line for T38 operation, the analog fax machine attached to the system can make and receive fax calls via the SIP provider.



Scenario 2

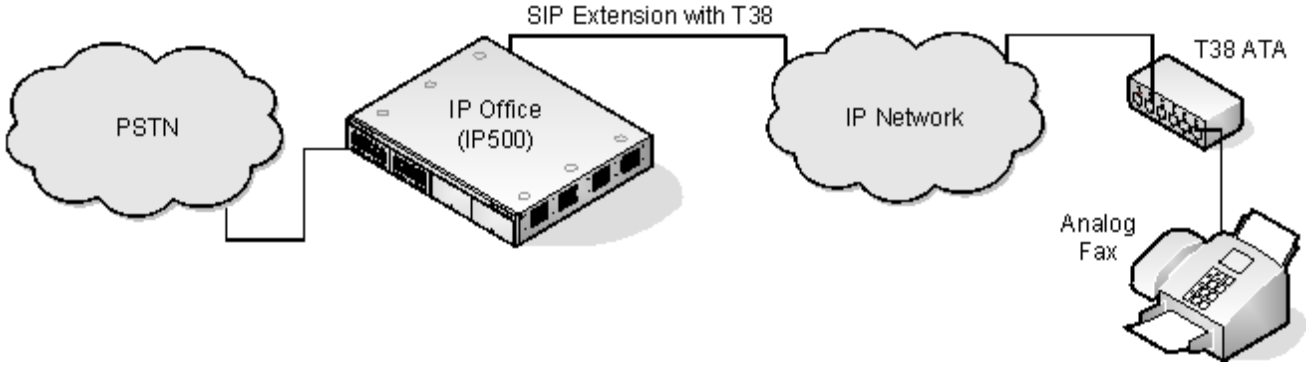
This scenario is similar to the previous. However, fax calls via the SIP line are also transported across the multi-site network to a fax machine attached to another system in the network. In this scenario, on the IP500, 2 VCM channels are used for the T38 fax call.

This method is also significant in that it allows non-IP500 systems running Release 5 to make use of SIP lines for fax.



Scenario 3

In this scenario, an ATA (Analog Telephone Adaptor) that supports T38 is used to connect the fax machine as a SIP extension on the system.



System Requirements for T38

IP500 V2 system with an IP500 VCM, IP500 VCM V2 or IP500 Combination card.

The SIP line or extension must support **Re-Invite**.

Outgoing Fax Calls

When sending a fax via T38, the call must be correctly indicated as being (or potentially being) a fax call. This can be done in 2 ways.

Analog Fax Extension Setting For an analog fax device, the extension's Equipment Classification setting (Extension | Analog) can be set to **FAX Machine**.

Dial Fax Short Code Calls can be routed to a Dial Fax short code which has the SIP line as its destination.

Caller Display

Caller display displays details about the caller and the number that they called. On internal calls, the system provides this information. On external calls it uses the Incoming Caller Line Identification (ICLID) received with the call. The number is also passed to system applications and can be used for features such as call logging, missed calls and to make return calls.

Analog extension can be configured for caller display via the system configuration (Extension | Extn | Caller Display Type).

Adding the Dialing Prefix Some systems are configured to require a dialing prefix in front of external numbers when making outgoing calls. When this is the case, the same prefix must be added to the ICLID received to ensure that it can be used for return calls. The prefix to add is specified through the Prefix field of each line.

Directory Name Matching The system configuration contains a directory of names and numbers. If the ICLID of an incoming call matches a number in the directory, the directory name is associated with that call and displayed on suitable receiving phones.

Applications such as SoftConsole also have directories that can be used for name matching. If a match occurs, it overrides the system directory name match for the name shown by that application.

Extended Length Name Display

In some locales, it may be desirable to change the way names are displayed on phones in order to maximize the space available for the called or calling name. There are two hidden controls which can be used to alter the way the system displays calling and called information.

These controls are activated by entering special strings on the Source Numbers tab of the NoUser user. These strings are:

LONGER_NAMES This setting has the following effects:

- On DS phones, the call status display is moved to allow the called/calling name to occupy the complete upper line and if necessary wrap-over to the second line.

- For all phone types:
- On incoming calls, only the calling name is displayed. This applies even to calls forwarded from another user.
- On outgoing calls, only the called name is displayed.

HIDE_CALL_STATE This settings hides the display of the call state, for example **CONN** when a call is connected. This option is typically used in conjunction with **LONGER_NAMES** above to provide additional space for name display.

Parking Calls

Parking a call is an alternative to holding a call. A call parked on the system can be retrieved by any other user if they know the system park slot number used to park the call. When the call is retrieved, the action is known as Unpark Call or Ride Call. While parked, the caller hears music on hold if available.

Each parked call requires a park slot number. Attempting to park a call into a park slot that is already occupied causes an intercept tone to be played. Most park functions can be used either with or without a specified park slot number. When parking a call without specifying the park slot number, the system automatically assigns a number based on the extension number of the person parking the call plus an extra digit 0 to 9. For example if 220 parks a call, it is assigned the park slot number 2200, if they park another call while the first is still parked, the next parked call is given the park slot number 2201 and so on.

Park slot IDs can be up to 9 digits in length. Names can also be used for application park slots.

The **Park Timeout** setting in the system configuration (System | Telephony | Telephony | Park Timeout) controls how long a call can be left parked before it recalls to the user that parked it. The default time out is 5 minutes. Note that the recall only occurs if the user is idle has no other connected call.

There are several different methods by which calls can be parked and unparked. These are:

Using Short Codes

The short code features, Call Park and Unpark Call, can be used to create short codes to park and unpark calls respectively. The default short codes that use these features are:

- *37*N# - Parks a call in park slot number N.
- *38*N# - Unparks the call in park slot number N.

Using the SoftConsole Application

The SoftConsole application supports park buttons. SoftConsole provides 16 park slot buttons numbered 1 to 16 by default.

The park slot number for each button can be changed if required. Clicking on the buttons allows the user to park or unpark calls in the park slot associated with each button. In addition, when a call is

parked in one of those slots by another user, the application user can see details of the call and can unpark it at their extension.

Using Programmable Buttons

The Call Park feature can be used to park and unpark calls. If configured with a specified park slot number, the button can be used to park a call in that slot, unpark a call from that slot and will indicate when another user has parked a call in that slot. If configured without a number, it can be used to park up to 10 calls and to unpark any of those calls.

Phone Defaults

Some telephones support facilities to park and unpark calls through their display menu options (refer to the appropriate telephone user guide). In this case parked calls are automatically put into park slots matching the extension number.

Configuring Call Access Control

Call Admission Control (CAC) is a method of controlling system resources using defined locations. Calls into and out of each location are allowed or disallowed based upon configured call constraints. In Manager, use the **Location** tab to define a location and configure the maximum calls allowed for the location.

Related Links

Manager location tab on page 562
Assigning a network entity to a location on page 563
System actions at maximum call threshold on page 563
Example on page 564

Manager location tab

Configuring location settings

On the Manager **Location** tab, set the following parameters for a location:

- Location Name
- Subnet Address
- Subnet Mask

Configuring Call Access Control settings

On the Manager Location tab, set the following CAC parameters:

- **Internal Maximum Calls**: Calls that pass from the location to another configured location.
- **External Maximum Calls**: Calls that pass from the location to an unmanaged location.
- **Total Maximum Calls**: The total internal and external calls permitted.

Related Links

Configuring Call Access Control on page 562

Assigning a network entity to a location

The **Location** field is a drop down list of locations defined on the **Location** tab. Network entities are assigned to a location using the **Location** field on the following Manager tabs.

- **System**
- **Extension**
- **SIP Line | VoIP**
- **H323 Line | VoIP**

The following default settings are applied.

- Each IP Office system can be configured with a defined location. For Server Edition deployments, the configuration of locations is done solution wide. All IP Office systems in the solution share the same location configuration.
- Digital phones default to the system location.
- The default setting for IP phones is **Automatic**. Phones registering from a subnet matching that of a location will be treated as within that location. Otherwise, the phone is assigned the same location as the system. Cloud can be used for phones whose Location is variable or unknown.
- IP Lines default to **Cloud**.

Related Links

Configuring Call Access Control on page 562

System actions at maximum call threshold

- A congestion alarm is raised.
- Calls that exceed the CAC maximum values are not allowed.
- Calls from extensions to public trunks through Alternate Route Selection (ARS) are queued and display **Waiting for Line**.
- Calls from extensions to public trunks which do not route through ARS receive a fast-busy tone and display **Congestion**.
- Idle phones display **Emergency/Local calls only**.
- Alternative routing to a local PSTN gateway follows ARS priority escalation rules.
- SIP calls that would exceed call limits and have no other targets are declined with **cause=486** or **cause = 503**.

Allowed calls

When CAC limits have been reached, the following calls are allowed.

- Emergency calls are always allowed.
- Established calls are never torn down to achieve limits.
- A phone on a remote site that parks a call is always allowed to retrieve it.
- Request Coaching Intrusion calls are allowed.

Related Links

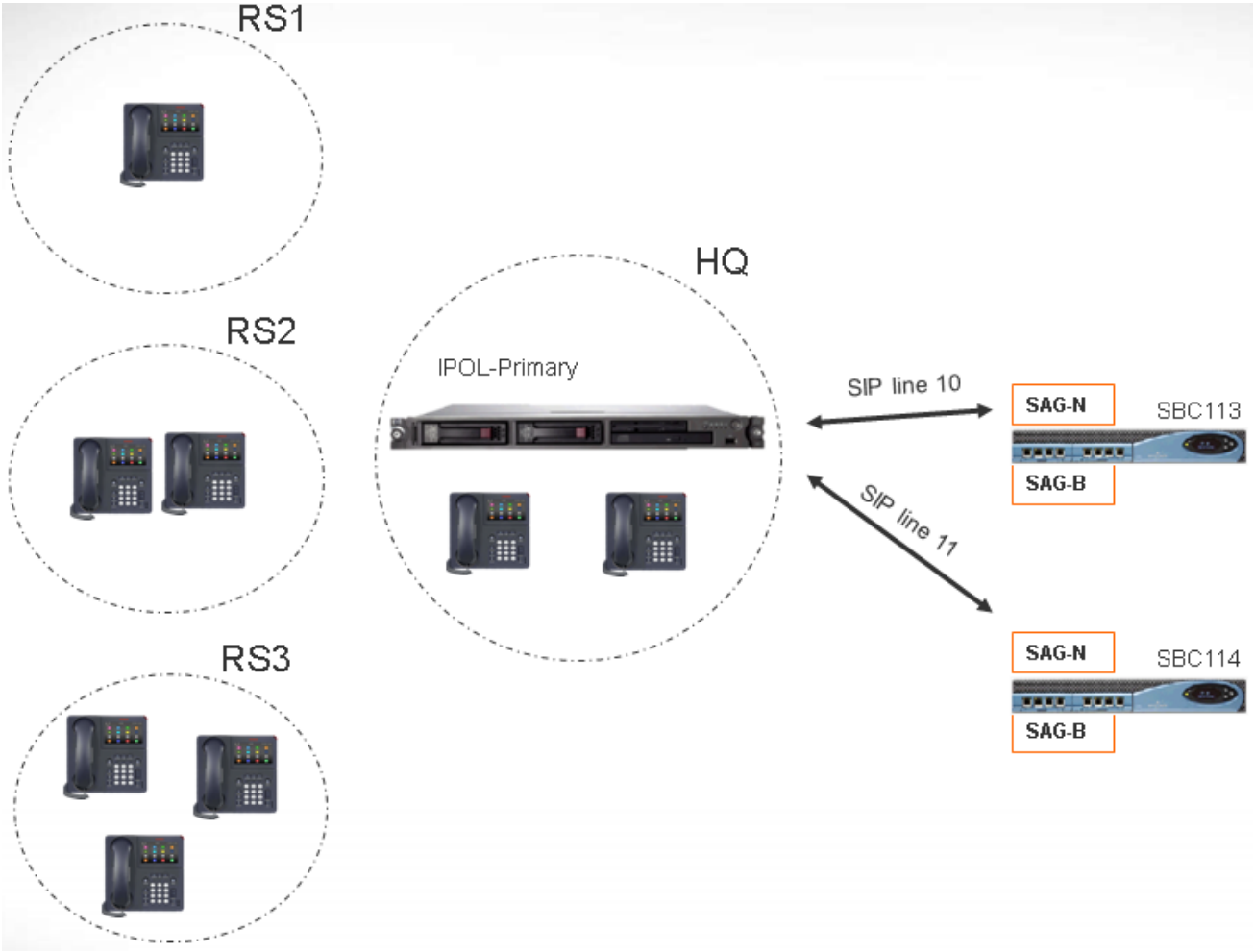
Configuring Call Access Control on page 562

Example

The example configuration has four locations.

Location	Max Calls
HQ	20
RS1	5
RS2	10
RS3	15
+Cloud	unlimited

SIP Line 10 and SIP Line 11 are configured with 20 channels.



Notes

- Calls between locaton RS1 and SBC113 do not increment the call count for HQ.
- The HQ call count includes calls across the HQ boundary which anchor media inside HQ. SBC113 and SBC 114 are both included.
- The HQ maximum calls value is separate and complementary to the individual trunk call maximum.
- Incoming calls from SIP to RS1 (direct media) only need to verify that the RS1 location maximum call value is not exceeded.
- SIP calls that are not allowed to RS1 may go to HQ voicemail if the HQ call limit is not exceeded.

Related Links

Configuring Call Access Control on page 562

Ring Tones

Ring tones can be defined in the following terms:

- **Distinctive Ringing - Inside, Outside and Ringback** A distinctive ring tone can be given for each of the different call types: an internal call, an external call and a ringback calls (voicemail calls, ringback when free calls, calls returning from park, hold or transfer).
  - The distinctive ringing patterns used for most non-analog phones are as follows:
    - **Internal Call**: Repeated single-ring.
    - **External Call**: Repeated double-ring.
    - **Ringback Call**: Repeated single-ring followed by two short rings.
  - For analog extensions, the ringing pattern used for each call type can be set through the system configuration in Manager. This is done using the settings on System | Telephony | Tones & Music and or User | Telephony | Call Settings tabs.
  - For non-analog extension the ringing pattern used for each call type by the system is not configurable.
- **Personalized Ringing** This term refers to control of the ringing sound through the individual phones. For non-analog phones, while the distinctive ringing patterns cannot be changed, the ringer sound and tone may be personalized depending on the phone's own options. Refer to the appropriate telephone user guide.

Analog Phone Ringing Patterns

For analog phone users, the distinctive ringing pattern used for each call type can be adjusted. From the System | Telephony | Tones & Music tab, the default ring tone for each call type can be configured. The setting for an individual user associated with the analog extension can be altered from the system default through the User | Telephony | Call Settings tab.

Note that changing the pattern for users associated with fax and modem device extensions may cause those devices to not recognize and answer calls.

The selectable ringing patterns are:

- **RingNormal** This pattern varies to match the **Locale** set in the **System | System** tab. This is the default for external calls.
- **RingType1**: 1s ring, 2s off, etc. This is the default for internal calls.
- **RingType2**: 0.25s ring, 0.25s off, 0.25s ring, 0.25s off, 0.25s ring, 1.75s off, etc. This is the default for ringback calls.
- **RingType3**: 0.4s ring, 0.8s off, …
- **RingType4**: 2s ring, 4s off, …
- **RingType5**: 2s ring, 2s off, …
- **RingType6**: 0.945s ring, 4.5s off, …
- **RingType7:** 0.25s ring, 0.24 off, 0.25 ring, 2.25 off, …

- **RingType8**: 1s ring, 3s off, …
- **RingType9**: 1s ring, 4s off, …
- **RingType0**: Same as **RingNormal** for the United Kingdom locale.
- **Default Ring**: Shown on the User | Telephony | Call Setting tab. Indicates follow the settings on the System | Telephony | Tones & Music tab.

Media Connection Preservation

Media Connection Preservation maintains calls that experience end-to-end signaling loss or refresh failures that still have an active media path. The call is put into a Preserved state and a Preservation Interval timer is started on IP Office for that call. The maximum duration of a preserved call is two hours. Once put into the Preserved state, a call can only transition to the Terminated state. Call restoration is not supported.

Only the following call types are preserved:

Connected active calls

Two party calls where the other end is a phone, trunk, or voicemail

Conference calls

Calls on hold and calls to hunt groups are not preserved.

Phone Display

When a call is a preserved state but the phone's local signalling connection with it's host IP Office is still present, the phone call state display is prefixed with (!). Hold, transfer, and conference soft keys are not displayed. For signalling loss between the phone and host IP Office, only Avaya H.323 phones that support connection preservation will maintain the call. The phone display will not be updated and the only permitted action will be to terminate the call.

Configuration

When enabled on the System | Telephony | Telephony tab, Media Connection Preservation is applied at a system level to SCN trunks and Avaya H.323 phones that support connection preservation. All systems in a Small Community Network (SCN) must be enabled for end to end connection preservation to be supported.

When enabled on the Line | SM | Session Manager tab, Media Connection Preservation is applied to Enterprise Branch deployments. Media Connection Preservation preserves only the media and not the call signaling on the SM Line. Media Connection Preservation does not include support for the Avaya Aura Session Manager Call Preservation feature.

When enabled on the Line | SIP Line tab, Media Connection Preservation is applied to the SIP trunk. The value of connection preservation on public SIP trunks is limited. Media Connection Preservation on public SIP trunks is not supported until tested with a specific service provider. Media Connection Preservation is disabled by default for SIP trunks.

Music On Hold

Each system can provide music on hold (MOH) from either internally stored files or from externally connected audio inputs. Up to 4 different hold music sources are supported.

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

Related Links

System Source on page 568
Alternate Source on page 569

System Source

The first source is called the **System Source**. This source is numbered source 1. The possible options for this source are:

- **WAV**: A file called `holdmusic.wav` downloaded by the system.
- **External**: For IP 500 v2 systems, use the audio source connected to the back of the control unit. For Linux systems, the first available USB source is used.
- **Tone**: A double beep tone. Used automatically if the System Source is set to WAV and the **holdmusic.wav** file has not been successfully downloaded.

WAV Files

The system can use internal music on hold files that it stores in its non permanent memory. The file properties should be: PCM, 8kHz 16-bit, mono, maximum length 90 seconds (30 seconds on non-IP500 systems, 600 seconds on Linux based systems). If the file downloaded is the incorrect format, it will be discarded from memory after the download.

The files, when specified by the system source or an alternate source setting, are loaded as follows:

- Following a reboot, the system will try using TFTP to download the file or files.
- The initial source for TFTP download is the system's configured **TFTP Server IP Address** (**System | System | LAN Settings**). The default for this is a broadcast to the local subnet for any TFTP server.
- Manager can act as a TFTP server while it is running. If Manager is used as the TFTP server, then the wav file or files should be placed in the Manager applications working directory.
- On Linux based systems, if no successful TFTP download occurs, the system will automatically look for the files in `opt/ipoffice/tones/mohwavdir`.
- The name of the system music .wav file should be **holdmusic.wav**. The name of alternate source .wav files should be as specified in the **Alternate Sources** table (**System | Telephony | Tones and Music**) minus the **WAV**: prefix.

WAV File Download and Storage:

- If no successful TFTP download occurs, the system will automatically look for the file on the control unit's memory card (in the system/primary folder) and will download it from there if found. On Linux based systems, if no successful TFTP download occurs, the system will

automatically look for the file on the server's disk in the `opt/ipoffice/system/primary` folder and will download it from there if found.

- If a music on hold file is downloaded, the system will automatically write a copy of that file to its memory card if present. This will overwrite any existing file of the same name already stored on the card.
- For files downloaded from a System SD card, the system will download the file again if the SD card is shutdown and restarted or if files are copied to the card or uploaded using File Manager.
- If a music on hold file is downloaded via TFTP, the system will automatically write a copy of that file to its disk. This will overwrite any existing file of the same name already stored on the disk.
- The system will download the file again if new files are copied to the disk or uploaded using File Manager.

Tone

If no internal music on hold file is available and **External** is not selected as the **System Source**, then the system will provide a default tone for music on hold. The tone used is double beep tone (425Hz repeated (0.2/0.2/0.2/3.4) seconds on/off cadence). **Tone** can be selected as the **System Source**, overriding both the use of the external source port and the downloading of **holdmusic.wav**.

Related Links

Music On Hold on page 568

Alternate Source

The names of up to 3 alternate sources can be specified on the **System | Telephony | Tones & Music** tab. The available options depends on the system type.

Alternate Option	Linux	IP 500 V2
WAV:<filename>	• The <filename> parameter specifies the filename to be played. • <filename>: - can be up to 27 IA5 characters - cannot contain spaces - any extension is allowed - case sensitive • A TFTP read is attempted first, then the file location: `opt/ipoffice/system/primary`. • When a MOH source is activated, the playback resumes from where it left off last time, instead of starting every time from the beginning.	• The <filename> parameter specifies the filename to be played. <filename>: - can be up to 27 IA5 characters - cannot contain spaces - any extension is allowed - case sensitive • A TFTP read is attempted first, then the file location: `/system/primary`. • The WAV file is continuously played and connected to calls as required. • At any moment, all users listening to a given MOH source will hear the

Table continues…

Alternate Option	Linux	IP 500 V2
	• At any moment, all users listening to a given MOH source will hear the same thing (instead of every user hearing from a different file position). • This is a streamed source suitable for use with the **LINE** option.	same thing (instead of every user hearing from a different file position).
XTN: <extension>	N/A	Any analog extension with its Equipment Classification set as MOH Source can be entered as the alternate source. Enter XTN: followed by the extension's Base Extension number. For example XTN:224
WAVRST:<filename>	• The <filename> parameter specifies the filename to be played. • A TFTP read is attempted first, then the file location: `opt/ipoffice/system/primary`. • When a MOH source is activated, the playback is started every time from the beginning. • At any moment, all users listening to a given MOH source will hear a different WAV file or file position.	N/A
WAVDIR:	• No additional parameter is required. • The directory used is `opt/ipoffice/tones/mohwavdir`. • Up to 255 files, up to 10 minutes per file. • The files are played in filename order (numerical, lower then upper case). • When a MOH source is activated, the playback resumes from where it left off last time. • At any moment, all users listening to a given MOH source will hear the same thing. • There can only be one WAVDIR: or WAVDIRRST: entry per system. • This is a streamed source suitable for use with the **LINE** option.	N/A
WAVDIRRST:	• No additional parameter is required. • Directory used is `opt/ipoffice/tones/mohwavdir`.	N/A

Table continues…

Alternate Option	Linux	IP 500 V2
	• Up to 255 files, up to 10 minutes per file. • The files are played in filename order (numerical, lower then upper case). • When a MOH source is activated, the playback is started every time from the beginning. • At any moment, all users listening to a given MoH source will hear a different WAV file or file position. • There can only be one WAVDIR: or WAVDIRRST: entry per system.	
USB: <number>	• The <number> parameter is the logical USB device number. • USB:1 is the first source found and is automatically used for the System Source when set to External. • Additional devices are numbered sequentially. For example, USB:2, USB:3 • IPOffice will auto-configure USB sound devices with settings that work well in most cases. Line input is selected and volume is set close to maximum. If no line input is identified on the card, microphone input is used instead. • The following USB audio devices have been tested: - Creative X-FI GO Pro USB - Asus Xonar U3 Any ALSA conformant USB sound card should work • External USB sound devices are hot-pluggable. They can be added and removed from the system at any time. • Care should be taken when adding or removing USB sound cards as this may change the logical number. • When an USB MOH source becomes unavailable, the default MOH tone will be played instead. • A USB MOH source is not supported on virtual servers.	N/A

Table continues…

Alternate Option	Linux	IP 500 V2
	• This is a streamed source suitable for use with the **LINE** option.	
LINE:<X,Y>	This option is applicable to both Linux and IP 500 V2 systems. • Two parameters are supplied. - X = SCN line number to the Linux Server (not outgoing group ID). - Y = The MOH source number on the Linux Server. • The Linux Server is typically the Primary, but the Secondary Server can be used. • The MOH Source must be a stream type (Not WAVRST: or WAVDIRRST:) • Centralised MOH will place a VoIP call to the MOH source when MOH is required. • Takes one call capacity from the trunk and therefore, can be subject to CAC limits. • Uses the SCN trunks' codec preferences. • G.729 not recommended (better results are achieved with G.711). • Calls are dropped after 30s of no use. • If 30s is not appropriate, it can be changed with the NoUser source number HOLD_MUSIC_TIMEOUT=x, where x is number of seconds (range = 0 and 600). 0 means never tear down the call (and never retry – should not be used!) • The status displayed in SSA • Note that as this option can only be specified as an alternate source, centralized MOH cannot be used as the System Source. That is, it cannot be used for internal calls' MOH.	

Controlling the Music on Hold Source Used for Calls

Unless specified, the System Source is used for any calls put on hold by system users. For any call, the last source specified for the call is the one used. The following options allow the source to be changed.

- **Hunt Group** Each hunt group can specify a **Hold Music Source** (**Group | Group**). That source is then used for calls presented to the hunt group.

  In a multi system network, a hunt group member will hear the music on hold (MOH) from their local system. For example, a call comes in to site A and rings a hunt group with members from system A and system B. If a hunt group member from system B answers the call, they hear the MOH from system B.

- **Incoming Call Route** Each incoming call route can specify a **Hold Music Source** (**Incoming Call Route | Standard**). That source is then used for incoming calls routed by that incoming call route.

- **Short Code** The **h** character can be used in the **Telephone Number** field of short codes to specify the hold music to associate with calls routed by that short code. The format **h(X)** is used where **X** is the source number. This method can be used to specify a hold music source for outgoing calls.

Checking Music on Hold

The system short code feature Hold Music can be used to listen to the hold music sources. Dial ***34N#**, replacing **N** with the source number 1 (System Source) or 2 to 4 (Alternate Sources).

Related Links

Music On Hold on page 568

Conferencing

The IP Office system supports a number of conference features and allows multiple simultaneous conferences.

Conference Types

There are 2 types of conference supported by the system:

- **Ad-Hoc Conferencing** An ad-hoc conference is one created on the fly, typically by holding an existing call, making another call and then pressing a conference key on the phone. Other people can be added to the conference by repeating the process.
- **Meet Me Conferencing** Conference Meet Me allows users to join or start a specific numbered conference. This method of operation allows you to advertise a conference number and then let the other parties join the conference themselves.

User Personal Conference Number Each user's own extension number is treated as their own personal conference number. Only that user is able to start a conference using that number as the conference ID. Any one else attempting to start a conference with that number will find themselves in a conference but on hold until the owner also joins. Personal conferences are always hosted on the owner's system. Note, when a user calls from their mobile twinned number, the personal conference feature will only work if they access the conference using an FNE 18 service.

Conference Notes

Other Uses of Conference Resources System features such as call intrusion, call recording and silent monitoring all use conference resources for their operation. On IP500 V2 systems, each Embedded Voicemail call in progress also reduces the conference capacity.

Automatically Ending Conferences The behavior for the system automatically ending a conference varies as follows:

- A conference remains active until the last extension or trunk with reliable disconnect leaves. Connections to voicemail or a trunk without reliable disconnect (for example an analog loop-start trunk) will not hold a conference open.
- The **Drop External Only Impromptu Conference** setting controls whether a conference is automatically ended when the last internal party exits the conference.

Analog Trunk Restriction In conferences that include external calls, only a maximum of two analog trunk calls are supported. This limit is not enforced by the system software.

Recording Conferences If call recording is supported, conference calls can be recorded just like normal calls. Note however that recording is automatically stopped when a new party joins the conference and must be restarted manually. This is to stop parties being added to a conference after any "advice of recording" message has been played.

IP Trunks and Extensions Conferencing is performed by services on the system's non-IP interface. Therefore a voice compression channel is required for each IP trunk or extension involved in the conference.

Call Routing A short code routing calls into a conference can be used as an Incoming Call Route destination.

Conference Tones The system provides conference tones. These will be either played when a party enters/leaves the conference or as a regularly repeated tone. This is controlled by the Conferencing Tone (**System | Telephony | Tones & Music**) option.

Related Links

Conference Phones on page 574
Ad-Hoc Conferencing on page 575
Meet Me Conferencing on page 576
Routing External Callers on page 578
Context Sensitive Conferencing on page 578

Conference Phones

The system does not restrict the type of phone that can be included in a conference call.

Use Mute When not speaking, use of the mute function helps prevent background noise from your location being added to the conference call. This is especially important if you are attempting to participate handsfree.

Handsfree Participation While many Avaya telephones can be used fully handsfree during a call, that mode of operation is intended only for a single user, seated directly in front of the phone. Attempting to use a handsfree phones for multiple people to listen to and participate in a call will rarely yield good results. See below for details of conference phones supported by the system.

Dedicated Conference Phones

To allow multiple people in one room to speak and listen to a conference call, the system supports the following conference phones:

- B100 Conference Phones (B149, B159 and B179).
- Audio Conferencing Unit (ACU).

Group Listen

The **Group Listen** function can be used via a programmable button or short code. It allows the caller to be heard through a phones handsfree speaker while only being talked to via the phone's handset.

Related Links

Conferencing on page 573

Ad-Hoc Conferencing

Conference add controls can be used to place the user, their current call and any calls they have on hold into a conference. When used to start a new conference, the system automatically assigns a conference ID to the call. This is termed ad-hoc (impromptu) conferencing.

If the call on hold is an existing conference, the user and any current call are added to that conference. This can be used to add additional calls to an ad-hoc conference or to a meet-me conference. Conference add can be used to connect two parties together. After creating the conference, the user can drop from the conference and the two incoming calls remain connected.

Related Links

Conferencing on page 573

The methods below use the system's default system short codes

About this task

Short Code

The Conference Add short code action is used to create short codes for ad-hoc conferencing. By default, the short code *47 is added to new systems.

Starting an ad-hoc conference using a short code:

Procedure

1. Place your current call on hold.
2. Call the party that you want to also include in the call.

Result

- If answered and the other party wants to join the conference, put the call on hold and dial *47.
- If not answered or diverted to voicemail or answered but the party does not want to join the conference, put the call on hold and dial *52 to clear it.

You and the held calls are now in conference.

Conference Button

About this task

The Conference Add action can be assigned to a programmable button on phones that support programmable buttons. The button can then be used to start an ad-hoc conference or to add additional users to an existing conference.

On many Avaya phones, the same function is provided by a permanent Conference button. Alternatively the phone may display a Conf soft-key option during calls. Refer to the appropriate phone user guide.

Starting an ad-hoc conference using a button or softkey:

Procedure

1. With a current call connected, press the button.

   The current call is put on hold pending the conference.

2. Call the party that you want to also include in the call.

Result

- If answered and the other part wants to join the conference, press the conference button again.
- If not answered or diverted to voicemail or answered but the party does not want to join the conference, end the call. Press the button representing the held call to reconnect to it.

You, the held call and the new call are now in a conference.

Adding Calls to a Conference

You can use the same processes as above to add additional calls to a conference. While you hold a conference on your own telephone system, the existing members of the conference can still talk to each other.

Meet Me Conferencing

Conference meet-me refers to features that allow a user or caller to join a specific conference by using the conference's ID number (either pre-set in the control or entered at the time of joining the conference).

IP500 V2 systems require a **Preferred Edition** license.

Note:

Conference Meet Me features can create conferences that include only one or two parties. These are still conferences that are using resources from the host system's conference capacity.

Conference ID Numbers

By default, ad hoc conferences are assigned numbers starting from 100 for the first conference in progress. Therefore, for conference Meet Me features specify a number away from this range ensure that the conference joined is not an ad hoc conference started by other users. It is not possible to join a conference using conference Meet Me features when the conference ID is in use by an ad-hoc conference.

User Personal Conference Number Each user's own extension number is treated as their own personal conference number. Only that user is able to start a conference using that number as the conference ID. Any one else attempting to start a conference with that number will find themselves in a conference but on hold until the owner also joins. Personal conferences are always hosted on the owner's system.

Note:

When a user calls from their mobile twinned number, the personal conference feature will only work if they access the conference using an FNE 18 service.

Multi-Site Network Conferencing

Meet Me conference IDs are now shared across a multi-site network. For example, if a conference with the ID 500 is started on one system, anyone else joining conference 500 on any system will join the same conference. Each conference still uses the conference resources of the system on which it was started and is limited by the available conference capacity of that system.

Previously separate conferences, each with the same conference ID, could be started on each system in a multi-site network.

Other Features

Transfer to a Conference Button A currently connected caller can be transferred into the conference by pressing **TRANSFER**, then the Conference Meet Me button and **TRANSFER** again to complete the transfer. This allows the user to place callers into the conference specified by the button without being part of the conference call themselves. This option is only support on Avaya phones with a fixed **TRANSFER** button (excluding T3 and T3 IP phones).

Conference Button Status Indication When the conference is active, any buttons associated with the conference ID indicate the active state.

Short Codes

The Conference Meet Me short code action is used to create short codes for Meet Me conferencing. There are no default short codes in a new system for this type of function. It can also be used to transfer caller's into a Meet Me conference.

Example 1: Specific Meet Me Conference Short Code

The following example system short code allows the dialing user to join a specific conference, in this meet-me conference 500.

Short Code: *500

Telephone Number: 500

Feature: Conference Meet Me

Example 2: General Meet Me Conference Short Code

The following example system short code allows any extension to dial *67* and then the number of the conference which they want to join followed by #. For example dialing *67*600# will put the user into meet-me conference 600.

Short Code: *67*N#

Telephone Number: N

Feature: Conference Meet Me

Programmable Buttons

The Conference Meet Me action can be assigned to a programmable button on phones that support programmable buttons. The button can then be used to join a specified Meet Me conference. It can also be used to transfer caller's into a meet-me conference.

For buttons configured with a specific conference ID, the button will indicate whether a conference is in progress or not. For a button configured to a user's personal conference number, the button will indicate when other people are in the conference and when the owner is also in the conference.

Related Links

Conferencing on page 573

Routing External Callers

Internal users can access Meet Me conferencing using short code and buttons. Additional methods need to be provided for external callers. Typically this is done using a system short code to which the external call is then directed by one of the options below. This has the advantage that internal users can also dial the same short code to access the same conferences.

Transferring Callers

Conference Meet Me short codes and buttons can be used as the destination for call transfers by other users. If the short code or button is not configured with a specific conference ID, that value needs to be entered by the person transferring the call before completing the transfer.

Incoming Call Routing

The method by which calls requiring access to a conference can be identified will depend on the customer requirement. However, once that is determined, a system short code configured for the specific conference required can be used as the destination for the appropriate incoming call route added to the system configuration.

If general access to more than one possible conference is required, Voicemail Pro is used. See below.

Voicemail Pro

Voicemail Pro call flows can include transfer actions. If the target is a short code for a specific conference, the call flow user is added to that conference. The use if a short code for this also allow internal users to access the same conference.

This option can be used with call flow feature such as automatic attendants to provide access to more than one specific conference. For example, the call flow can prompt the caller to enter the ID of the conference they want to join. The call flow can then use the digits the caller dials as part of the short code to which the call is transferred.

Related Links

Conferencing on page 573

Context Sensitive Conferencing

On 1400, 1600, 9500 and 9600 Series telephones there have been changes to the display and handling of calls put on hold pending transfer. See Context Sensitive Transfer. For those phones there have also been changes to which calls are conferenced when a **Conference** button or **Conf** display option is pressed on the telephone.

Previously, pressing **Conference** would put the user's current call and all held calls into a conference. That included any calls that had be put on hold pending transfer by pressing **Transfer**.

The result of pressing **Conference** on the telephone now depends on which call is currently highlighted on the phone display and what other calls are held or held pending transfer.

Which call is highlighted on the display	Other condition (in priority order)	Result when Conference is pressed:	Calls Conferenced		
			Connected Call	Held Calls	Held Pending Transfer
Connected call	**No call held pending transfer**	Conferences the connected call and all held calls.	✓	✓	–
	Call held pending transfer	Conferences the connected call and the held pending transfer call. Any other held calls are unaffected.	✓	–	✓
Held call	**Connected call**	Conferences the held call and the connected call. Any other held calls including held pending transfer are unaffected.	✓	–	–
	Held pending transfer call	Conferences the held and held pending transfer call. All other held calls are unaffected.	–	–	✓
	Held calls	Conferences with all other held calls.	–	✓	–
Held pending transfer call	**Connected call**	Conferences the held pending transfer call to a connected call. Any other held calls are unaffected.	✓	–	✓
	Held calls	Conferences the call held pending transfer with all other held calls.	–	✓	✓

Note that this new behaviour only applies to conferences being initiated from the telephone. The original behaviour of conferencing all calls still applies if the conference function is initiated from elsewhere such as from an application like one-X Portal.

Changing which call is currently highlighted On phones with a set of cursor keys (four cursor keys around an **OK** key), the up and down cursor key can be used to change the current highlighted call (or call appearance if idle). This can be done even whilst there is a currently connected call. On touchscreen phones, the cursor buttons on the right-hand edge of the screen can be used for the same purpose. The method of highlighting is

- **1400 Series/1600 Series Telephones** On these phones only details of a single call are shown on the display at any time. The displayed call is the currently highlighted call.
- **9500 Series/9600 Series Telephones** On most phones in these series, the background of the shading is changed for the currently selected call. The except is 9611, 9621 and 9641 telephones where a yellow symbol is shown on the right of the highlighted call.

Related Links

Conferencing on page 573

Paging

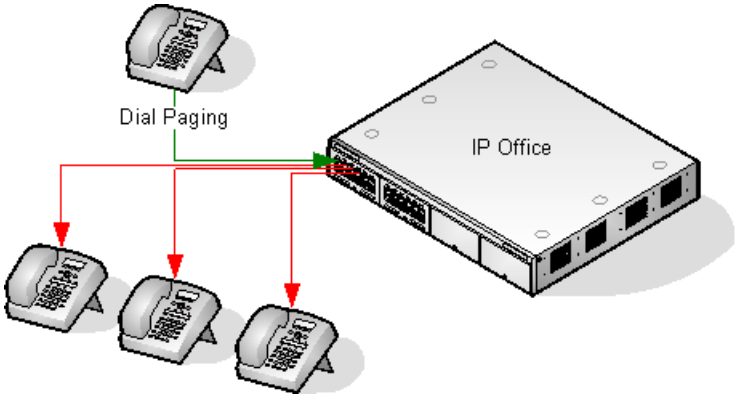
Paging limits

The maximum recommended size for paging groups is 64 parties on IP500 V2 systems and 128 parties on Server Edition Linux servers.

Paging Scenarios

Paging Scenario	Paged Device Connects to...	Short Code/ Button Feature
Phone to Phone Simple paging to other system extensions.	Digital Station and Avaya H.323 Phones	**Dial Paging**
Mixed Paging This refers to simultaneous paging to phones and a paging speaker.	Analog Extension (Paging Speaker)	**Dial Paging**
Paging Interface Device This refers to paging to a paging interface device such as a UPAM.	Analog Extension (IVR Port)	**Dial Extn**
	Analog Trunk	**Dial**

Phone to Phone Paging



Paging is supported from all phone types. A page call can be to a single phone or a group of phones.

- From analog and non-Avaya phones, use a Dial Paging short code.
- From Avaya feature phones, a programmable button set to Dial Paging can be used.

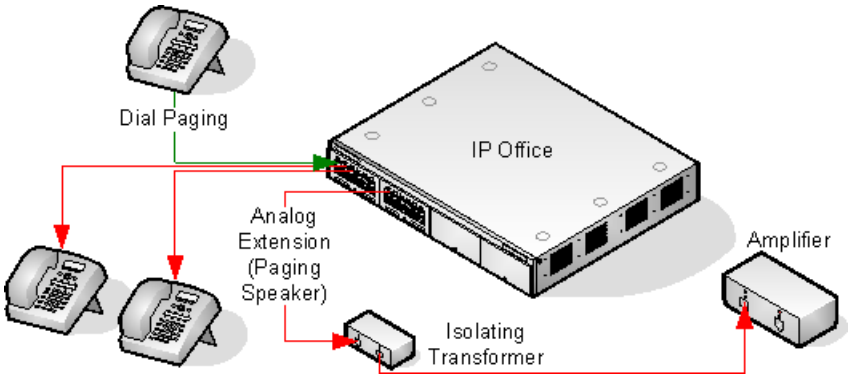
Paging is only supported to Avaya phones that support auto answer.

The page is not heard on phones that are active on another call.

The page is not heard on phones where the user is set to Do Not Disturb or has Forward Unconditional active.

On Avaya phones with a dedicated **Conference** button, the user can answer a page call by pressing that button. This turns the page into a normal call with the pager.

Mixed Paging



Uses an amplifier connected to an analog extension port via a 600ohm isolating transformer. Some amplifiers include an integral transformer.

Avaya/Lucent branded amplifiers are designed for connection to special paging output ports not provided on systems. They are not suitable for supporting mixed paging.

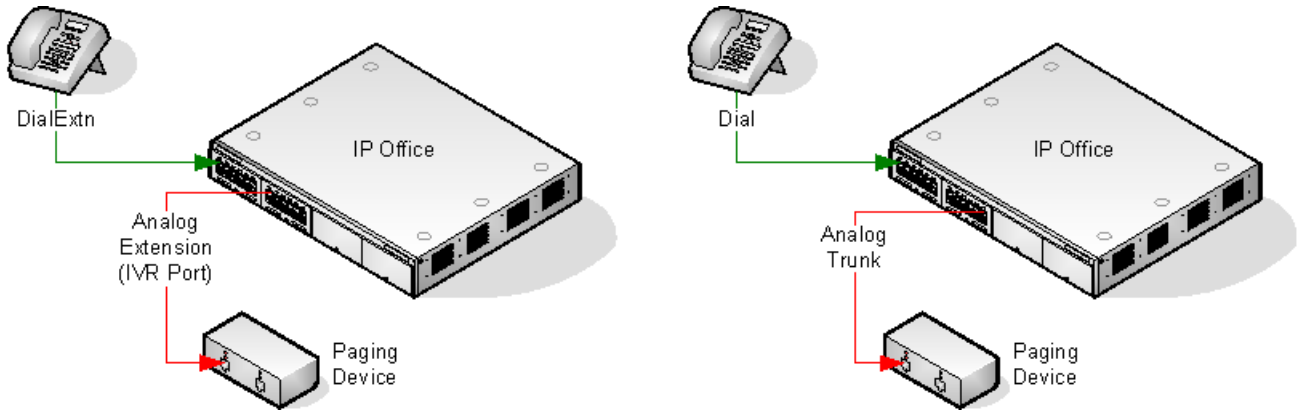
The transformer and amplifier must be connected when the system is restarted.

If background music is required between pages, the amplifier must support a separate background music connection and VOX switching.

The analog extension port is set as a Paging Speaker in the system configuration (Extn | Analog | Equipment Classification).

Short code/programmable button: Use DialPaging.

Paging Interface Device



Uses a paging interface device such as a UPAM or amplifier with analog trunk/extension interface.

The device can be connected to an analog trunk port or analog extension port.

If connected to a trunk port:

Short code: Use Dial and the same Line Group ID as the Outgoing Line ID set for the analog trunk.

If connected to an extension port:

- Set the analog extension as an IVR Port in the system configuration (Extn | Analog | Equipment Classification).
- Short code/programmable button: Use Dial Extn.

Related Links

Paging Via Voicemail Pro on page 582

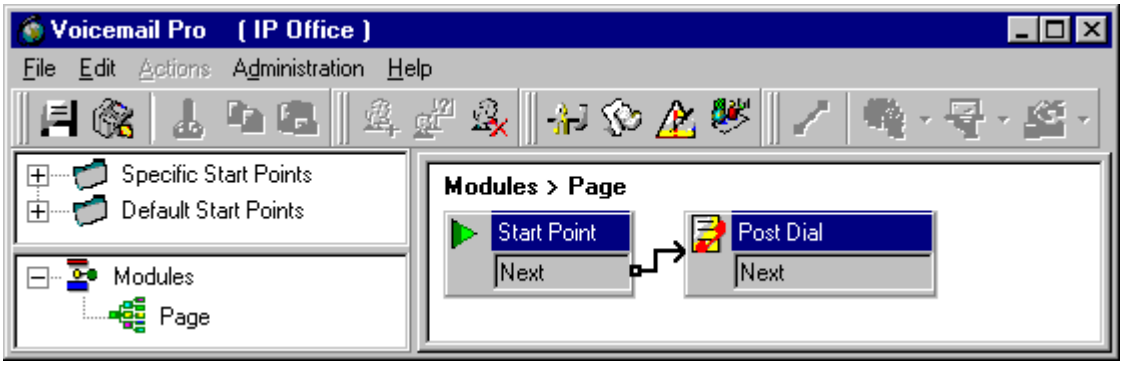
Paging Via Voicemail Pro

Voicemail Pro can be used to deliver pre-recorded announcements. This can be useful when the same announcement is repeated frequently. This method requires the paging port to be an analog extension.

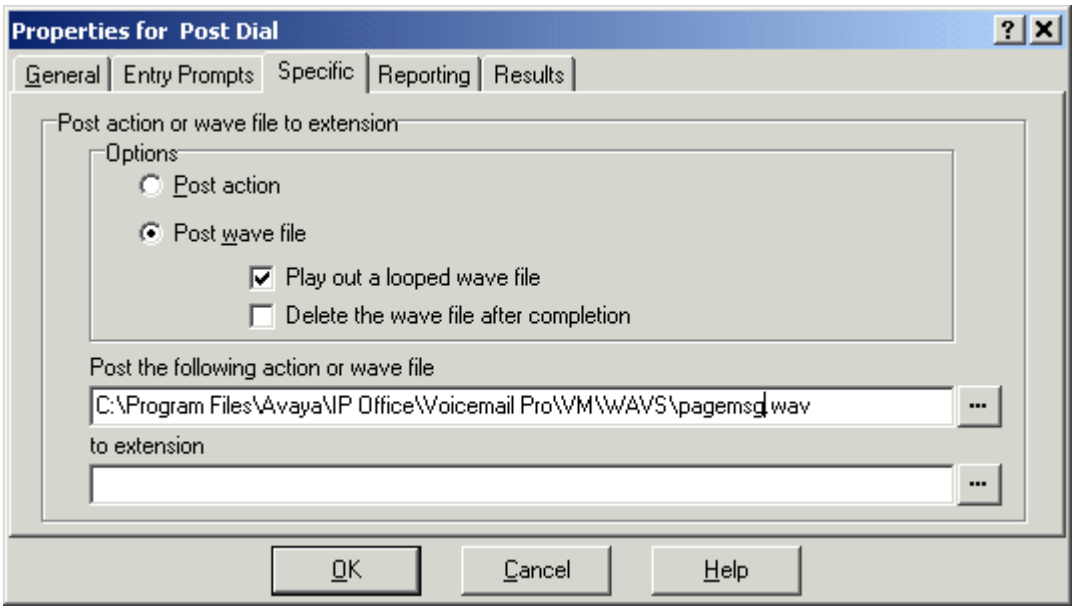
This method also removes the feedback loop that can occur on some sites as the page is first recorded and then played.

Example 1

1. In Voicemail Pro, a new Module was added and named Page.



2. A Post Dial action was added to the module. The properties of the Specific tab were set as shown:



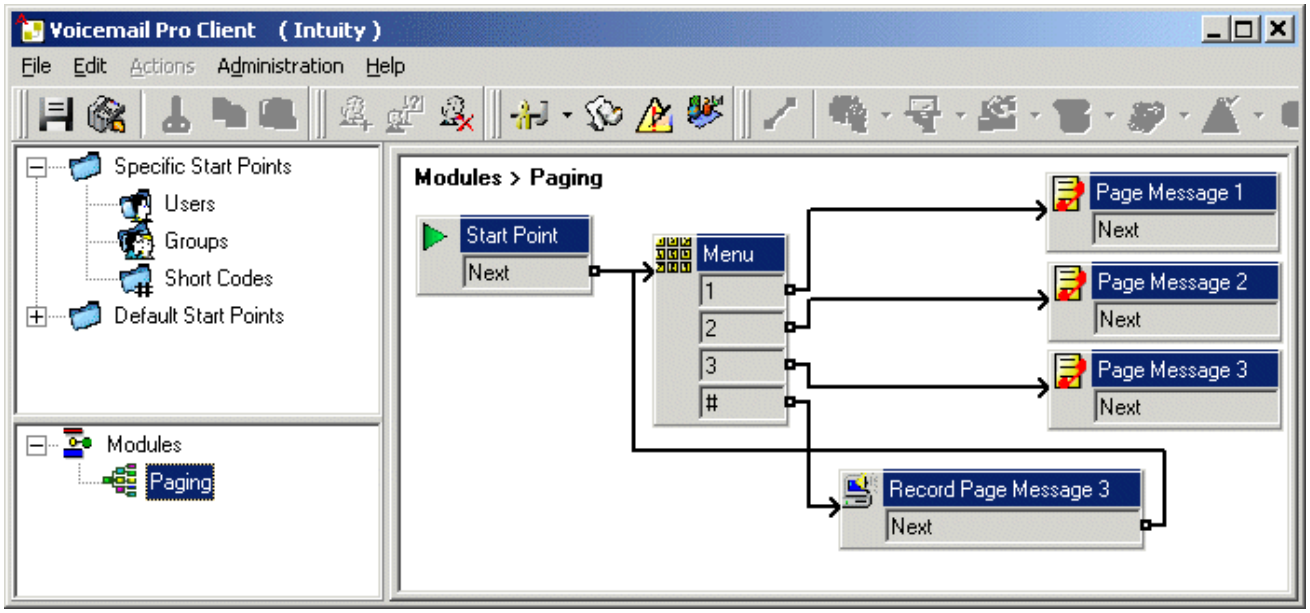
3. We then saved and made live the new Voicemail Pro call flow.
4. In Manager we received the system configuration and created a new short code.

- Short Code: *80
- Telephone Number : "Page"
- Feature: VoicemailCollect.

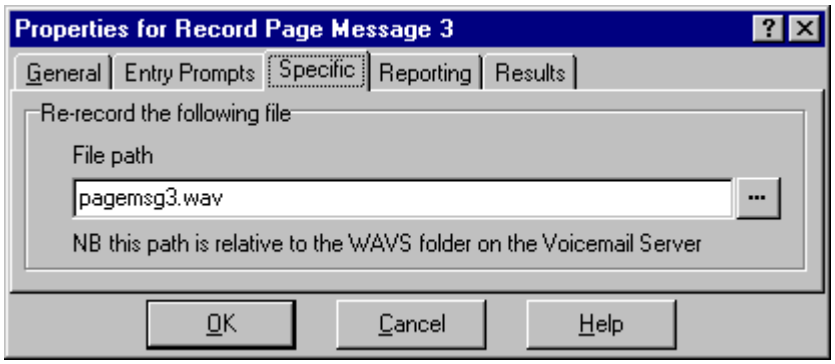
The new system configuration was then merged.

Example 2

This example builds on example 1 by allowing the user to select which message is played from a menu. In this example the user can press 1, 2 or 3 for different messages. They can also re-record the message associated with option 3 by pressing #.



A Play List action was added and in this example set to record pagemsg3.wav. Note that just the file name was specified as this action saves files relative to the Voicemail Server's WAVS folder.



In the Post Dial action that plays back pagemsg3.wav note that the full file path needs to be used.

In Manager, we then added a short code that triggers the module "Paging" using the VoicemailCollect feature.

Related Links

Paging on page 580

Automatic Intercom Calls

Automatic intercom functions allow you to call an extension and have the call automatically answered on speaker phone after 3 beeps. The extension called must support a handsfree speaker. If the extension does not have a handsfree microphone then the user must use the handset if they

want to talk. If the extension is not free when called, the call is presented as a normal call on a call appearance button if available.

Making Automatic Intercom Calls

The following programmable button functions can be used to make automatic intercom calls:

- **Automatic Intercom**
- **Dial Direct**
- **Dial Intercom**

The following short code function can be used to make automatic intercom calls:

Dial Direct

On M-Series and T-Series phones, the code **Feature 66** followed by the extension number can be used to make a direct voice (automatic intercom) call.

Deny automatic intercom calls

When enabled, any automatic intercom calls to the user's extension are automatically turned into normal calls.

Deny automatic intercom calls can be configured per user on the **User | Telephony | Supervisor Settings** tab. Deny automatic intercom call can also be enabled using the Auto Intercom Deny On short code or the Auto Intercom Deny button action.

Voice over IP Features

Wide Band Audio Support

IP Office systems support the G.722 64K codec for wide band audio. G.722 can be used with H.323 and SIP trunks. If can also be used with some SIP and H.323 IP telephones (see below). G.722 uses a higher speech sample rate (16KHz) than is used by most other audio codecs (8KHz).

G.722 is only supported by systems that are using IP500 VCM, IP500 VCM V2 and or IP500 Combination cards.

Avaya Phone Support

Use of G.722 is supported by the following Avaya phones on a IP Office system: **1010**, **1040**, **1120E**, **1140E**, **B179**.

Using the G.722 Codec

The G.722 codec is not available for use by default. If the codec is to be used, it must first be selected in the system's **Available Codecs** list (System | Codecs). The codec can then be used in the system's default codec preference list and or in the individual codec preferences of IP lines and extensions.

The method of codec selection for specific phones will depend on the phone type. Refer to the appropriate installation manual.

Conferencing

Where devices using G.722 are in a system conference, the system can attempt to ensures that the speech between devices using G.722 remains wide-band even if there are also narrow-band audio devices in the same conference. This is done if the system's High Quality Conferencing option is enabled (**System | Telephony | Telephony**).

Known Limitations

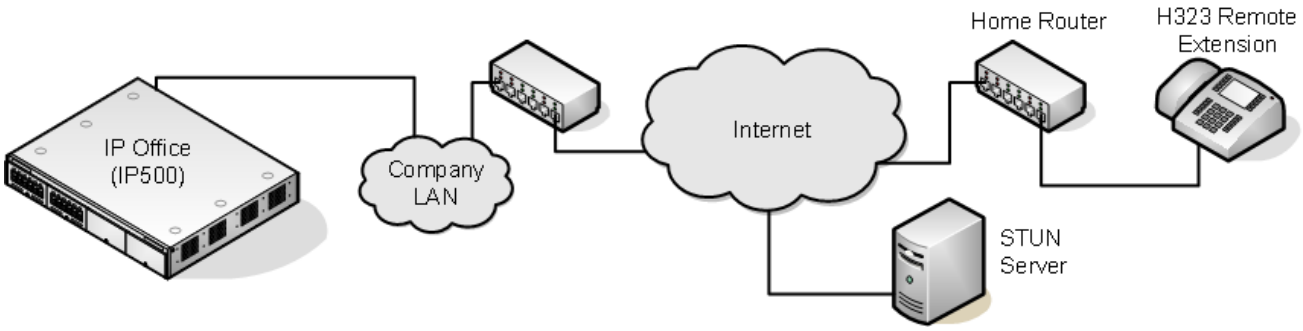
The following limitations apply to G.722 wide band audio operation:

- Call recording uses G.711.
- Page calls only use G.722 when all devices being paged can use G.722.
- Fax is not supported in G.722, use G.711 or T38.
- Soft tones provided by the system use G.711.
- A maximum of 15 G.722 devices receiving wide-band audio are supported in conferences.

Remote H.323 Extensions

The configuration of remote H.323 extensions is supported without needing those extensions to be running special VPN firmware. This option is intended for use in the following scenario:

- The customer LAN has a public IP address which is forwarded to the IP Office system. That address is used as the call server address by the H.323 remote extensions.
- The user has a H.323 phone behind a domestic router. It is assumed that the domestic router allows all outbound traffic from the home network to pass through and allows all symmetric traffic. That is, if the phone sends RTP/RTCP to a public IP address and port, it will be able to receive RTP/RTCP from that same IP address and port. If this is not the case, the configuration of the user's router to support that is not covered by this documentation.



Other scenarios can be configured. For example one of the IP Office's LAN interfaces can be connected to the public internet.

Supported Telephones Currently remote H.323 extension operation is only supported with 9600 Series phones already supported by the IP Office system.

License Requirements For non-Server Edition systems, by default only 4 users can be configured for remote H.323 extension usage. Additional users can be configured if those additional users are licensed and configured with either **Teleworker** or **Power User** user profiles. On Server Edition

systems remote workers can only be configured for users licensed and set to the **Power User** user profile.

Customer Network Configuration

The corporate LAN hosting the IP Office system requires a public IP address that is routed to the LAN interface of the IP Office system configured for remote H.323 extension support.

STUN from the IP Office system to the Internet is used to determine the type of NAT being applied to traffic between the system and the Internet. Any routers and other firewall devices between the H.323 phone location and the IP Office system must allow the following traffic.

Protocol	Port	Description
UDP	**1719**	UDP port 1719 traffic to the IP Office system must be allowed. This is used for H225 RAS processes such as gatekeeper discovery, registration, keepalive, etc. If this port is not open, the phone will not be able to register with the IP Office system.
TCP	**1720**	TCP port 1720 traffic must be allowed. This is used for H225 (call signalling).
RTP	**Various**	The ports in the range specified by the system's **RTP Port Number Range (Remote Extn)** settings must be allowed.
RTCP		

User Network Configuration

It is assumed that the domestic router allows all outbound traffic from the home network to pass through and allows all symmetric traffic. That is, if the phone sends RTP/RTCP to a public IP address and port, it will be able to receive RTP/RTCP from that same IP address and port. If this is not the case, the configuration of the user's router to support that is not covered by this documentation.

System Configuration

About this task

This is a summary of the system configuration changes necessary. Additional details and information for H.323 telephone installation are included in the H.323 IP Telephone Installation manual. This section assumes that you are already familiar with IP Office system and H.323 IP telephone installation.

Procedure

1. Licensing:

   For non-Server Edition systems, by default only 4 users can be configured for remote H.323 extension usage. Additional users can be configured if those additional users are licensed and configured with either **Teleworker** or **Power User** user profiles. On Server Edition

systems remote workers can only be configured for users licensed and set to the **Power User** user profile.

2. System Configuration:

   The following needs to be configured on the IP Office system LAN interface to which the public IP address is routed.

3. Select **System | LAN1/LAN2 | VoIP**.

   Check that the **H.323 Gatekeeper Enable** setting is selected.

4. Due to the additional user and extension settings needed for remote H.323 extension configuration, we assume that the extension and user records for the remote H.323 extensions and users are added manually.

5. Select **H.323 Remote Extn Enable**.

6. Set the **RTP Port Number Range (Remote Extn)** range to encompass the port range that should be used for remote H.323 extension RTP and RTCP traffic. The range setup must provide at least 2 ports per extension being supported.

   Note:

   When the system is configured on an open internet connection, the standard RTP port range is used for all H.323 calls including remote workers. In such a case the **RTP Port Number Range** is used.

7. Network Topology Configuration:

   STUN can be used to determine the type of NAT/firewall processes being applied to traffic between between the IP Office system and the Internet.

8. Select the **Network Topology** tab.

   Set the **STUN Server IP Address** to a known STUN server. Click **OK**. The **Run STUN** button should now be enabled. Click it and wait while the STUN process is run. The results discovered by the process will be indicated by **!** icons next to the fields.

9. If STUN reports the **Firewall/NAT Type** as one of the following, the network must be reconfigured if possible as these types are not supported for remote H.323 extensions: **Static Port Block**, **Symmetric NAT** or **Open Internet**.

10. H.323 Extension Configuration: H.323 remote extensions use non default settings and so cannot be setup directly using auto-create.

11. Within Manager, add a new H.323 extension or edit an existing extension.

12. On the **Extn** tab, set the **Base Extension** number.

13. On the **VoIP** tab, select **Allow Remote Extn**.

14. The other settings are as standard for an Avaya H.323 telephone.

    - The IP Address field can be used to restrict the the source IP address that can used by the Remote Worker. However, it should not used in the case where there is more than one phone behind the domestic router.

- Regardless of direct media configuration, direct media is not used for remote H.323 extensions.

15. User Configuration:

    For non-Server Edition systems, by default only 4 users can be configured for remote H.323 extension usage.

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

    a. In the user configuration, select **Enable Remote Worker**.

    b. If the user's **Extension Number** matches the **Base Extension** setting of an IP extension, the **Allow Remote Extn** setting of that extension is automatically changed to match the user's **Enable Remote Worker** setting and vice versa.

Phone Configuration

About this task

The phones do not require any special firmware. Therefore they should first be installed as normal internal extensions, during which they will load the firmware provided by the IP Office system.

Once this process has been completed, the address settings of the phone should be cleared and the call server address set to the public address to be used by remote H.323 extensions.

It is assumed that at the remote location, the phone will obtain other address information by DHCP from the user's router. If that is not the case, the other address setting for the phone will need to be statically administered to match addresses suitable for the user's home network.

Creating a Virtual WAN Port

Procedure

1. Select **WAN Port**.
2. Click and select **PPP**.
3. In the **Name** field, enter either **LINEx.y** where:
   - **LINE** must be in uppercase.
   - **x** is the line number. For a PRI/T1 module in Slot A, this will be 1. For a PRI/T1 module in Slot B, this will be 5.
   - **y** is the lowest numbered channel number to be used by the WAN link minus 1. For example, if the lowest channel to be used is channel 1 then y = 1 - 1 = 0.
4. In the **Speed** field, enter the total combined speed of the maximum number of channels sets in the Service.

   In this example, 12 channels x 64000 bits = 76800.

Note:

The maximum number of channels that can be used will be limited by the number of data channels supported by the system Control Unit and not already in use.

5. In the **RAS Name** field, select the RAS name created when the new Service of that name was created.
6. Click **OK**.

Configuring authorization codes

Note:

In release 9.1, authorization codes can no longer be associated with User Rights. If an authorization code was configured in relationship with User Rights in an earlier release configuration, this authorization code will be lost during upgrade. The administrator must re-configure the authorization code, after upgrade. The authorization code must be associated with a user.

Authorization codes are enabled by default.

A user dials a number that matches a short code set to **Force Authorization Code**. The user is prompted to enter an authorization code.

They dial their authorization code. If a matching entry is found in **Authorization Codes** records the system checks the corresponding user. Note that the user checked does not necessarily need to be connected with the user dialing or the user whose extension is being used to make the call.

The dial string is checked against the short codes with the matching user. If it matches a dial short code or no short code the call is allowed, otherwise it is blocked. Note that the short code is not processed, it is just checked for a match. If multi-tier authorization codes are required there must be blocking (busy) short codes (or a wild card '?')

Example:

A restaurant has a number of phones in publicly accessible areas and want to control what calls can be made by staff. Staff must not be able to dial long distance numbers. staff should be able to dial local and cell phone numbers.

ARS Table
In the Main (50) ARS table, add the following short codes: • 044XXXXXXXXX/Dial/044N/ • 01XXXXXXXXX/Dial/01N/Force Auth Code checked
Authorization Codes
Configure an authorization code for each staff member that is allowed to make long distance calls. For example, for staff members Alice and Bob: AuthCode: **2008 - Alice** AuthCode: **1983 - Bob**

It is recommended to use short codes that use X characters to match the full number of characters to be dialed. That ensures that authorization code entry is not triggered until the full number has been dialed rather than mid-dialing. For example 09 numbers are premium rate in the UK, so you would create a **09XXXXXXXXX/Dial/N** short code set to Forced Authorization. In the associated user or user right short code it is recommended to use 09N type short codes.

System short codes that route to ARS will not have their **Force Authorization Code** setting used. However short codes within an ARS table will have their **Force Authorization** Code setting used.

Forcing Authorization Codes

There are two methods to force a user to enter an authorization code in order to complete dialing an external call.

- **To Force Authorization Codes on All External Calls** A user can be required to enter an authorization code for all external calls. This is done by selecting Force Authorization Code (**User | Telephony | Supervisor Settings**).
- **To Force Authorization Codes on Specific Calls** To require entry of an authorization code on a particular call or call type, the Force Authorization Code option should be selected in the short code settings. This can be used in user or system short codes in order to apply its effect to a user or all users respectively. You need to ensure that the user cannot dial the same number by any other method that would by pass the short code, for example with a different prefix.

Related Links

Entering an Authorization Code on page 591

Entering an Authorization Code

Where possible, when an authorization code is required, the user can enter it through their phones display. However, this is not possible for all type of phone, for example it is not possible with analog phones and Avaya XX01 or XX02 phones. The users of these device must either enter the authorization code using a short code set to the Set Authorization Code feature immediately before making the call.

When entry of an authorization code is triggered, the user can enter any authorization code with which they are directly associated.

Note the following.

- If authorization code entry is setup for a particular number, calls forwarded or transferred to that number will also trigger authorization code entry.
- On systems using line appearances to BRI trunk channels to make outgoing calls, authorization code entry may not be triggered. This can be resolved by adding a short code such as [9]XN;/Dial/XN/0 (adjust the prefix and line group as necessary).

Related Links

Configuring authorization codes on page 590

Configuring ARS

When a dialed number matches a short code that specifies that the number should be dialled, there are two methods by which the routing of the outgoing call can be controlled.

Routing Calls Directly to a Line:

Every line and channel has an Outgoing Group ID setting. Several lines and channels can have belong to the same Outgoing Group ID. Within short codes that should be routed via a line within that group, the required Outgoing Group ID is specified in the short code's Line Group ID setting.

Routing Calls via ARS:

The short code for a number can specify an ARS form as the destination. The final routing of the call is then controlled by the setting available within that ARS form.

ARS Features

Secondary Dial Tone:

The first ARS form to which a call is routed can specify whether the caller should receive secondary dial tone.

Out of Service Routing:

ARS forms can be taken out of service, rerouting any calls to an alternate ARS form while out of service. This can be done through the configuration or using short codes.

Out of Hours Routing:

ARS forms can reroute calls to an alternate ARS form outside the hours defined by an associated time profile.

Priority Routing:

Alternate routes can be made available to users with sufficient priority if the initial routes specified in an ARS form are not available. For users with insufficient priority, a delay is applied before the alternate routes become available.

Line Types:

ARS can be used with all line types.

A SIP line is treated as busy and can follow alternate routes based on the SIP line setting **Call Initiation Timeout**. Previously a SIP line was only seen as busy if all the configured channels were in use.

IP lines use the NoUser Source Number setting **H.323SetupTimerNoLCR** to determine how long to wait for successful connection before treating the line as busy and following ARS alternate routing. This is set through the IP line option **Call Initiation Timeout**.

Multi-Site Network Calls:

Calls to multi-site extension numbers are always routed using the appropriate network trunk. ARS can be configured for multi-site network numbers but will only be used if the network call fails due to congestion or network failure.

Main Route:

The ARS form 50, named "Main" cannot be deleted. For defaulted systems it is used as a default route for outgoing calls.

Routing Calls to ARS

1. Create the ARS form.
2. Create the required system, user or user rights short code to match the user dialing.
    a. In the **Telephone Number** field, define the digits that will be used to match a short code in the ARS form.
    b. Use the **Line Group ID** field drop-down to select the ARS form required for routing the call.

Related Links

Example ARS Operation on page 593
ARS Operation on page 594

Example ARS Operation

The simplest example for ARS operation are the settings applied to a defaulted system. These vary between U-Law systems and A-Law systems. For Server Edition systems refer to Server Edition Outgoing Call Routing.

A-Law Systems

This set of defaults is applied to A-Law systems, typically supplied to locales other than North America. The defaults allow any dialing that does not match an internal number to be routed off-switch as follows:

System Short Code - ?/Dial/./50:Main:

The default system short code ? will match any dialing for which no other user, user rights or system short code match is found. This short code is set to route all the digits dialed to ARS form 50.

ARS Form - 50:Main:

This form contains just a single short code.

?/Dial3K1/./0 This short code matches any digits passed to the ARS form. It then dials the digits out on the first available line within line group 0 (the default outgoing line group for all lines).

U-Law Systems

This set of defaults is applied to U-Law systems, typically supplied to locales in North America. The defaults route any dialing prefixed with a 9 to the ARS and secondary dial tone.

System Short Code - 9N/Dial/N/50:Main:

The default system short code 9N is used to match any dialing that is prefixed with a 9. It passes any digits following the 9 to ARS form 50.

ARS Form - 50:Main:

This form has secondary dial tone enabled. It contains a number of short codes which all pass any matching calls to the first available line within line group 0 (the default outgoing line group for all

lines). Whilst all these short code route calls to the same destination, having them as separate items allows customization if required. The short codes are:

- **11/Dial Emergency/911/0** This short code matches an user dialing 911 for emergency services.
- **911/Dial Emergency/911/0** This short code matches an user dialing 9911 for emergency services.
- **0N;/Dial3K1/0N/0** This short code matches any international calls.
- **1N;/Dial3K1/1N/0** This short code matches any national calls.
- **XN;/Dial3K1/N/0** This short code matches 7 digit local numbers.
- **XXXXXXXXXX/Dial3K1/N/0** This short code matches 10 digit local numbers.

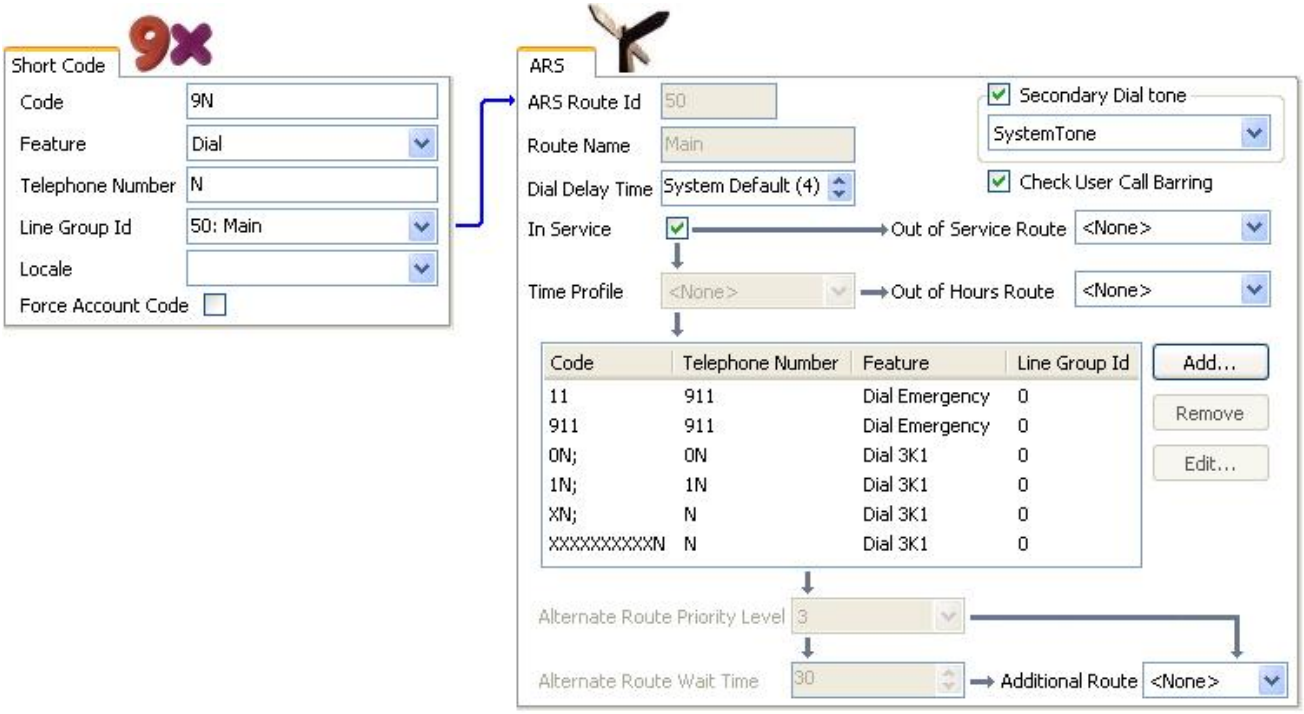
Related Links

[Configuring ARS](#) on page 592

ARS Operation

The diagram below illustrates the default ARS routing applied to systems (other than Server Edition) defaulted to the **United States** system locale. In summary:

- Any dialing prefixed with 9 will match the default system short code **9N**.
- That short code routes calls to the default ARS form **50:Main**.
- The short codes in that ARS form route all calls to an available line that has its **Outgoing Group ID** set to **0**.



The table describes in more detail the process that the system has applied to the user's dialing, in this example 91555707392200.

The user dials...	
9	The **Dial Delay Count** is zero, so the system begins looking for short code matches in the system and user's short codes immediately. Since there is only one match, the **9N** system short code, it is used immediately. The **9N** short code is set to route the call to the ARS form **Main**. It only passes those digits that match the N part of the dialing, ie. the 9 is not passed to the ARS, only any further digits dialed by the user. **Secondary Dial Tone** is selected in the ARS form. Since no digits for ARS short code matching have been received, secondary dial tone is played to the user.
1	Having received some digits, the secondary dial tone stops. The ARS form short codes are assessed for matches. The **11** and **1N;** short codes are possible matches. The **911** and **0N;** short codes are not possible matches. The **XN;** and **XXXXXXXXXXN;** short codes are also not matches because the **1N;** short code is already a more exact match. Since there is more than one possible match, the system waits for further digits to be dialed.
555	The **11** short code is no longer a possible match. The only match is left is the **1N;** short code. The **;** in the short code tells the system to wait for the **Dial Delay Time** to expire after the last digit it received before assuming that dialing has been completed. This is necessary for line providers that expect to receive all the routing digits for a call 'en bloc'. The user can also indicate they have completed dialing by pressing **#**.
707392200	When the dialing is completed, a line that has its **Outgoing Group ID** set to 0 (the default for any line) is seized. If no line is available, the alternate route settings would applied if they had been configured.

Related Links

ARS Short Codes

The short codes in the default ARS form have the following roles:

Code	Feature	Telephone Number	Line Group ID	Description
11	**Dial Emergency**	**911**	**0**	These two short codes are used to route emergency calls. A **Dial Emergency** call is never blocked. If the required line is not available, the system will use the first available line. Similarly, calls using **Dial Emergency** ignore any outgoing call bar settings that would be normally applied to the user.
911	**Dial Emergency**	**911**	**0**	
0N;	**Dial 3K1**	**0N**	**0**	Matches international numbers.
1N;	**Dial 3K1**	**1N**	**0**	Matches national numbers.
XN;	**Dial 3K1**	**N**	**0**	Matches 7 digit local numbers.
XXXXXXXXXXN;	**Dial 3K1**	**N**	**0**	Matches 10 digit local numbers.

ARS Short Code Settings

Code The digits used for matching to the user dialing.

Feature ARS short codes can use any of the **Dial** short code features or the **Barred** feature. When a **Barred** short code is matched, the call will not proced any further.

Telephone Number The number that will be output to the line as the result of the short code being used as the match for the user dialing. Short code characters can be used such as N to match any digits dialed for N or X in the **Code**.

Line Group ID The line group from which a line should be seized once short code matching is completed. Another ARS form can also be specified as the destination.

Locale Not used for outgoing external calls.

Forced Account Code If enabled, the user will be prompted to enter a valid account code before the call can continue. The account code must match one set in the system configuration.

Related Links

ARS Operation on page 594

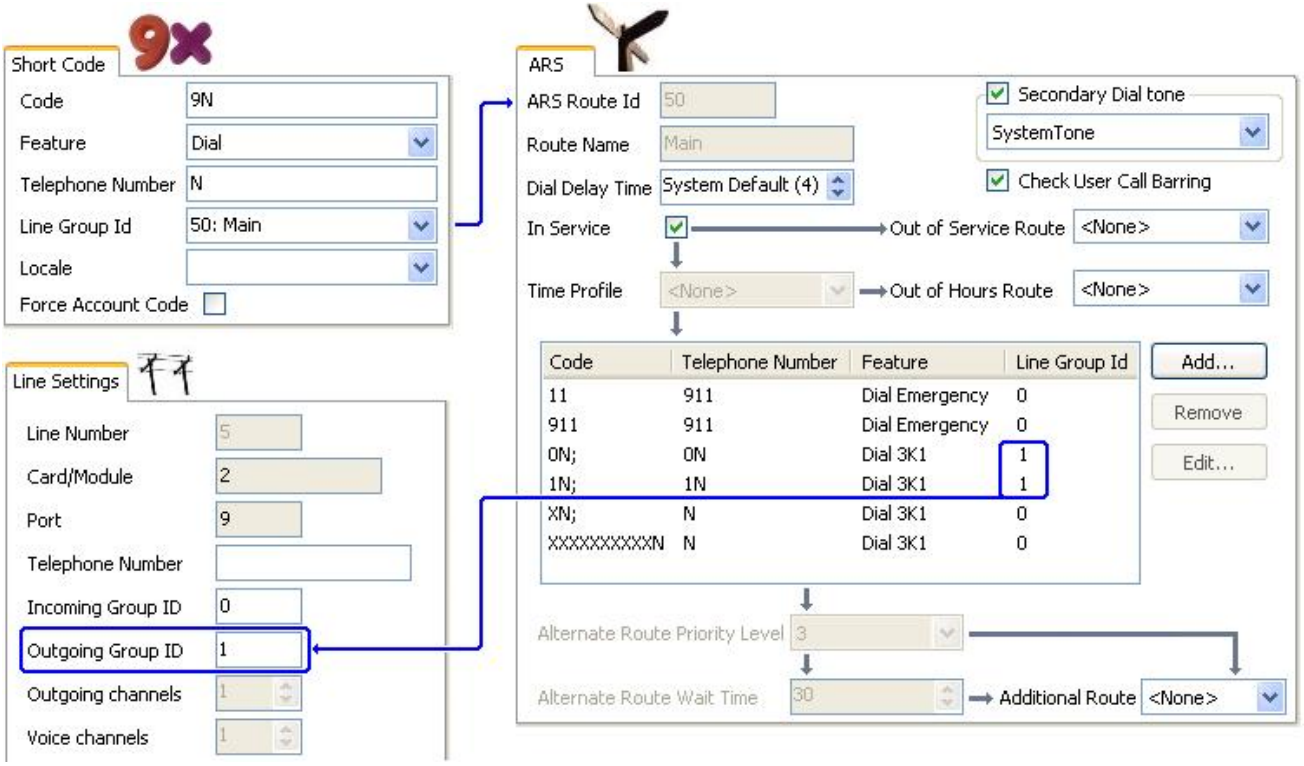
Simple Alternate Line Example

Using the default ARS settings, despite having several short codes in the ARS form, all outgoing calls are actually routed the same way using the same trunks. However, by having separate short codes for different call types present, it is easy to change the routing of each call type if required.

For this example, the customer has separate sets of lines for local calls and for national/international calls. These have been configured as follows:

- The lines for local and emergency calls have been left with the default **Outgoing Group ID** of **0**.
- The lines for national and international calls have been set with the **Outgoing Group ID** of **1**.

The default ARS can be configured to match this by just changing the **Line Group ID** settings of the default ARS short codes to match.



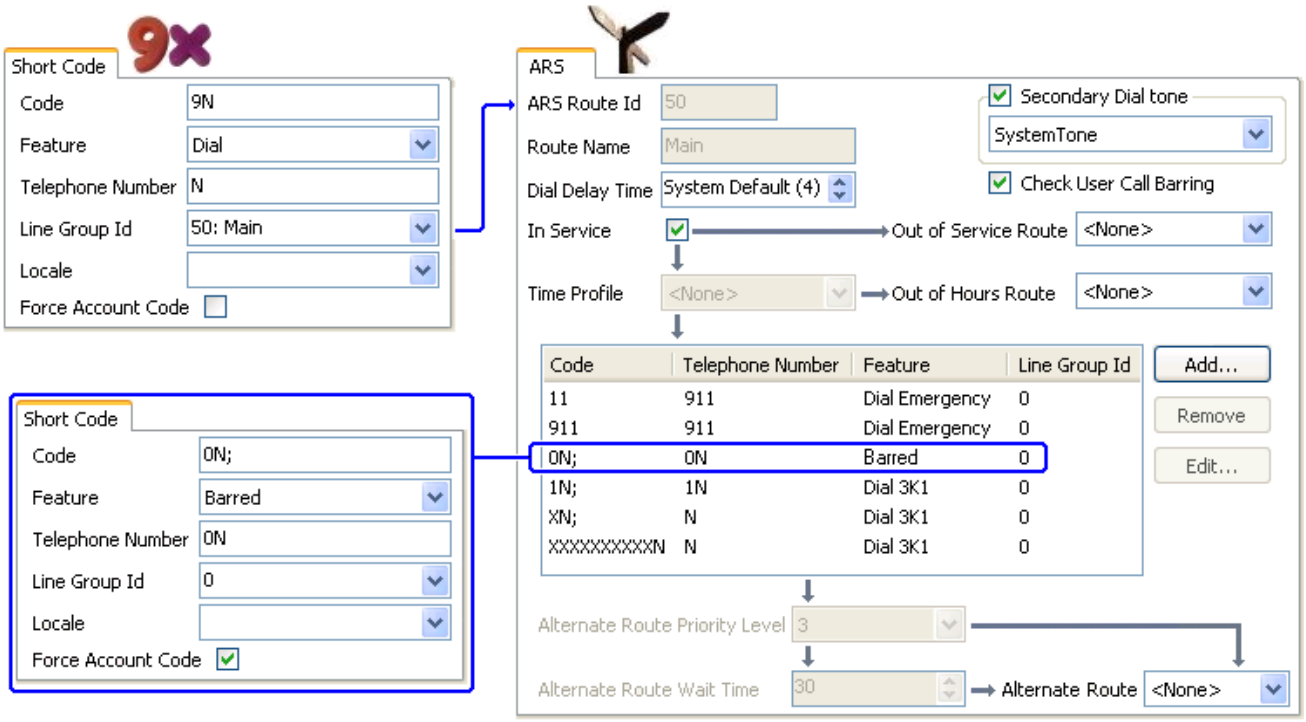
Related Links

ARS Operation on page 594

Simple Call Barring

All ARS short codes use one of the **Dial** short code features. The exception is the **Barred** short code feature. This can be selected for ARS short codes that match dialing that is not allowed.

In the example below, any user dialing an international number will be routed to the **Barred** short code. This prevents the dialing of external numbers prefixed with 0.



To restrict a user from making any outgoing external calls, use the user's Outgoing Call Bar option.

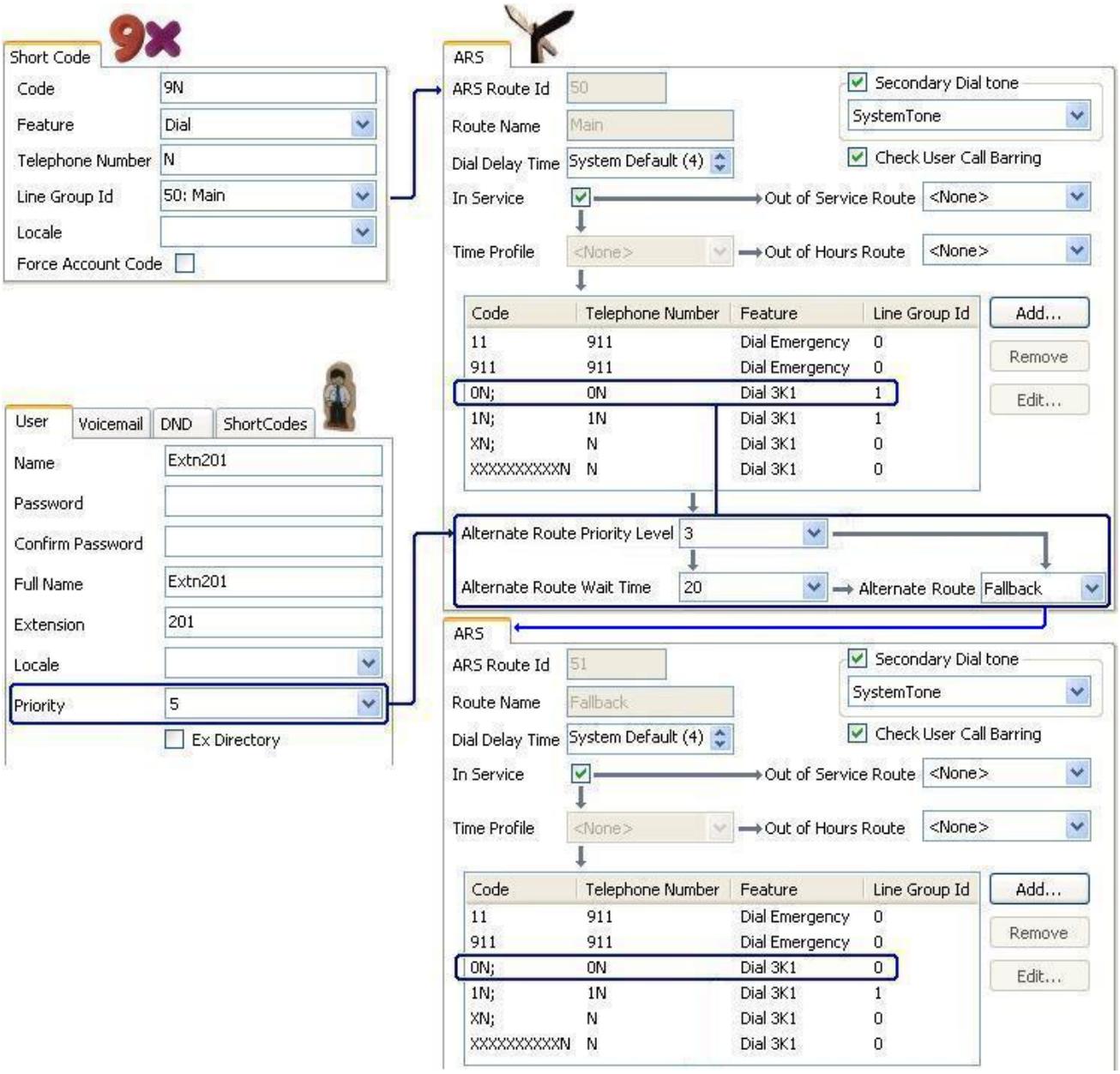
Related Links

ARS Operation on page 594

User Priority Escalation

User priority can be used to alter call routing when the required route is not available.

In this example, international calls are initially targeted to seize a line in outgoing line group 1. However an alternate route has been defined which will be used if no line in line group 1 is available. The fallback ARS form allows international calls to seize a line from line group 0. Whether this is done immediately or after a delay is set by whether the users priority is high enough.



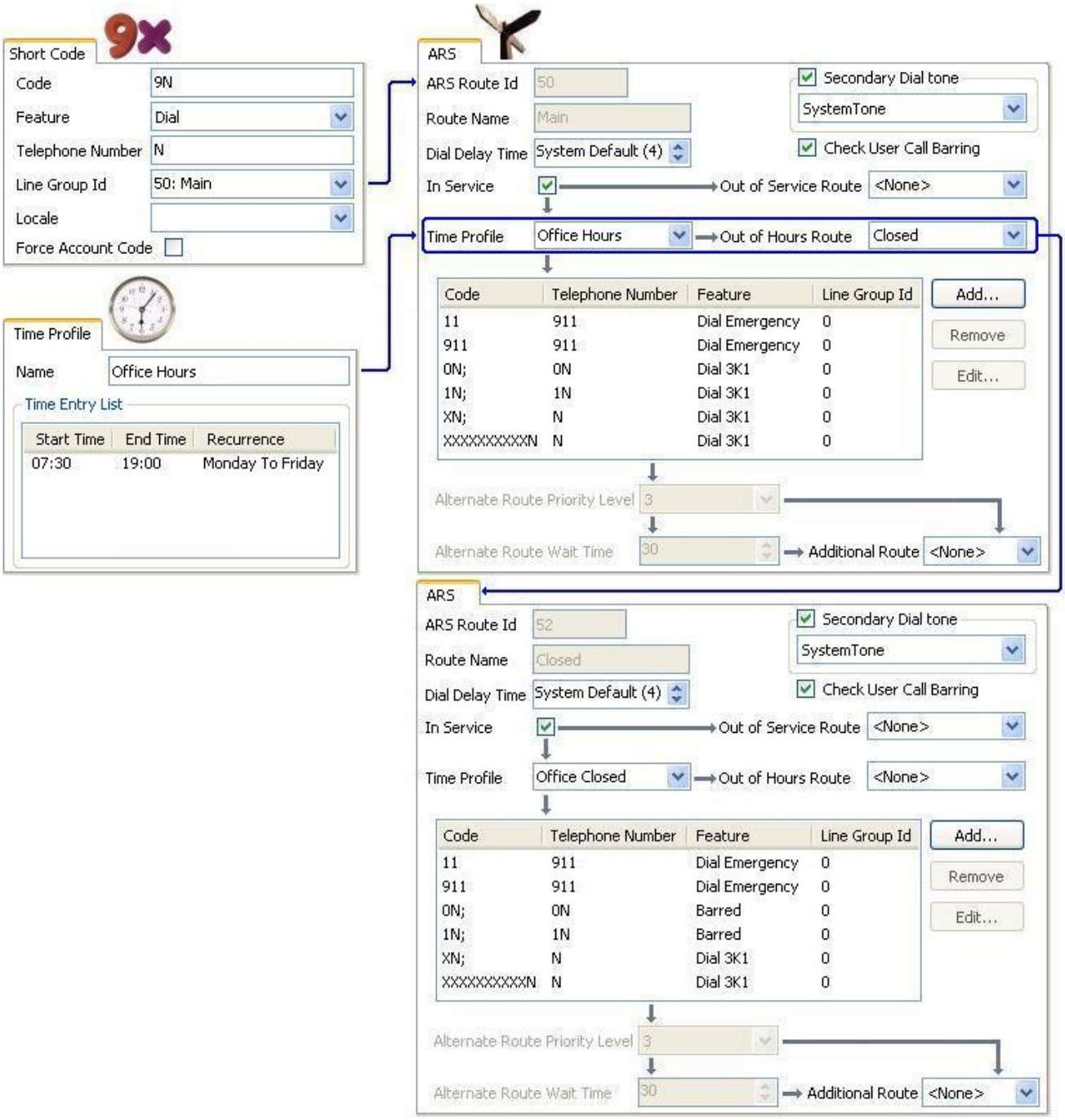
Related Links

ARS Operation on page 594

Time Based Routing

Time profiles can be used to switch call routing from one ARS form to another.

In the example below, a time profile has been define that sets the hours for normal operation. Outside the times set in the time profile, the other ARS form is used. This other ARS form only allows local and emergency calls.



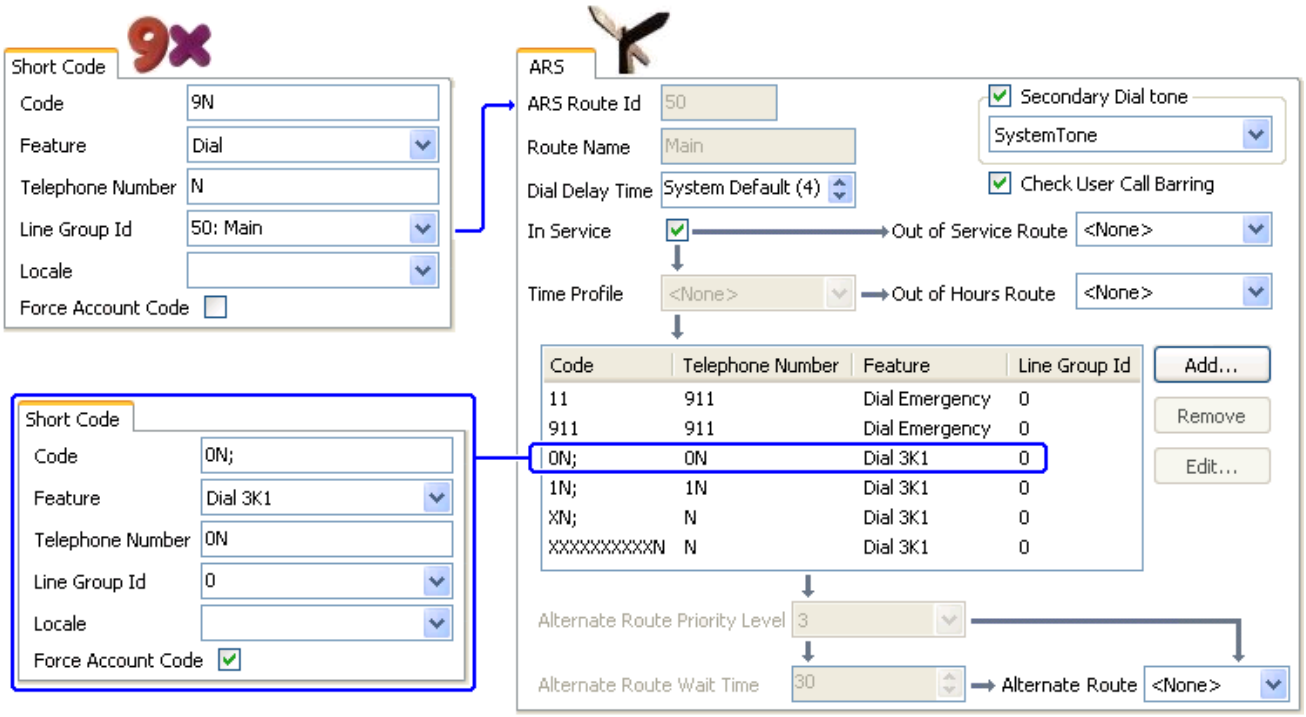
Related Links

ARS Operation on page 594

Account Code Restriction

The short codes within an ARS form can be individually set to require an account code before allowing any call that matches it to proceed.

In the example below, the short code for international calls has been set to require the user to enter an account code. A valid account code must be dialed to continue with the call.



If a user should always enter an account code to make any external call, the user option Force Account Code should be used.

Related Links

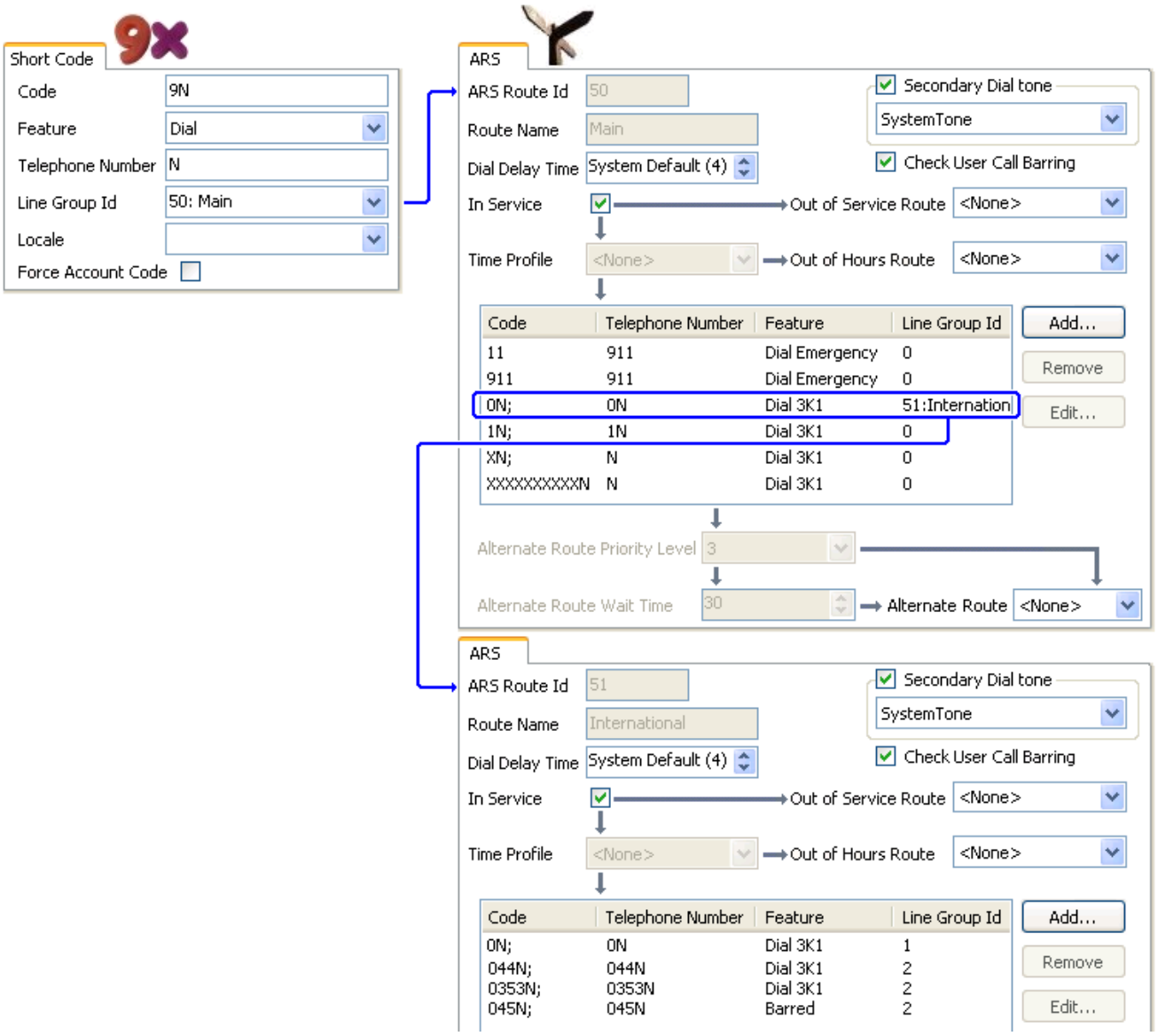
ARS Operation on page 594

Tiered ARS Forms

It is possible for an ARS short code in one form to have another ARS form as its destination. Dialing that matches the short code is then subject to further matching against the short codes in the other ARS form.

In the example below, the user wants different routing applied to international calls based on the country code dialed. To do that in the default ARS form would introduce a large number of short codes in the one form, making maintenance difficult.

So the short code matching calls with the international dialing prefix 0 has been set to route matching calls to another ARS form. That form contains short codes for the different country dialing codes of interest plus a default for any others.



Related Links

[ARS Operation](#) on page 594

Planning ARS

Using the methods shown in the previous examples, it is possible to achieve ARS that meets most requirements. However the key to a good ARS implementation is planning.

A number of questions need to be assessed and answered to match the system's call routing to the customer's dialing.

What What numbers will be dialed and what needs to be output by the system. What are the different call tariffs and the dialing codes.

Where Where should calls be routed.

Who Which users should be allowed to use the call routes determined by the previous questions.

When When should outgoing external calls be allowed. Should barring be applied at any particular times? Does the routing of calls need to be adjusted for reasons such as time dependant call tariffs.

Related Links

ARS Operation on page 594

System Events

The system supports a number of methods by which events occurring on the system can be reported. These are in addition to the real-time and historical reports available through the System Status Application (SSA).

SNMP Reporting

Simple Network Management Protocol (SNMP) allows SNMP clients and servers to exchange information. SNMP clients are built into devices such as network routers, server PC's, etc. SNMP servers are typically PC application which receive and/or request SNMP information. The system SNMP client allows the system to respond to SNMP polling and to send alarm information to SNMP servers.

In order for an SNMP server application to interact with a system, the MIB files provided with the Manager installation software must be compiled into the SNMP server's applications database.

Note:

The process of 'on-boarding' (refer to the IP Office Installation manual and the IP Office SSL VPN Solutions Guide) may automatically configure SNMP and create a number of SNMP alarm traps. These will override any existing SNMP configuration settings.

SMTP Email Reporting

The system can send alarms to an SMTP email server. Using SMTP requires details of a valid SMTP email account user name and password and server address. If SMTP email alarms are configured but for some reason the system cannot connect with the SMTP server, only the last 10 alarms are stored for sending when connection is successful. Use of SMTP alarms requires the SMTP server details to be entered in the SMTP tab.

Syslog Reporting

The system can also send alarms to a Syslog server (RFC 3164) without needing to configure an SNMP server. In addition Syslog output can include audit trail events.

Multiple event destinations can be created, each specifying which events and alarms to include, the method of reporting to use (SNMP, Syslog or Email) and where to send the events. Up to 2 alarm destinations can be configured for SNMP, 2 for Syslog and 3 for SMTP email.

Related Links

Configuring Alarm Destinations on page 605

Configuring Alarm Destinations

About this task

The Alarms section of the System Events tab displays the currently created alarm traps. It shows the event destinations and the types of alarms that will trigger the send of event reports. Up to 2 alarm destinations can be configured for SNMP, 2 for Syslog and 3 for SMTP email.

Procedure

1. In the navigation pane, select **System**.
2. In the details pane, select **System Events** and then select the **Alarms** sub-tab.
3. Use the **Add**, **Remove** and **Edit** controls to alter the traps.
4. Click **Add** or select the alarm to alter and then click **Edit**.
5. For a new alarm, set the **Destination** to either **Trap (SNMP)** or **Syslog** or **Email (SMTP)**.

   Note that once a destination has been saved by clicking **OK** it cannot be changed to another sending mode.
6. The remaining details will indicate the required destination information and allow selection of the alarm events to include.
7. When completed, click **OK**.
8. Click **OK**again.

Related Links

System Events on page 604

Preventing Toll Bypass

Use this procedure to prevent toll bypass in Enterprise Branch and Small Community Network (SCN) deployments. Toll bypass is prevented by only allowing PSTN calls where the originating location and terminating location are the same.

The location of non-IP lines is the same as the system location. If an IP address is not resolved to any location, then that device is assumed to be in the system location. The location of public IP lines must be configured to same as PSTN termination location.

The **Location** field for extensions with simultaneous login must be automatic and the location tab must be properly configured for the IP range.

Enterprise Branch deployments: All the distributed users must be in the same location as system location. Users registering from a location different from the system location are not supported.

Procedure

1. In the navigation pane on the left, select **System**.

2. In the details pane, click the **Telephony** tab.
3. Under **Telephony**, click the **Telephony** tab.
4. On the **Telephony** tab:
   a. Click the check box to turn **Restrict Network Interconnect** on.
   b. Click the check box to turn **Include location specific information** on.

      Setting the two configuration setting on the **Telephony** tab adds a **Network Type** field to the configuration settings for each trunk.
5. For Enterprise Branch deployments, open the **SM Line | Session Manager** tab. For SCN deployments, open the **IP Office Line | Line** tab.
6. If the line is a PSTN trunk (includes SIP), set **Network Type** to **Public**. If the line is an enterprise trunk, set the **Network Type** to **Private**.
7. If the **Network Type** is **Private**, the **Include location specific information** field is available.

   If the line is connected to an Avaya Aura® system release 7.0 or higher, or an IP Office release 9.1 or higher, set **Include location specific information** to **On**.

Configuring unknown locations

Use this procedure to configure extensions where the location is unknown.

Procedure

1. In the navigation pane, select **Location**.
2. Enter **a Location Name**.
3. Set **Parent Location for CAC** to **Cloud**.
4. In the **Extension | Extn** tab, set the **Location** field to the location defined in step 2.

Overriding call barring

When a system or user short code is configured to bar outgoing calls, you can override call barring. Typically, this configuration is used for a phone in a shared or public area. By default, the phone has outgoing calls barred. The administrator can override call barring for specific dialed numbers by entering numbers with a record in the external directory. When the dialed number exists in the external directory and the **Directory Overrides Call Barring** setting is enabled, call barring is overridden.

The System Directory entries must use the format (shortcode)number. For example, if the number to dial is 61234, where 6 is the shortcode used to dial externally and 1234 is the number, the System Directory entry must be (6)1234. If the dial shortcode contains a name string rather than digits, then **Directory Overrides Call Barring** will not work.

The **Directory Overrides Barring** setting is located on the **System | Telephony | Telephony** tab.

For information on the directory, see the description for the **System | Directory Services** tab.

Server Edition configuration

For Server Edition deployments, the **Directory Overrides Barring** must be enabled on each node. It is not a system wide setting.

For example, if the Primary Server uses an IP500 v2 expansion system as an ISDN gateway, **Directory Overrides Barring** must be enabled on the Primary Sever for Primary Server users dialing on external ISDN lines. For the IP500 v2 expansion users, **Directory Overrides Barring** must be enabled on the IP500 v2 expansion system.

It is recommend that the short code configured to dial externally on ISDN lines be the same on all nodes. For example, if Primary Server users and IP500 v2 expansion users want to reach PSTN number 123456789 on ISDN lines, configure the dial codes as follows.

- Primary Server: 6N/Dial/6N/XX (XX is the line group ID for the SCN line)
- IP 500 v2 expansion: 6N/Dial/N/YY (YY is the line group ID for ISDN line)
- Directory Entry number defined on Primary Server: (6)123456789

Chapter 13: Configure Server Edition system settings

Opening the System Configurations

Manager is used to configure the telephony settings of the Server Edition systems by loading the configuration of the Primary Server server. During that process it will automatically also attempt to load the configuration of any Secondary Server and expansion systems associated with the Primary Server.

Opening the Configuration in Manager

1. Start Manager.

   If you do not have Manager installed, it can be downloaded and installed from the Primary Server.

2. Click on  or select **File | Open Configuration**. The Select IP Office window appears, listing those systems that responded.

   If Manager is not currently running in Server Edition mode, it will display any systems detected included Server Edition expansion systems and non-Server Edition systems.

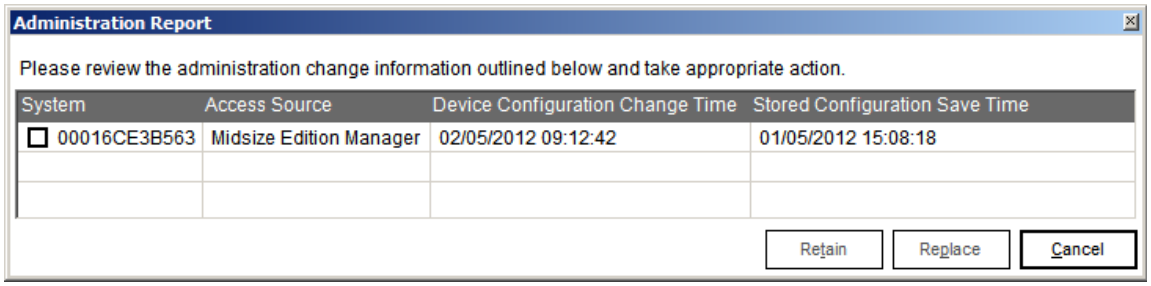
   a. Select the required Primary Server.
   b. Ensure that the Open with Server Edition Manager option is selected.
   c. The Use Remote Access option can be used to load the configuration using an SSL VPN service. This option is only displayed if **Use Remote Access for Multi-Site** is selected in the Manager application's preferences.
   d. Click **OK**.

3. If Manager is currently running in Server Edition mode, it will display any Primary Servers detected.

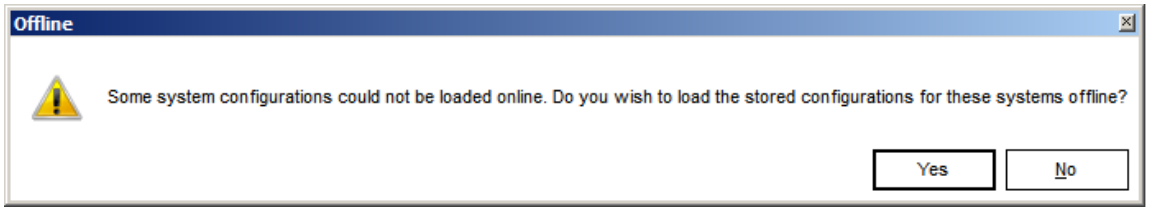
   a. Select the required Primary Server.
   b. The Use Remote Access option can be used to load the configuration using an SSL VPN service. This option is only displayed if **Use Remote Access for Multi-Site** is selected in the Manager application's preferences.
   c. Click **OK**.
   d. Enter a name and password for configuration access. The defaults are **Administrator** and **Administrator**.

e. A number of special windows may be displayed if the Server Edition mode Manager detects a problem.

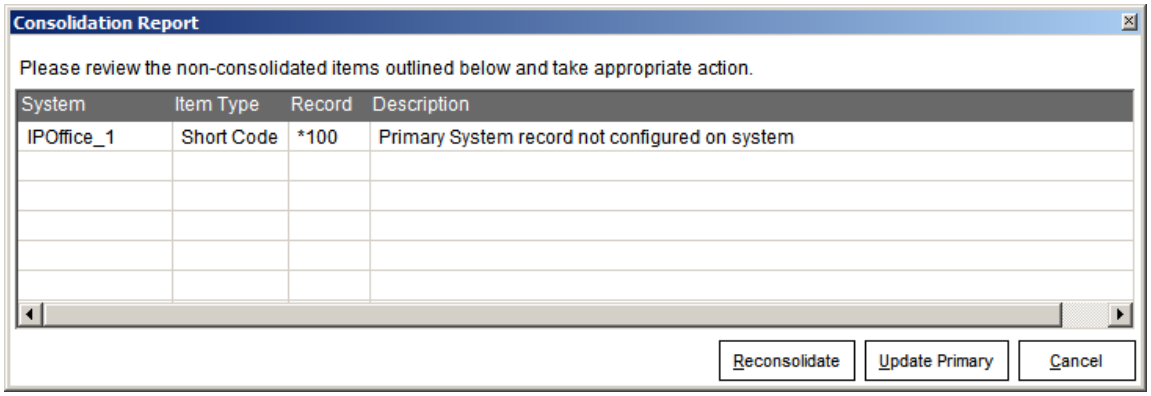
f. Each time a configuration is changed, as well as being sent to the system, a copy is stored on the Primary Server. The Administration Report is displayed if the time and date of the last change to a configuration differs from that of the last copy stored on the server. The menu allows you to select whether to use (**Retain**) the configuration just received or to replace (**Replace**) it with the stored copy.



g. The configuration of the Primary Server includes details of the Secondary Server and expansion systems and Manager automatically attempts to also load the configurations from those systems. If it cannot load the current configurations of those systems, it will offer to load the last copies of their configurations that it has stored on the Primary Server.



h. Once the configurations are loaded, Manager checks for inconsistencies between the settings that are common to all servers in the network. If it finds any inconsistencies, it displays a Consolidation Report listing the inconsistencies found and allowing them to be corrected.



4. Reconsolidate: Update the setting on the system to match that of the Primary Server.

5. Update Primary: Update the Primary Server setting to match that of the system. This will also affect all other servers in the network.

The configuration of the network and the servers can now be edited as required.

Opening Configurations in Non-Server Edition Mode Manager

By default, the configuration of Server Edition systems cannot be opened in Manager if it is not running in Server Edition mode. That behavior is controlled by the security settings of the servers. For Server Edition systems, the Service Access Source setting of the server's Configuration service is set to **Business Edition Manager**. If this setting is changed to **Unrestricted**, the Server Edition system can be opened in Manager in its normal **Advanced View** mode.

Warning:

Opening the configuration of a Server Edition system in Manager running in any mode other than Server Edition mode should be avoided unless absolutely necessary for system recovery. Even in that case, Manager will not allow renumbering, changes to the voicemail type and changes to H.323 lines.

Configuring the Systems

From the Server Edition Solution View, there are a number of ways to access the configuration settings of the systems.

Click on the  Configuration link on the right-hand edge of the menu. Then navigation pane for configuration records is displayed.

or

Using the drop-down options of the

navigation toolbar from left to right select the configuration record that you want to edit.

Saving Configuration Changes

After making configuration changes using Manager, the process of saving the changes performs several actions:

- The configurations are validated for consistency.
- For those systems for which configuration changes have been made, the new configuration is sent to that system.

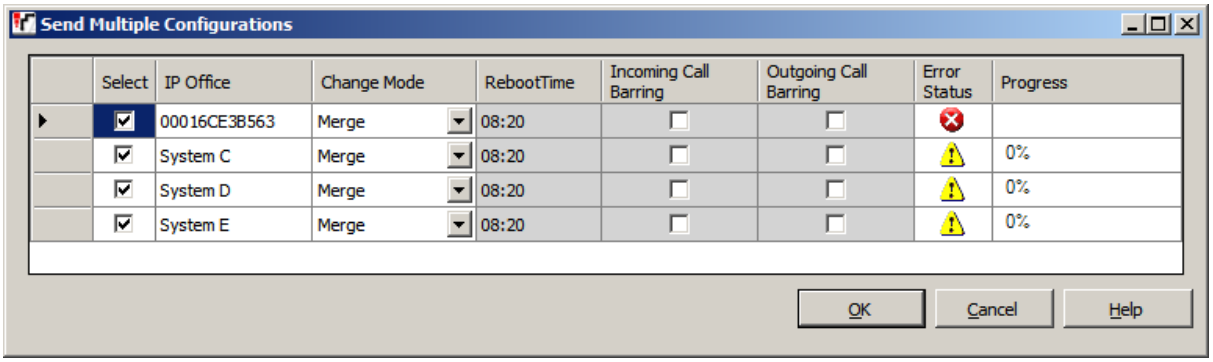
Manager defaults to rebooting those systems where a reboot is necessary for the configuration changes to come into effect.

A time stamped copy of the new configuration is also stored on the Primary Server server.

- For a new Secondary Server or expansion system added to the network configuration using the create off-line configuration option, the offline file is stored, allowing the new system to be configured even though not yet physically present.
- When opening the configuration from a network, if the timestamp of the stored copy differs from that of the actual system configuration, Manager will prompt for which configuration it should load for editing.

Saving Configuration Changes

1. Click in the main toolbar or select **File | Save Configuration** from the menu bar.
2. The menu displayed only shows details for those systems where the system configuration has been changed and needs to be sent back to the system.



- **Select** By default all systems with configuration changes are selected. If you want to exclude a system from having its configuration updated, either deselect it or cancel the whole process.
- **Change Mode** If Manager thinks the changes made to the configuration settings are mergeable, it will select **Merge** by default, otherwise it will select **Immediate**.
- **Merge** Send the configuration settings without rebooting the system. This mode should only be used with settings that are mergeable. Refer to Mergeable Settings.
- **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. This mode can be combined with the **Incoming Call Barring** and **Outgoing Call Barring** options.
- **Store Offline** It is possible to add a reference for a Server Edition Secondary or for a Server Edition Expansion System to create a configuration file for that system even though it is not physically present. Store Offline saves that configuration on the Server Edition Primary in its file store. The same file is retrieved from there until such time as the physical server is present at which time you are prompted whether to use the stored file or the actual servers current configuration.

- **Timed** The same as **When Free** but waits for a specific time after which it then wait for there to be no calls in progress. The time is specified by the **Reboot Time**. This mode can be combined with the **Incoming Call Barring** and **Outgoing Call Barring** options.
- **Reboot Time** This setting is used when the reboot mode **Timed** is selected. It sets the time for the system reboot. If the time is after midnight, the system's normal daily backup is canceled.
- **Incoming Call Barring** This setting can be used when the reboot mode **When Free** or **Timed** is selected. It bars the receiving of any new calls.
- **Outgoing Call Barring** This setting can be used when the reboot mode **When Free** or **Timed** is selected. It bars the making of any new calls.

Click **OK**. The progress of the sending of each configuration is displayed.

Starting System Status

The System Status Application is an application that can be used to view the status of a system and activity on the system. System Status Application can be started via Manager.

Using the following method automatically starts System Status Application with information about the system being monitored.

1. In the Server Edition Solution View, select the system for which you want to view its status.
2. Click on the  **System Status** link on the right-hand edge of the menu.
3. A copy of the System Status Application application hosted by the system is started.

Alternate Method

If System Status Application is installed as an application on the same PC as Manager, it can be started locally. When started this way, it will be necessary to manually enter the IP address and other details of the system you want to monitor after starting System Status Application.

Click **File | Advanced | System Status**.

Voicemail Administration

If the Voicemail Pro client application is installed on the same PC as Manager, it can be launched from Manager. If not already installed, the Voicemail Pro client application can be downloaded from the Primary Server via its web control menus. Refer to the Server Edition Deployment Guide.

Starting the Voicemail Pro Client

Using the following method automatically starts the Voicemail Pro client with information about the system to be administered.

1. In the Server Edition Solution View, select the server for which you want to administer the voicemail application that the server hosts. This can be either the Primary Server or

Secondary Server. If **Solution** is selected, it is assumed that the voicemail server on the Primary Server is being administered.

2. Click on the  **Voicemail Administration** link on the right-hand edge of the menu.

Alternate Method

The Voicemail Pro client can . When started this way, it will be necessary to manually enter the IP address and other details of the system you want to monitor after starting the System Status Application.

Click **File | Advanced | Launch Voicemail Pro Client**.

Configuring Resiliency

Within the Server Edition network, some functions hosted by a particular system can be taken over by another system in the event of a system failure or loss of network link. That behaviour is referred to as fallback or resilience.

The options that can be supported in fallback are:

IP Phones This option is used for Avaya 9600 Series phones registered with the system. When selected, it will share information about the registered phones and users on those phones with the other system.

- If the local system is no longer visible to the phones, the phones will reregister with the other system. The users who were currently on those phones will appear on the other system as if they had hot desked.
- Note that when the local system is restored to the network, the phones will not automatically re-register with it. A phone reset via either a phone power cycle or using the System Status Application is required.
- When phones have registered with the other system, they will show an **R** on their display.

If using resilience backup to support Avaya IP phones, **Auto-create Extn** and **Auto-create User** should not be left enabled after initial configuration or any subsequent addition of new extensions and users. Leaving auto-create options enabled on a system that is a failover target may cause duplicate extension/user records on the multi-site network under multiple failure scenarios.

Hunt Groups When selected, any hunt groups the local system is advertising to the network are advertised from the other system when fallback is required. The trigger for this occurring is Avaya H.323 phones registered with the local system registering with the other system, ie. **Backs up my IP Phones** above must also be enabled. In a Server Edition network this option is only available on the H.323 trunk from the Primary Server to the Secondary Server.

When used, the only hunt group members that will be available are as follows:

- If the group was a distributed hunt group, those members who were remote members on other systems still visible within the network.
- Any local members who have hot desked to another system still visible within the network.

When the local system becomes visible to the other system again, the groups will return to be advertised from the local system.

Voicemail In a Server Edition network this option is available on the H.323 trunk from the Primary Server to the Secondary Server. It is assumed as being on and is automatically set by the **Resilience Administration** tool.

This option requires the other system to have licenses for the Voicemail Pro features that are required to operate during any fallback period.

Notes

Fallback handover takes approximately 3 minutes. This ensure that fallback is not invoked when it is not required, for example when the local system is simply being rebooted to complete a non-mergeable configuration change.

Fallback is only intended to provide basic call functionality while the cause of fallback occurring is investigated and resolved. If users make changes to their settings while in fallback, for example changing their DND mode, those changes will not apply after fallback.

If the fallback system is rebooted while it is providing fallback services, the fallback services are lost.

Fallback features require that the IP devices local to each system are still able to route data to the fallback system when the local system is not available. This will typically require each system site to be using a separate data router from the system.

When an IP Phone re-registers to a secondary IP Office on the failure of the primary control unit, the second system will allow it to operate indefinitely as a “guest”, but only until the system resets. Licenses will never be consumed for a guest IP phone.

Remote hot desking users on H323 extensions are automatically logged out.

Setting Up Resilience

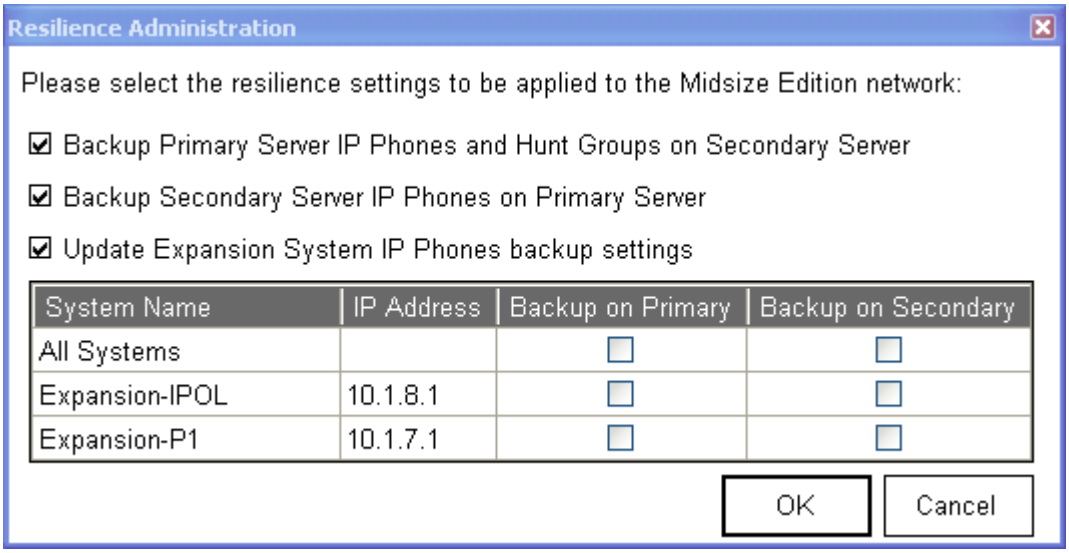
About this task

This process adjusts the individual settings of the H.323 IP lines between systems to indicate which lines are being used to give/receive fallback options and what fallback options.

Procedure

1. In the Server Edition Solution View, select the  **Secondary Server** link on the right.
2. The **Resilience Administration** menu is displayed.

   Select the options required.



- **Backup Primary Server IP Phones and Hunt Groups on Secondary Server** When selected, the Secondary Server will support hunt group operation during any failure of the Primary Server. Also when selected, the Secondary Server will support the continued operation of Avaya IP phones normally registered to the Primary Server.
- **Backup Secondary Server IP Phones on Primary Server** When selected, the Primary Server will support the continued operation of Avaya IP phones normally registered to the Secondary Server.
- **Update Expansion System IP Phones backup settings** Select whether Avaya IP phones registered to the system can fallback to either the Primary Server or the Secondary Server during any failure of the expansion system.

3. Select the options required and click **OK**.
4. The individual **Supplementary Services** and **SCN Backup Options** settings of the H.323 IP lines in each system are adjusted to match the selections.

Configuring Location Based Extension Resiliency

On Server Edition deployments, you can configure a group of phones to fall back to a specific node. Define the fallback group by assigning each phone to a location. The location based fallback overrides the system fallback configuration. Location based resiliency is support on the following phones.

- 96x1
- 96x0
- 16xx

Procedure

1. In Manager, open the **Location** page and define a location for the phone group.

2. If the phone group is in a remote location, you can define the **Time Settings** for the group.
3. In the **Fallback System** field, select the system where the phone group will fall back to.

   Note that the **Fallback System** list only contains systems where an IP Office Line has been configured.
4. Save the location.
5. For all phones that will be part of the group, open the extension page for the phone and select the new **Location**.

   Note that you can also set an IP address and subnet mask at the location level to match the phone IP addresses.
6. On the system where the extension is configured, open the **Line | IP Office Line** page.
7. Under **SCN Backup Options**, enable **Supports Fallback**.

Adding a Secondary Server

The Server Edition Solution View can be used to add details of a Secondary Server server to the network configuration. This process automatically adds the necessary H.323 IP trunks for connection to the new server into the configuration of the other servers already in the network.

Adding a Secondary Server

About this task

Procedure

1. In the Server Edition Solution View, select the  **Secondary Server** link on the right.
2. Enter the **IP Address** of the server and click **OK**.

   Alternatively, click on the browse icon to display the Select IP Office menu to select a discovered system.
3. The next steps depend on whether a system is found at the address specified:
4. **Physical System Found** The following process is applied if there is a server at the address specified.

   - If you select **No**: The new system is added to the network configuration but cannot be edited.
   - If you select **Yes**: You are taken through the process of creating a basic offline configuration for the system. That configuration is then editable in Manager as part of the

Server Edition network configuration. When the configuration is saved, a copy of it is saved on the Primary Server server.

a. The Offline Configuration Creation menu is displayed.

   Set the **Locale** and, if required, the **Extension Number Length**.

b. Click **OK**.

c. The Avaya IP Office Initial Configuration menu is now displayed.

   Complete the settings and click **Save**.

Next steps

Additional Configuration Required

The addition of a secondary server or expansion system requires updates to the configuration of the one-X Portal for IP Office in order to support that system. The details of how to add the provider entries required in the one-X Portal for IP Office configuration refer to the one-X Portal for IP Office Administration Manual.

Adding an Expansion System

The Server Edition Solution View can be used to add details of a new Expansion System (L) or Expansion System (V2) to the network configuration. This process automatically adds the necessary H.323 IP trunks for connection to the new server into the configuration of the other servers already in the network.

Adding an Expansion System

About this task

Procedure

1. In the Server Edition Solution View, select the **Expansion System** link on the right.
2. Enter the **IP Address** of the server and click **OK**.

   Alternatively, click on the browse icon to display the Select IP Office menu to select a discovered system.
3. The next steps depend on whether a system is found at the address specified:
4. **Physical System Found** The following process is applied if there is a server at the address specified.

   a. The **Initial Configuration** menu is displayed, with the fields pre-filled with the current settings of the system.

   b. Update the fields as required.

      For example, you can change the IP address settings.

c. Click **Save**.

d. The system is rebooted.

   Click **OK**.

e. The icon in the **Description** column will alternate between green and grey until the system reboot is complete.

5. **Physical System Not Found** The following process is applied in no server is found at the address specified. It allows the option of creating an offline configuration for the new system that can be saved and applied to that system when it is connected to the network.

   Manager prompts whether you want to run the offline configuration tool. This is used to specify the type of physical server and for Expansion System (V2) the hardware fitted in the system.

   - If you select **No**: The new system is added to the network configuration but cannot be edited.
   - If you select **Yes**: You are taken through the process of creating a basic offline configuration for the system. That configuration is then editable in Manager as part of the Server Edition network configuration. When the configuration is saved, a copy of it is saved on the Primary Server server.

   a. The Offline Configuration Creation menu is displayed.

      Set the **Locale** and, if required, the **Extension Number Length**.

   b. In **System Units**, select either a Expansion System (L) or Expansion System (V2).

   c. For a Expansion System (V2), select the other hardware options to match the components installed in the system.

      Click **OK**.

   d. The Avaya IP Office Initial Configuration menu is now displayed.

      Complete the settings and click **Save**.

Next steps

Additional Configuration Required

The addition of a secondary server or expansion system requires updates to the configuration of the one-X Portal for IP Office in order to support that system. The details of how to add the provider entries required in the one-X Portal for IP Office configuration refer to the one-X Portal for IP Office Administration Manual.

Displaying the System Inventories

The method for displaying the system inventory depends on what is currently being displayed by Manager.

In the Server Edition Solution View, using the table at the bottom of the menu, click on the server for which you want to display the system inventory. Click on **Network** for the inventory of the Server Edition network.

or

In the navigation pane, click on the  icon of the server for which you want to display the system inventory. Click on the  **Network** icon for the inventory of the Server Edition network.

Removing an Expansion/Secondary Server

About this task

Manager can be used to remove a Secondary Server, Expansion System (L) or Expansion System (V2) from the network. Doing this removes all configuration records for the server from the network. It also removes details of any H.323 IP trunks to the removed system from the configuration of other systems.

Removing an Expansion or Secondary Server

Procedure

1. In the Server Edition Solution View, right-click on the server to be removed in the table at the bottom of the menu.
2. Select **Remove**.
3. Select **Yes** to confirm the removal.

Synchronizing the Configurations

About this task

Normally during configuration of the Server Edition solution, records that are shared (Incoming Call Route, Time Profile, Account Code and User Rights) are automatically synchronized with the configuration of the individual servers as they are edited. However, when new servers are added to the network or systems have their configuration individually edited, it is possible that some share records may become out of synch with the Primary Server. This process can be used to re-establish the correct shared records.

Synchronizing the Configurations

Procedure

1. In the Server Edition Solution View, right-click on **Solution**.
2. Select **Synchronize Configurations**.
3. Select **Yes** to confirm the removal.

Displaying the Solution View

Manager normally starts with the Server Edition Solution View when the configuration for a Server Edition network is loaded. However, there are a number of ways to return to the solution view at any time.

Click on the **Server EditionSolution View** icon in the toolbar.

or

Click on the **Solution** icon in the navigation pane.

Starting Web Control

About this task

Web control is the term used for a set of web based administration menus used by Linux based servers. That includes the Primary Server, Secondary Server and Expansion System (L) in a Server Edition solution. The menus provide functions such as stopping and starting individual services being run by the server. The menus for the Primary Server provide special network functions such as backing up and upgrading the whole network.

Starting System On-Boarding

Procedure

1. In the Server Edition Solution View, select the system for which you want to display its web control menus.

   The option is not available for Expansion System (V2).

2. Click on the **Web Control** link on the right-hand edge of the menu.
3. The PCs default web browser is started with the address to the system.
4. When the login menu is displayed, login using the same configuration name and password as used for Manager configuration access.

On-boarding

About this task

On-boarding is a process used to register a system for support and to upload a settings file that configures an SSL VPN connection that can then be used for remote support. The on-boarding process is done through a set of web browser based configuration menus.

For full details on how to configure and administer SSL VPN services, refer to the Avaya IP Office SSL VPN Solutions Guide.

Starting System On-Boarding

Procedure

1. In the Server Edition Solution View, select the system for which you want to on-board.
2. Click on the  **On-boarding** link on the right-hand edge of the menu.
3. The PCs default web browser is started with the address to the system.
4. From the menu that is displayed select IP Office Web Management.
5. When the login menu is displayed, login using the same configuration name and password as used for Manager configuration access.
6. When logged in, select **Tools** and then **On-boarding**.

Shared Administration

About this task

When managing multiple systems, it may be useful to create a common user name and password on all the systems for configuration access. This tool can be used to create a new service user account, **SCN_Admin**, for configuration access.

This process requires you to have a user name and password for security configuration access to each of the systems.

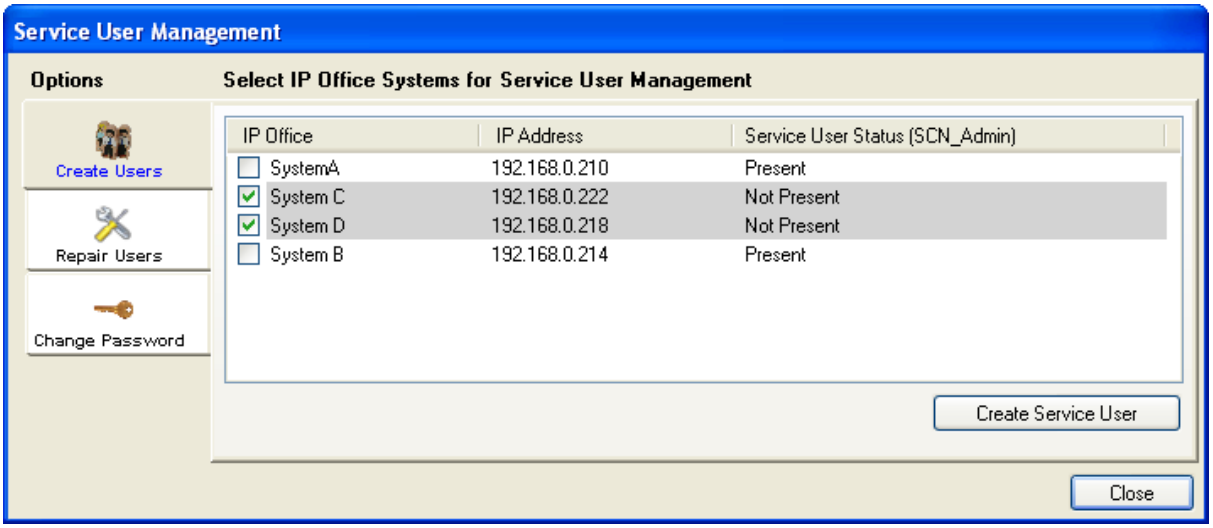
Managing a Common Configuration Administration Account

Procedure

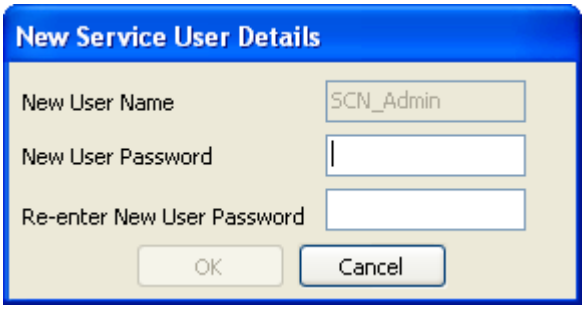
1. Select **Tools | Server Edition Service User Management**.
2. The **Select IP Office** menu displays the list of discovered systems.
3. Select the systems for which you want to create a common configuration account.

   Typically this should be all systems. Click **OK**.
4. A user name and password for security configuration access to each system is requested.

   Enter the values and click **OK**. If the same values can be used for all systems enter those values, select **Use above credentials for all remaining, selected IPOs**. If each system requires a different security user names and password, deselect **Use above credentials for all remaining, selected IPOs**.
5. The systems will be listed and whether they already have an **SCN_Admin** account is shown.



6. To create the **SCN_Admin** account on each system and set the password for those account click on **Create Service User**.



7. Enter the common password and click **OK**.
8. The password can be changed in future using the Change Password option.
9. Click **Close**.

Chapter 14: Configure user settings

Configuring User Rights

For most settings in a user rights template, the adjacent drop down list is used to indicate whether the setting is part of the template or not. The drop down options are:

- **Apply User Rights Value** Apply the value set in the user rights template to all users associated with the template.
  - The matching user setting is grayed out and displays a lock symbol.
  - Users attempting to change the settings using short codes receive inaccessible tone.
- **Not Part of User Rights** Ignore the user rights template setting.

Default User Rights

For defaulted systems, the following user rights are created as a part of the default configuration. Fields not listed are not part of the user rights.

Note:

When a user logs in as a Outbound Contact Express agent, the Outdialer user rights are automatically applied. When the agent logs out, the previous user rights are applied.

✓ = Set to On. ✗ = Set to Off. – = Not part of the user rights.

User Rights	Call Center Agent	Boss	Application	Default	IP Hard Phone	Mailbox	Paging	T3	Outdialer
Priority	✓ 5	✓ 5	✓ 5	✓ 5	✓ 5	✓ 5	✓ 5	✓ 5	✓ 5
Voicemail	–	–	–	–	–	✓	–	–	✗
Voicemail Ringback	✗	✗	✗	✗	✗	✗	–	✗	✗
Outgoing Call Bar	✗	✗	✗	✗	✗	✗	✗	✗	✓

Table continues…

User Rights	Call Center Agent	Boss	Application	Default	IP Hard Phone	Mailbox	Paging	T3	Outdialer
No Answer Time	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	0
Transfer Return Time	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	✓ 0	0
Individual Coverage Time	✓ 10	✓ 10	✓ 10	✓ 10	✓ 10	✓ 10	✓ 10	✓ 10	10
Busy on Held	✗	✗	✗	✗	✗	–	–	✗	✓
Call Waiting	✗	✗	✓	✗	✗	✗	✗	✓	✗
Can Intrude	✗	✗	✗	✗	✗	✗	✗	✗	✗
Cannot be Intruded	✗	✗	✓	✓	✓	✗	✗	✗	✗
Deny Auto Intercom Calls	–	–	–	–	–	–	–	–	✗
Enable Inhibit Off-Switch Forward/ Transfer	–	–	–	–	–	–	–	–	✓
Enable Outgoing Call Bar	–	–	–	–	–	–	–	–	✓
Centralized Logging	–	–	–	–	–	–	–	–	✗
Force Login	✓	–	–	–	–	–	–	–	
Force Account Code	✗	✗	✗	✗	✗	✗	✗	✗	

Table continues…

User Rights	Call Center Agent	Boss	Application	Default	IP Hard Phone	Mailbox	Paging	T3	Outdialer
Button Programming	1: a= 2: b= 4: HGEna 5: DNDOn 6: Busy	1: a= 2: b= 3: c= 6: DNDOn 7: Dial *17	✓	1: a= 2: b= 3: c=	1: a= 2: b= 3: c= 6: Dial *17	✓	-	✓	1: a= 2: b= 3: Supervisor 4: Extn Logout

Related Links

Adding User Rights on page 625
Creating a User Right Based on an Existing User on page 625
Associating User Rights to a User on page 626
Copy User Rights Settings over a User's Settings on page 626

Adding User Rights

About this task

Procedure

1. Select **User Rights**.
2. Click and select **User Rights**.
3. Enter a name.
4. Configure the user rights as required.
5. Click **OK**.

Related Links

Configuring User Rights on page 623

Creating a User Right Based on an Existing User

About this task

Procedure

1. Select **User Rights**.
2. In the group pane, right-click and select **New User Rights from a User**.
3. Select the user and click **OK**.

Related Links

Configuring User Rights on page 623

Associating User Rights to a User

About this task

Procedure

1. Select  **User Rights** or  **User**.
2. In the group pane, right-click and select **Apply User Rights to Users**.
3. Select the user rights to be applied.
4. On the **Members of this User Rights** sub tab select the users to which the user rights should be applied as their Working Hours User Rights.
5. On the **Members when out of hours** sub tab select which users should use the selected user rights as their out of hours user rights.
6. Click **OK**.

Related Links

Configuring User Rights on page 623

Copy User Rights Settings over a User's Settings

About this task

This process replaces a user's current settings with those that are part of the selected user rights. It does not associate the user with the user rights.

Procedure

1. Select  **User Rights**.
2. In the group pane, right-click and select **Copy user rights values to users**.
3. Select the user rights to be applied.
4. Click **OK**.

Related Links

Configuring User Rights on page 623

Account Code Configuration

Forcing Account Code Entry for Specific Numbers

Account code can be set a being required for any dialing that matches a particular short code. This is done by ticking the Force Account Code option found in the short code settings. Note that the

account code request happens when the short code match occurs. Potentially this can be in the middle of dialing the external number, therefore the use of **X** wildcards in the short code to ensure full number dialing is recommended.

Entering Account Codes

The method for entering account codes depends on the type of phone being used. Refer to the relevant telephone User's Guide for details.

Account Code Button:

The Account Code Entry action (**User | Button Programming | Emulation | Account Code Entry**) and Set Account Code action (**User | Button Programming | Advanced | Set | Set Account Code**) can be assigned to a programmable button on some phones. They both operate the same. The button can be preset with a specific account code or left blank to request account code entry when pressed. The button can then be used to specify an account code before a call or during a call.

Setting an Account Code using Short Codes:

The **Set Account Code** feature allows short codes to be created that specify an account code before making a call.

Show Account Code Setting :

This setting on the **System | Telephony | Telephony** tab controls the display and listing of system account codes.

When on and entering account codes through a phone, the account code digits are shown while being dialed.

When off and eentering account codes through a phone, the account code digits are replaced by **s** characters on the display.

Server Edition Account Code Management

Accounts codes configured on Server Edition are shared by all systems in the network.

Related Links

Setting a User to Forced Account Code on page 627

Setting a User to Forced Account Code

Procedure

1. Receive the system configuration if one is not opened.
2. In the left-hand panel, click **User**. The list of existing user is shown in the right-hand panel.
3. Double-click the required user.
4. Select the **Telephony** tab.
5. Tick the Force Account Code option.
6. Click **OK**.
7. Merge the configuration.

Related Links

Account Code Configuration on page 626

Mobile Call Control

Mobile call control is only supported on digital trunks including SIP trunks. It allows a user receiving a call on their twinned device to access system dial tone and then perform dialing action including making calls and activating short codes.

After answering a twinned call, the Mobile Call Control user can dial ** (within 1 second of each other) to place that call on hold and instead get dial tone from the system. Any dialing is now interpreted as if the user is logged into a basic single line extension on the system using their user settings. That also include user BLF status indication.

Licenses are required in the system configuration for all the users that will be configured for any of the mobility features including Mobile Call Control and one-X Mobile Client usage. The same licenses also allows the user to use other mobility features such as mobile twinning, mobile call control and one-X Mobile if required.

- Users licensed for a Profile of **Mobile Worker** or **Power User** are able to use mobility features.
- Mobility features are available for all users independent of their user profile. They are enabled for the whole system by the **Essential Edition** license.
- If a Mobile Call Control user remote hot desks to another system within a multi-site network, they take their licensed status with them rather than consuming or requiring a license on the remote system.

Trunk Restrictions Mobile call control is only supported on systems with trunk types that can give information on whether the call is answered. Therefore, mobile call control is not supported on analog or T1 analog trunks. All other trunk types are supported (ISDN PRI and BRI, SIP, H323).

Routing via trunks that do not support clearing supervision (disconnect detection) should not be used.

DTMF detection is applied to twinned calls to a user configured for this feature. This will have the following effects:

DTMF dialing is muted though short chirps may be heard at the start of any DTMF dialing.

DTMF dialed by the user will not be passed through to other connected equipment such as IVR or Voicemail.

Warning:

This feature allows external callers to use features on your phone system and to make calls from the phone system for which you may be charged. The only security available to the system is to check whether the incoming caller ID matches a configured users' **Twinned Mobile Number** setting. The system cannot prevent use of these features by caller's who present a false caller ID that matching that of a user configured for access to this feature.

Mobile Call Control Features and FNE Services

Mobile call control uses a short code set to invoke an FNE service. The codes relevant to mobile call control are summarized below.

FNE 31 = Mobile Call Control This code allows a user called or calling the system to invoke mobile call control and to then handle and make calls as if they were at their system extension.

FNE 32 = Mobile Direct Access Mobile direct access FNE32 immediately redials on switch the DDI digits received with the call rather than returning dial tone and waiting for DTMF digits as with FNE31 .

FNE 33 = Mobile Callback Mobile callback allows the user to call the system and then hang up. The system will then make a call to the user's CLI and when answered, provide them with dial tone from the system to make calls.

Using Mobile Call Control

In addition to using ** to access mobile call control, the user has access to the following additional controls:

- **Clearing a Call: *52** It may be necessary to clear a connected call, for example after attempting a transfer and hearing voicemail or ringing instead. To do this dial **** for dial tone and then ***52** (this is a default system short code and can be changed if required).
- **Return to Dial Tone: ##** Return to dial tone after getting busy, number unobtainable or short code confirmation tones from the system.

Enabling Outgoing Mobile Call Control

1. **License Mobile Features** Enter the licenses for Mobile Twinning and confirm that they are valid by merging and retrieving the configuration.
2. **Configure the user for Mobile Twinning and Mobile Call Control** On the User | Mobility tab do the following:

- Enable **Mobility Features** for the user.
- Set the **Twinned Mobile Number** for the user's twinned calls destination.
- Digits are matched from right to left.
- The match must be at least 6 digits. If either the CLI or the Mobile Twinned Number is less than 6 digits no match will occur.
- Matching is done for up to 10 digits. Further digits are ignored. If either the CLI or Mobile Twinned Number is less than 10 digits, matching stops at that shorter length.
- If multiple matches occur the first user in the configuration is used. Manager will warn against configuration where such a conflict may exist.

Select **Can do Mobile Call Control**.

On systems with some unsupported trunk types, further changes such as Outgoing Group ID, system shorts codes and ARS may be necessary to ensure that calls to the mobile twinned numbers are only routed via the

Incoming Mobile Call Control

The system can be configured to allow Mobile Call Control users to use this function when making an incoming call to the system. This requires the user to make the incoming call from the same CLI as their Mobile Twinning Number (even if they do not actually use Mobile Twinning).

The call will be rejected:

- If the caller ID is blank or withheld.
- If the caller ID does not match a Twinned Mobile Number of a user with Can do Mobile Call Control enabled.
- If the call is received on a trunk type that does not support Mobile Call Control.

Enabling Incoming Mobile Call Control

License Mobile Features Enter the licenses for Mobile Twinning and confirm that they are valid by merging and retrieving the configuration.

Configure the user for incoming Mobile Call Control On the User | Mobility tab do the following:

- Enable **Mobility Features** for the user.
- Set the **Twinned Mobile Number** to match the CLI of the device from which the user will be making calls.
- Select **Can do Mobile Call Control**.

 **Add a FNE Short Code** In the system short codes section of the configuration add a short code similar to the following. Key points are the use of the **FNE Service** feature and the **Telephone Number** value **31**.

- **Short Code**: *89
- **Feature**: FNE Service
- **Telephone Number**: 31

 **Add an Incoming Call Route for the user** Create an incoming call route that matches the user's CLI and with the FNE short code created above as its destination.

On systems with some unsupported trunk types, further changes such as Incoming Group ID changes may be necessary to ensure that only calls received on trunks that support Mobile Call Control are routed to this short code.

Related Links

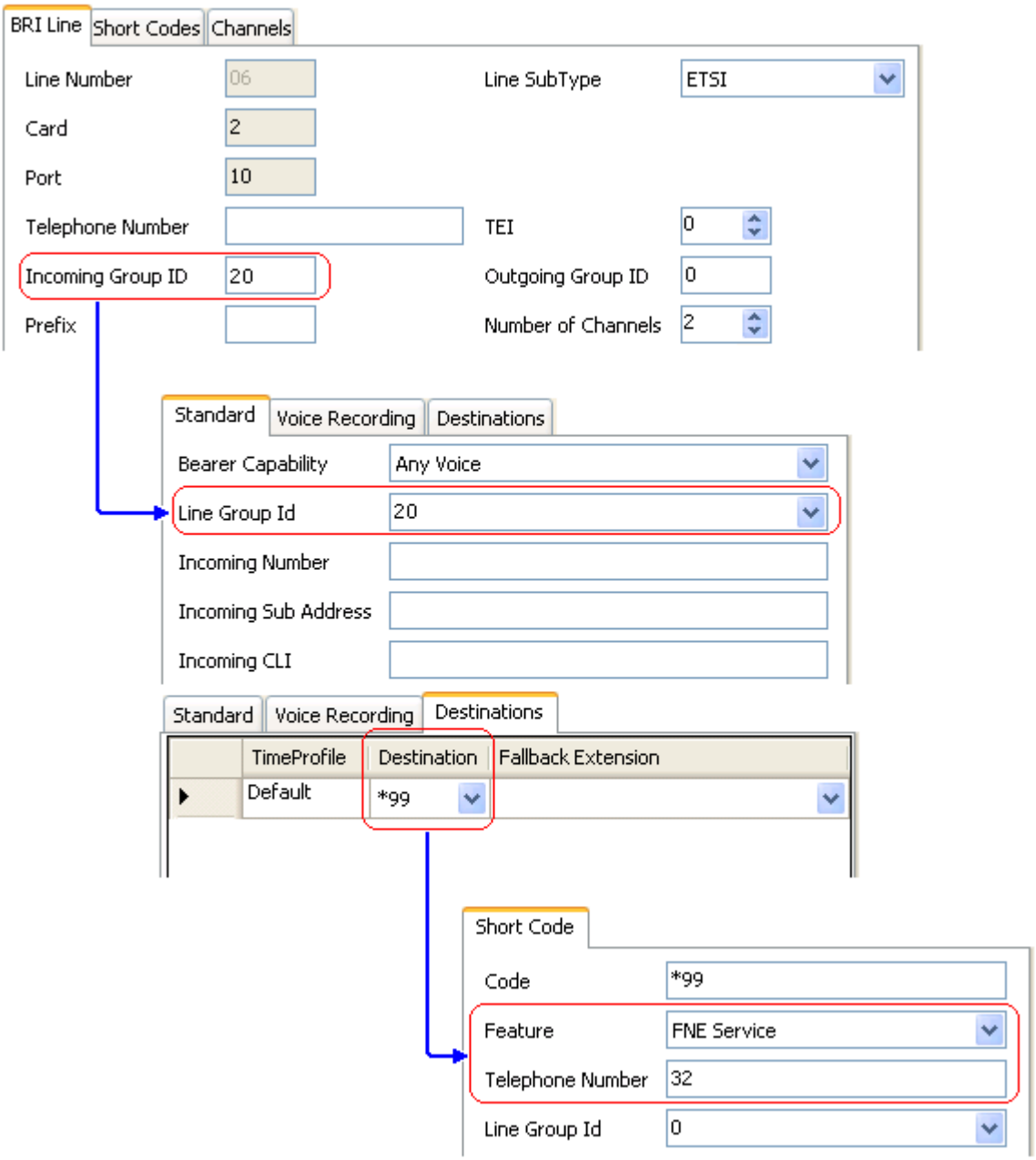
Mobile Direct Access (MDA) on page 630
Mobile Callback on page 632

Mobile Direct Access (MDA)

For a Mobile Call Control or one-X Mobile client user, FNE32 immediately redials on switch the DDI digits received with the call rather than returning dial tone and waiting for DTMF digits as with FNE31. This is called Mobile Direct Access (MDA).

MDA requires the user's external telephony provider to provide a direct trunk with DDI to the system (ie. an ISDN or SIP trunk). By assigning a specific incoming line group ID to the trunk, an incoming call route can be created for the same line group ID with blanks incoming number and incoming CLI fields. The destination is a short code set to FNE32.

User validation is performed using the CLI in the same way as for normal Mobile Call Control. In addition the call will be rejected no DDI digits are provided. Once connected the user can use the other Mobile Call Control features such as **.



Related Links

Mobile Call Control on page 628

Mobile Callback

Mobile callback allows the user to call the system and then hang up. The system will then make a call to the user's CLI and when answered, provide them with dial tone from the system to make calls.

Mobile callback is subject to all the normal trunk type and user licensing restrictions of mobile call control. In addition the user must have the **Mobile Callback** (**User | Mobility**)setting enabled in the system configuration.

When the user makes a call using a DDI that is routed to an FNE33 short code, the system will not connect (answer) the call but will provide ringing while it waits for the user to hang up (after 30 seconds the system will disconnect the call).

- The system will reject the call if the CLI does not match a user configured for Mobile Callback or does not meet any of the other requirements for mobile call control.
- The system will reject calls using FNE33 if the user already has a mobile twinning or mobile call control call connected or in the process of being connected. This includes a mobile callback call in the process of being made from the system to the user.

If the CLI matches a user configured for mobile callback and they hang up within the 30 seconds, the system will within 5 seconds initiate a callback to that user's CLI.

- If the call is answered after the user's **Mobile Answer Guard** time and within the user's **No Answer Time**, the user will hear dial tone from the system and can begin dialling as if at their system extension.
- If the call is not answered within the conditions above it is cleared and is not reattempted.

Related Links

Mobile Call Control on page 628

Twinning

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

	Internal	Mobile
Twinning Destination	Internal extensions only	External numbers only.
Supported in	All locales.	All locales.
License Required	No	No

User BLF indicators and application speed dials set to the primary user will indicate busy when they are connected to a twinned call including twinned calls answered at the mobile twinning destination.

Do Not Disturb and Twinning

Mobile Twinning

Selecting DND disables mobile twinning.

Internal Twinning

- Logging out or setting do not disturb at the primary stops twinned calls alerting at the secondary also.
- Logging out or setting do not disturb at the secondary only affects the secondary.

Do Not Disturb Exceptions List

For both types of twinning, when DND is selected, calls from numbers entered in the user's Do Not Disturb Exception List are presented to both the primary and secondary phones.

Internal Twinning

Internal twinning can be used to link two system extensions to act as a single extension. Typically this would be used to link a users desk phone with some form of wireless extension such as a DECT or WiFi handset.

Internal twinning is an exclusive arrangement, only one phone may be twinned with another. When twinned, one acts as the primary phone and the other as the secondary phone. With internal twinning in operation, calls to the user's primary phone are also presented to their twinned secondary phone. Other users cannot dial the secondary phone directly.

- If the primary or secondary phones have call appearance buttons, they are used for call alerting. If otherwise, call waiting tone is used, regardless of the users call waiting settings. In either case, the **Maximum Number of Calls** setting applies.
-
- Calls to and from the secondary phone are presented with the name and number settings of the primary.
- The twinning user can transfer calls between the primary and secondary phones.
- Logging out or setting do not disturb at the primary stops twinned calls alerting at the secondary also.
- Logging out or setting do not disturb at the secondary only affects the secondary.
- User buttons set to monitor the status of the primary also reflect the status of the secondary.
- Depending on the secondary phone type, calls alerting at the secondary but then answered at the primary may still be logged in the secondary's call log. This occurs if the call log is a function of the phone rather than the system.
- Call alerting at the secondary phone ignoring any **Ring Delay** settings applied to the appearance button being used at the primary phone. The only exception is buttons set to No Ring, in which case calls are not twinned.

The following applies to internal twinned extensions:

If using a T3, 1400, 1600, 9500 or 9600 Series phone as the secondary extension:

- The secondary extension's directory/contacts functions access the primary user's Centralized Personal Directory records in addition to the Centralized System Directory.

- The secondary extension's call Log/call List functions access the primary user's Centralized Call Log.
- The secondary extension's redial function uses the primary users Centralized Call Log. Note that the list mode or single number mode setting is local to the phone.

It is also shown on 3700 Series phones on a DECT R4 system installed using system provisioning .

For all phone types, changing the following settings from either the primary or secondary extension, will apply the setting to the primary user. This applies whether using a short code, programmable button or phone menu. The status of the function will be indicated on both extensions if supported by the extension type.

- Forwarding settings.
- Group membership status and group service status.
- Voicemail on/off.
- Do Not Disturb on/off and DND Exceptions Add/Delete.

Mobile Twinning

This method of twinning can be used with external numbers. Calls routed to the secondary remain under control of the system and can be pulled back to the primary if required. If either leg of an alerting twinned call is answered, the other leg is ended.

Mobile twinning is only applied to normal calls. It is not applied to:

- Intercom, dial direct and page calls.
- Calls alerting on line appearance, bridged appearance and call coverage buttons.
- Returning held, returning parked, returning transferred and automatic callback calls.
- Follow me calls.
- Forwarded calls except if the user's **Forwarded Calls Eligible for Mobile Twinning** setting is enabled.
- Hunt group calls except if the user's **Hunt Group Calls Eligible for Mobile Twinning** setting is enabled.
- Additional calls when the primary extension is active on a call or the twinning destination has a connected twinned call.

A number of controls are available in addition to those on this tab.

Button Programming Actions:

The **Emulation | Twinning** action can be used to control use of mobile twinning. Set on the primary extension, when that extension is idle the button can be used to set the twinning destination and to switch twinning usage on/off. When a twinned call has been answered at the twinned destination, the button can be used to retrieve the call at the primary extension.

Mobile Twinning Handover:

When on a call on the primary extension, pressing the **Twinning** button will make an unassisted transfer to the twinning destination. This feature can be used even if the user's **Mobile Twinning** setting was not enabled.

- During the transfer process the button will wink.

- Pressing the twinning button again will halt the transfer attempt and reconnect the call at the primary extension.
- The transfer may return if it cannot connect to the twinning destination or is unanswered within the user's configured **Transfer Return Time** (if the user has no **Transfer Return Time** configured, a enforced time of 15 seconds is used).

Short Code Features:

The following short code actions are available for use with mobile twinning.

- **Set Mobile Twinning Number**.
- **Set Mobile Twinning On**.
- **Set Mobile Twinning Off**.
- **Mobile Twinned Call Pickup**.

Caller ID:

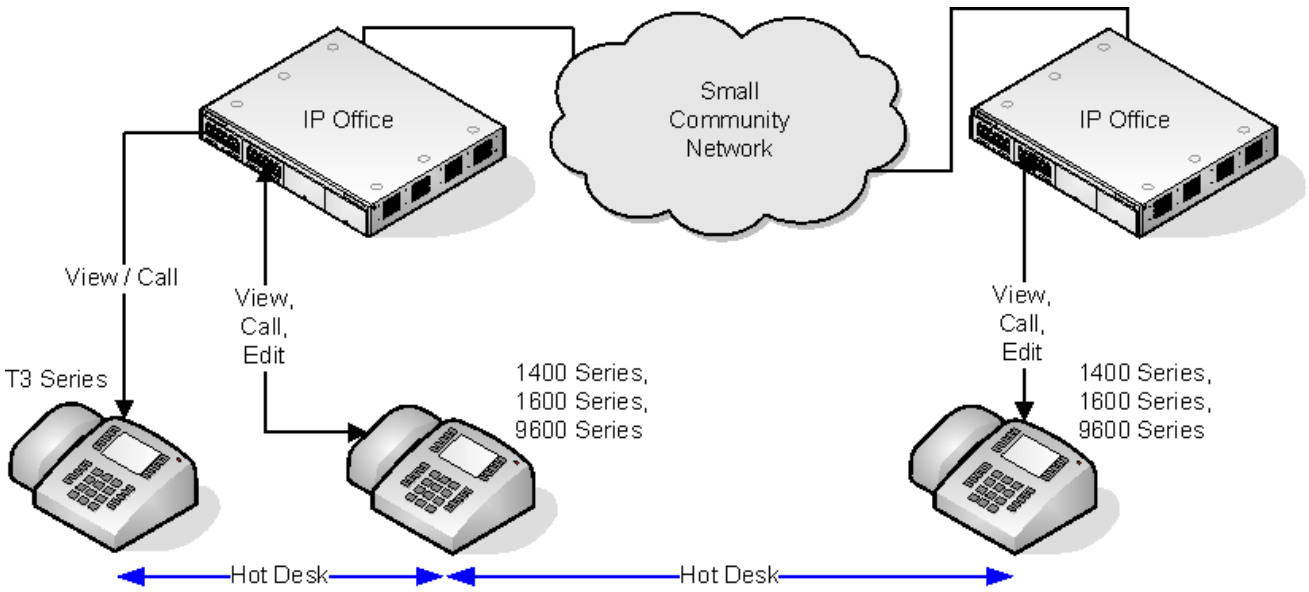
The options on the **System | Twinning** tab can be used to control which caller ID is sent with calls sent to the twinned destination. The use of those options may be restricted by the trunk type carrying the twinned call and the services provided by the line provider.

Centralized Personal Directory

Each system user is able to have up to 100 personal directory records stored by the system unless their home system limit has been reached (10800 total records).

A user's personal directory is also usable with 1400, 1600, 9500 and 9600 Series phones with a **CONTACTS** button. The user can view these records and use them to make calls.

1400, 1600, 9500 and 9600 Series phone users can edit their personal directory records through the phone. The user personal directory records can be edited using the Manager User | Personal Directory menu.



When the user hot desks to another phone that supports the centralized personal directory, their personal directory records become accessible through that phone. That also includes hot desking to another system in the network.

Users can also use and edit their personal directory records using one-X Portal for IP Office. Note that using one-X Portal for IP Office, users can have more that 100 personal directory records, with excess records stored by the one-X Portal server.

Centralized 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.

Call Log Information

The following information is included in each centralized call log record:

Information	Description

Table continues…

Name	The name, of the caller or the party called, if available. Up to 31 characters. This text is similar to that shown on the phone display of phones when they receive the call. For example, on forwarded call details of the original target and the caller name are included, eg. Bob > Sue.
Number	The number associated with the call. Up to 31 digits.
Tag	A text tag can be associated with calls by several different methods. See Call Tagging. Up to 31 characters. The tag is not shown within the call log display on phones.
Time and Date	The time and date of the call using the system time.
Duration	The call duration. For outgoing and answered calls this is the call connection time. For missed calls this is the call ringing time.
Record Type	Call log records can be **Incoming**, **Outgoing** or **Missed**. Note that these are calls to or from the user, not the phone, so it can include calls handled through a twinned device such as when using mobile call control. **Incoming** Calls to the user that the user then answered. This includes calls that the user answers on a twinned device. This also includes outgoing calls that are transferred to and answered by the user. **Outgoing** Calls made by the user. **Missed** Calls to the user that they did not answer. This includes calls while the user is logged off or in Do Not Disturb state. • Missed call records include an indication of what happened to the missed call. Options are **Answered by Another**, **Answered by Voicemail** or **Lost** (not answered on the system). • Missed call records are also marked as either acknowledged or unacknowledged. If the user's call log contains any unacknowledged call log records, the **Call Log** lamp is lit when using a 1608 or 1616 phone. From the phone, viewing an unacknowledged record changes it to acknowledged. • If the user has also be configured to included missed hunt group calls in their call log, those are also marked as acknowledged or unacknowledged.

Table continues…

Count	The number of times a matching call has been logged. A matching call is one with the same name, number and type. Only one record is kept for matching calls, with the count increased by 1 and using the time and date of the most recent matching call.

If missed hunt group calls are also being logged, the system stores up to 10 call records for each hunt group. When this limit is reached, new call records replace the oldest record.

Controlling Centralized Call Logging

The following controls exist for which users have their calls included in the centralized call log and which calls are included.

User Setting

The user centralized call log settings can be set through the user configuration (User | Telephony | Call Log) or through their associated user rights (User Rights | Telephony | Call Log).

Centralized Call Log: Default = System Default (On) This setting allows the use of centralized call logging to be enabled or disabled on a per user basis. The default is to match the system setting Default Centralized Call Log On (System | Telephony | Call Log). The other options are **On** or **Off** for the individual user. If off is selected, the call log shown on the users phone is the local call log stored by the phone.

System Settings (System | Telephony | Call Log)

Default Centralized Call Log On: Default = On. When selected, each user is defaulted to have the system store a call log of their calls. This call log is accessible on the phone when the user is using a phone with a **Call Log** or **History** button. The use of centralized call logging can be enabled/disabled on a per user basis using the Centralized Call Log user setting (User | Telephony | Call Log).

Log Missed Calls Answered at Coverage: Default = Off. This setting controls how calls to a user, that are answered by a covering user should be logged in the centralized call log. This option applies for calls answered elsewhere (covered) by pickup, call coverage (call coverage buttons or coverage group), bridged appearance button, user BLF, voicemail, etc.

Setting	Targeted User	Covering User
Off (Default)	Nothing	Answered Call
On	Missed Call	Answered Call

Log Missed Hunt Group Calls: Default = Off. By default, hunt group calls are not included in any user's centralized call log unless answered by the user. If this option is selected, a separate call log is kept for each hunt group of calls that are not answered by anyone. It includes hunt group calls that go to voicemail.

If missed hunt group calls are also being logged, the system stores up to 10 call records for each hunt group. When this limit is reached, new call records replace the oldest record.

Within the user call log setting (User | Telephony | Call Log), the list of hunt groups allows selection of which hunt groups' missed call records should be displayed as part of the user's centralized call log.

Call Scenarios

This is not a comprehensive list. However it summarizes how the user call log is used in some common call scenarios.

Scenarios	User Call Log Notes
Authorization/Account Codes	Account and authorization codes used as part of a call are not included in user call logs.
Automatic Callback	If answered, they will show as an outgoing call to the target.
Application Calls	Calls made and answered using applications (including CTI interfaces) are logged as if the user made or answered the call using an extension.
Conference Calls	Conference calls are not included in the user call log.
Hold	When a user holds and then un-holds a call, the call duration includes the time the call was on hold.
Follow-Me	Calls to the user still appear in their user call log. The follow me calls do not appear in the user call log of the user who was the follow me destination.
Forward on Busy **Forward on No Answer**	If the forwarded call is answered, the forwarding user will have a **Missed - Answered by Other** call log record. If the forwarded call times out to voicemail, the user will have a **Missed - Answered by Voicemail** call log record.
Forward Unconditional	When forwarding to another number, there will be no record of forwarded calls in the forwarding users call log. When using the To Voicemail option, the forwarded call will by logged as a Missed - Answered by Voicemail call record.
Page Calls	Page calls are not included in any user call logs unless the page is answered (by pressing Conference). When answered the page is logged as a normal call between the two users involved.
Park	Retrieving a call from Park (even if the user is the one who parked the call) is logged as a incoming call.
Short Codes	Calls are only logged if they result in a call being made or a call being answered. Calls made using Break Out are not included.

Table continues…

Scenarios	User Call Log Notes
Suppressed Digits	Calls made with digit suppression enabled (AD Suppress button) are not included in the users call log.
Transfers	If the user answers and accepts a supervised transfer, they will have a incoming calls records. One for the transfer enquiry call and one for the transferred call. If the user is the target of an unsupervised transfer, they will have an Incoming or Missed call log. Note that even if the call being transferred was originally an outgoing call, for the user answering the transfer it is logged as a incoming call.
Twinning and Mobility	When a user has a twinned device (either internal twinning or mobile twinning), the user's call log operates regardless of which device the user uses to make or answer calls. Calls between the twinned devices, ie. the user transferring a call between devices, are not included in their call log. This includes calls made using mobile call control or a one-X Mobile client.

Multi-Site Network

The user's call log records are stored by the system that is their home system, ie. the one on which they are configured. When the user is logged in on another system, new call log records are sent to the user's home system, but using the time and date on the system where the user is logged in.

Hunt group call log records are stored on the system on which the hunt group is configured.

Coverage Groups

For users with a **Coverage Group** selected, coverage group operation is applied to all external calls that are targeted to the user.

For external calls:

In scenarios where an external call would normally have gone to voicemail, it instead continues ringing and also starts alerting the members of the coverage group.

- The follow me settings of Coverage Group members are used, the forwarding settings are not.
- If the user is not available, for example if they have logged off or set to do not disturb, coverage group operation is applied immediately.

- If the user is configured for call forward on busy, coverage operation is applied to the user's calls forwarded to the forward on busy destination.

Coverage group operation is not applied to the following types of call:

Hunt group calls.

Recall calls such as transfer return, hold recall, park recall, automatic callback.

The Coverage Group is set through the user's User | Telephony | Supervisor Settings or through their associated User Rights | Telephony | Supervisor Settings. The only group settings used are:

- The list of group members. They are treated as a collective group regardless of the group's configuration.
- If the group has **Night Server Fallback Group** and or **Out of Service Fallback Group** set, the members of those groups are used if the coverage group is set to night service mode or out of service mode respectively.

Hunt Group Operation

Related Links

Hunt Group Types on page 641
Call Presentation on page 642
Hunt Group Member Availability on page 643
Example Hunt Group on page 645
CBC/CCC Agents and Hunt Groups on page 647

Hunt Group Types

At its most basic, a hunt groups settings consist of a hunt group name, an extension number, a list of hunt group members and a hunt type selection. It is the last two settings which determine the order in which incoming calls are presented to hunt group members.

The available hunt types are; Collective, Sequential, Rotary and Longest Waiting. These work are follows:

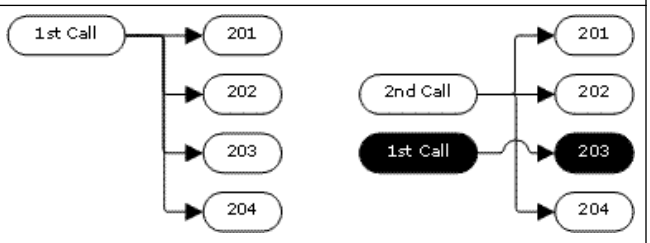
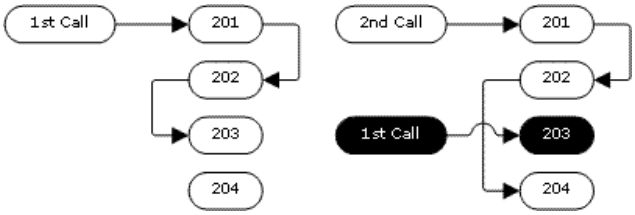
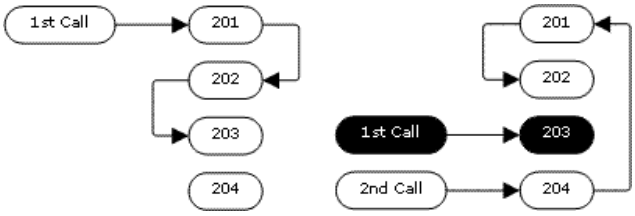
Collective Group (formerly Group Group)	
An incoming call is presented simultaneously to all the available hunt group members.	

Table continues…

Sequential Group (formerly Hunt or Linear Group)	
An incoming call is presented to the first available member in the list. If unanswered, it is presented to the next available member in the list. The next incoming call uses the same order. It is presented to the available members starting again from the top of the list.	
Rotary Hunt Type (formerly Circular Group)	
This hunt type operates similarly to Sequential. However the starting point for call presentation is the first available member after the last member to answer a call.	
Longest Waiting Hunt Type (formerly Idle or Most Idle)	
This hunt type does not present calls to hunt group members in the order that they are listed. It presents calls using the order of how long the available hunt group members have been idle. An incoming call is first presented to the available member who has been idle the longest. If unanswered it is presented to the next longest idle member. Release 4.2+: Where hunt group calls are being presented to a twinned extension, the longest waiting status of the user can be reset by calls answered at either their master or twinned extension.	

Related Links

Hunt Group Operation on page 641

Call Presentation

Summary: Calls are presented to each available hunt group member in turn. If having been presented to all the available members, none answers, the call is redirected to voicemail if available, otherwise it continues to be presented to the next available member.

In addition to the summary, options exist to have calls queued or to have calls also presented to agents in an overflow group or groups.

First and Next Available Members The first available member to which a call is presented and the order of the next available members to which a call is presented are determined by the hunt group's Hunt Type setting.

Additional Calls When additional calls are waiting to be presented, additional available hunt group members are alerted using the hunt group type. The way additional calls are presented if there are available members depends on the system software level.

Pre-Release 4.0 Additional calls ring around the group separately. This means that additional calls may be answered ahead of the first call.

Release 4.0 and Higher When any member answers a call it will be the first waiting call that is answered.

No Available Members If the number of incoming calls exceeds the number of available members to which calls can be presented, the following actions are usable in order of precedence.

Queuing If queuing has been enabled for the hunt, it is applied to the excess calls up to the limits specified for the number of queued calls or length of time queued.

Voicemail If voicemail has been enabled for the hunt group, excess calls are directed to voicemail.

Busy Tone Busy tone is returned to the excess calls (except analog and T1 CAS calls which remain queued).

No Answer Time This value is used to determine how long a call should ring at a hunt group member before being presented to the next available hunt group member. The **System | Telephony | Telephony | No Answer Time** setting is used unless a specific **Hunt | Hunt Group | No Answer Time** is set.

Voicemail If voicemail is being used, if having been presented to all the available group members the call is still not answered then it goes to voicemail.

The call will also go to voicemail when the hunt group's **Voicemail Answer Time** is exceeded. the mailbox of the originally targeted hunt group is used even if the call has overflowed or gone to a night server hunt group.

Calls Not Being Answered Quick Enough - Overflow In addition to ringing at each available member for the No Answer Time, a separate **Overflow Time** can be set. When a calls total ring time against the group exceeds this, the call can be redirected to an overflow group or groups.

No Available Member Answers If a call has been presented unanswered to all the available members, either of two actions can be applied. If voicemail is available, the call is redirected to voicemail. If otherwise, the call will continue being presented to hunt group members until answered or, if set, overflow is used.

Call Waiting For hunt groups using the Group hunt type, call waiting can be used.

Related Links

Hunt Group Operation on page 641

Hunt Group Member Availability

Summary: Details when a hunt group member is seen as being available to be presented a hunt group call.

The Hunt Group settings within Manager list those users who are members of the hunt group and therefore may receive calls directed to that hunt group. However there are a range of factors that can affect whether a particular hunt group member is available to take hunt group calls at any time.

Existing Connected Call Users with an existing connected call are not available to further hunt group calls. This is regardless of the type of connected call, whether the user has available call appearance buttons or is using call waiting.

Hunt Group Call Waiting For Collective hunt groups call waiting can be enabled using the **Ring Type** of **Collective Call Waiting**.

Logged In/Logged Out The system allows user's to log in and out extensions, a process known as 'hot desking'. Whilst a user is logged out they are not available to receive hunt group calls.

Release 4.2+: Mobile Twinning users with both **Hunt group calls eligible for mobile twinning** and **Twin when logged out** selected will still receive hunt group calls unless they switch off twinning.

Membership Enabled/Disabled The system provides controls to temporarily disable a users' membership of a hunt group. Whilst disabled, the user is not available to receive calls directed to that hunt group.

Do Not Disturb This function is used by users to indicate that they do not want to receive any calls. This includes hunt group calls. In call center environments this state is also known as 'Busy Not Available'. See Do Not Disturb.

Busy on Held When a user has a held call, they can receive other calls including hunt group calls. The Busy on Held settings can be used to indicate that the user is not available to further calls when they have a held call.

Forward Unconditional Users set to Forward Unconditional are by default not available to hunt group calls. The system allows the forwarding of hunt group calls to be selected as an option.

Idle /Off Hook The hunt group member must be idle in order to receive hunt group call ringing.

No Available Members If queuing has been enabled, calls will be queued. If queuing has not been enabled, calls will go to the overflow group if set, even if the overflow time is not set or is set to 0. If queuing is not enabled and no overflow is set, calls will go to voicemail. If voicemail is not available, external calls go to the incoming call routes fallback destination while internal calls receive busy indication.

Hunt Group Member Availability Settings	
Manager	Forwarding and do not disturb controls for a user are found on the User | Forwarding and User | DND tabs. Enabling and disabling a users hunt group membership is done by ticking or unticking the user entry in the hunt group's extensions list on the Hunt Group | Hunt Group tab.
Controls	The following short code features/button programming actions can be used:
SoftConsole	A SoftConsole user can view and edit a user's settings. Through the directory, select the required user. Their current status including DND, Logged In and hunt group membership states are shown and can be changed. Forwarding settings can be accessed by then selecting Forwarding.

Feature/Action	Short Code	Default	Button

Table continues…

Hunt Group Enable	✓	✗	✓HGEna - Toggles.
Hunt Group Disable	✓	✗	✓HGDis
Forward Hunt Group On	✓	✓-*50	✓FwDH+ - Toggles
Forward Hunt Group Off	✓	✓-*51	✓FwDH-
Busy on Held	✓	✗	✓BusyH
Do Not Disturb On	✓	✓-*08	✓DNDOn - Toggles
Do Not Disturb Off	✓	✓-*09	✓DNDOf
Extn Login	✓	✓-*35*N#	✓Login
Extn Logout	✓	✓-*36	✓Logof

Related Links

Hunt Group Operation on page 641

Example Hunt Group

The follow are simple examples of how a department might use the facilities of a hunt group.

1. Basic Hunt Group

Scenario	The Sales department want all sales related calls to be presented first to Jane, then Peter and finally Anne.
Actions	1. Create a hunt group named Sales and assign it an extension number. 2. Set the **Hunt Type** to **Sequential**. 3. Add Jane, Peter and Ann to the **User L** ist in that order. 4. Turn off queuing on the Queuing tab and voicemail on the Voicemail tab. 5. Route relevant calls to the Sales group by selecting it as the destination in the appropriate Incoming Call Routes.
Results	Any call received by the Sales hunt group is first presented to Jane if she is available. If Jane is not available or does not answer within 15 seconds the call is presented to Peter. If Peter is not available or does not answer within 15 seconds the call goes Anne. Since voicemail is not on, the call will continue to be presented around the group members in that order until it is answered or the callers hangs up.

2. Adding Voicemail Support

Scenario	A voicemail server has now been added to the system. The Sales department wants to use it to take messages from unanswered callers. When messages are left, they want Jane to receive message waiting indication.
Actions	1. Open the Sales hunt group settings and select **Voicemail On** on the Voicemail tab. 2. Select the User settings for Jane. On the **Source Numbers** tab, add the entry **HSales**.
Results	Once a call to the Sales group has been presented to all the available members, if it is still unanswered then the call will be redirected to the group's voicemail mailbox to leave a message. When a message has been left, the message waiting indication lamp on Jane's phone is lit.

3. Using the Queuing Facility

Scenario	The Sales department now wants calls queued when no one is available to answer. However if the number of queued calls exceeds 3 they then want any further callers directed to voicemail.
Actions	1. Open the Sales hunt group settings and select **Queuing On** on the **Queuing** tab. 2. Set the **Queue Limit** to **3**.
Results	When the Sales group are all on calls or ringing, any further calls to the group are queued and receive queuing announcements from the voicemail server. When the number of queued calls exceeds 3, any further calls are routed to the group's voicemail mailbox.

4. Using Out of Service Fallback

Scenario	During team meetings, the Sales department want their calls redirected to another group, for this example Support.
Actions	1. Open the Sales hunt group settings and select the **Fallback** tab. In the **Out of Service Fallback Group** field select the **Support** group. 2. Create a system short code ***88/Set Hunt Group Out of Service/300**. 3. Create a system short code ***89/Clear Hunt Group Out of Service/300**.
Results	Prior to team meetings, dialing *88 puts the Sales group into out of service mode. Its calls are then

Table continues…

	redirected to the Support group. Following the meeting, dialing *89 puts the Sales group back In Service.

5. Using a Night Service Time Profile

Scenario	Outside their normal business hours, the Sales department want their group calls automatically sent to voicemail. This can be done using a time profile and leaving the Night Service Fallback Group setting blank.
Actions	1. Create a Time Profile called **Sales Hours** and in it enter the times during which the Sales department are normally available. 2. Open the Sales hunt group settings and select the **Fallback** tab. 3. In the **Time Profile** field select **Sales Hours**.
Results	Outside the normal business hours set in the time profile, the Sales hunt group is automatically put into Night Service mode. Since no Night Service Fallback Group has been set, calls are redirected to voicemail.

Related Links

Hunt Group Operation on page 641

CBC/CCC Agents and Hunt Groups

The use of and reporting on hunt groups is a key feature of call center operation. For IP Office, reporting is provided through the Compact Business Center (CBC) or Compact Contact Center (CCC) applications.

In order for these applications to provide hunt group and hunt group user (agent) reports, the following rules apply:

- The hunt group names must be restricted to a maximum of 12 characters.
- The hunt group and user extension numbers should be a maximum of 4 digits.
- Hunt group members should be given a Login Code and set to Force Login.
- The agent state Busy Not Available is equivalent to Do Not Disturb. The agent state Busy Wrap Up is equivalent to hunt group disable.

Related Links

Hunt Group Operation on page 641

Malicious Call Tracing (MCID)

MCID (Malicious Caller ID) is an ISDN feature. It is supported on BRI and PRI trunks to ISDN service provider who provide MCID.

When used, it instructs the ISDN exchange to perform a call trace on the user's current call and to keep a record of the call trace at the exchange for the legal authorities. Trace information is not provided to or displayed by the system or system phones.

The use of MCID is subject to local and national legal requirements that will vary. The feature may also not be enabled until specifically requested from the service provider. You should consult with your ISDN service provider and with appropriate legal authorities before attempting to use MCID. Successful use of this feature is indicated by a tone on the phone and a "User Registered" message on T3 phones.

Activating MCID

1. **Liaise with the ISDN Service Provider** MCID should not be used with first confirming its usage with the ISDN service provider.
2. **Enabling MCID Call Tracing on a Line** BRI and PRI lines include a Support Call Tracing Option. which by default is off.
3. **Enabling MCID Call Tracing for a User** First the user must be allowed to use call tracing. Each user has a Can Trace Calls (User | Telephony | Supervisor Settings) option. This option is off by default.
4. **Providing an Active MCID Control** The user needs to be provided with a mechanism to trigger the MCID call trace at the exchange. This can be done using either a short code or a programmable button.

- **MCID Activate Button** The action MCID Activate (Advanced | Miscellaneous | MCID Activate) can be assigned to a programmable buttons. It allows a malicious call trace to be triggered during a call.
- **MCID Activate Short Codes** The feature MCID Activate can be used to create a short code to triggering a malicious call trace.

Call Restriction

Call barring can be applied in a range of ways.

Barring a User From Receiving Any External Calls For each user, Incoming Call Bar (User | Telephony | Supervisor Settings) can be selected to stop that user from receiving any external calls.

Barring a User From Making Any External Calls For each user, Outgoing Call Bar (User | Telephony | Supervisor Settings) can be selected to stop that user from making any external calls.

Barring Particular Numbers/Number Types System short codes are used to match user dialing and then perform a specified action. Typically the action would be to dial the number to an external line. However, short codes that match the dialing of particular numbers or types of numbers can be

added and set to another function such as Busy. Those short codes can be added to a particular user, to a User Rights associated with several users or to the system short codes used by all users.

The system allows short codes to be set at user, user rights, system and least cost route. These have a hierarchy of operation which can be used to achieve various results. For example a system short code for a particular number can be set to busy to bar dialing of that number. For a specific user, a user short code match to the same number but set to Dial will allow that user to override the system short code barring.

Using Account Codes The system configuration can include a list of account codes. These can be used to restrict external dialing only to users who have entered a valid account code.

- **Forcing Account Code Entry for a User** A user can be required to enter an account code before the system will return dialing tone. The account code that they enter must match a valid account code stored in the system configuration. The setting for this is Force Account Code (User | Telephony | Supervisor Settings).
- **Forcing Account Code Entry for Particular Numbers** Each system short code has a Force Account Code option. Again the account code entered must match a valid account code stored in the system configuration. for the call to continue.

Barring External Transfers and Forwards A user cannot forward or transfer calls to a number which they cannot normally dial. In addition there are controls which restrict the forwarding or transferring of external calls back off-switch. See Off-Switch Transfer Restrictions.

Call Intrusion

The system supports several different methods for call intrusion. The method used affects which parties can hear and be heard by other parties following the intrusion. Intrusion features are supported across a multi-site network

In the scenarios below, user A is on a call with B who may be internal or external. User C invokes one of the call intrusion methods targeting user A.

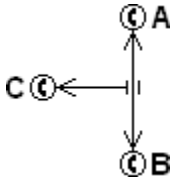
Feature	Description	Privacy Settings		
		User	Target	
		Can Intrude	Cannot Be Intruded	Private Call
Call Listen 	This feature allows you to monitor another user's call without being heard. Monitoring can be accompanied by a tone heard by all	Used	Used	Used

Table continues…

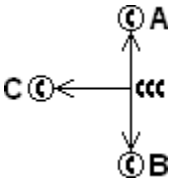
Feature	Description	Privacy Settings		
		User	Target	
		Can Intrude	Cannot Be Intruded	Private Call
	parties. Use of the tone is controlled by the Beep on Listen setting on the System | Telephony | Tones & Music tab. The default for this setting is on. If enabled, this is the only indication of monitoring given to the monitored user. There is no phone display indication of monitoring.			
Call Intrude 	This feature allows you to intrude on the existing connected call of the specified target user. All call parties are put into a conference and can talk to and hear each other. A **Call Intrude** attempt to a user who is idle becomes a Priority Call.	Used	Used	Used
Call Steal	This function can be used with or without a specified user target. If the target has alerting calls, the function will connect to the longest waiting call. If the target has no alerting calls but does have a connected call, the function will take	Used	Used	Used

Table continues…

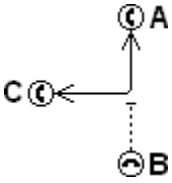
Feature	Description	Privacy Settings		
		User	Target	
		Can Intrude	Cannot Be Intruded	Private Call
	over the connected call, disconnecting the original user. This usage is subject to the **Can Intrude** setting of the **Call Steal** user and the **Cannot Be Intruded** setting of the target. If no target is specified, the function attempts to reclaim the user's last ringing or transferred call if it has not been answered or has been answered by voicemail.			
Dial Inclusion 	This feature allows you to intrude on another user's call to talk to them. Their current call is put on hold while you talk and automatically reconnected when you end the intrusion. The intruder and the target extension can then talk but cannot be heard by the other party. This can include intruding into a conference call, where the conference will continue without the intrusion target.	Used	Used	Used

Table continues…

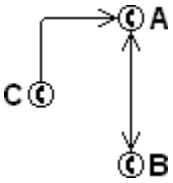
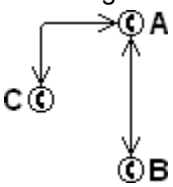
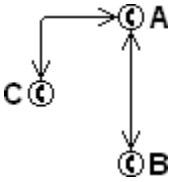
Feature	Description	Privacy Settings		
		User	Target	
		Can Intrude	Cannot Be Intruded	Private Call
	During the intrusion all parties hear a repeated intrusion tone. When the intruder hangs-up the original call parties are reconnected. Attempting to hold a dial inclusion call simply ends the intrusion. The inclusion cannot be parked.			
Whisper Page 	This feature allows you to intrude on another user and be heard by them without being able to hear the user's existing call which is not interrupted. For example: User A is on a call with user B. When user C intrudes on user A, they can be heard by user A but not by user B who can still hear user A. Whisper page can be used to talk to a user who has enabled private call.	Used	Used	Not Used
Coaching Intrusion 	This feature allows the you to intrude on another user's call and to talk to them without being heard by the other call parties to which they can still talk. For example: User A is on a call with	Used	Used	Used

Table continues…

Feature	Description	Privacy Settings		
		User	Target	
		Can Intrude	Cannot Be Intruded	Private Call
	user B. When user C intrudes on user A, they can hear users A and B but can only be heard by user A.			
Request Coaching Intrusion 	This feature allows you to request a call intrusion. While on a call, user A indicates to user C a request for coaching support. When user C intrudes on user A, they can hear users A and B but can only be heard by user A.	Used	Used	Used
Call Appearance	In addition to making and answering calls, appearance buttons that indicate 'in use elsewhere' can be pressed in order to join that call. The **Can Intrude** setting of the user is not used. The **Cannot Be Intruded** setting of the longest present internal party in the call is used.	Not Used	Used	Used
Bridged Appearance		Not Used	Used	Used
Line Appearance		Not Used	Used	Used

Warning:

The use of features to listen to a call without the other call parties being aware of that monitoring may be subject to local laws and regulations. Before enabling the feature you must ensure that you have complied with all applicable local laws and regulations. Failure to do so may result in severe penalties.

Intrusion Privacy Controls

The ability to intrude and be intruded is controlled by two configuration settings, the Can Intrude (User | Telephony | Supervisor Settings) setting of the user intruding and the Cannot Be Intruded (User | Telephony | Supervisor Settings) setting of target being intruded on. The setting of any other internal party is ignored. By default, no users can intrude and all users are set to cannot be intruded.

For intrusion using appearance buttons, the user's **Can Intrude** setting is not used. The **Cannot Be Intruded** setting of the longest present internal party in the call is used.

A user who can normally be intruded on can indicate that a call is a private call by using a Private Call short code or programmable button. While private call status is enabled, no intrusion is allowed except for **Whisper Page** intrusion.

In addition to the options above, **Call Listen** can only be used to intrude on calls by users in the user's Monitor Group (User | Telephony | Supervisor Settings).

For the **Call Steal** function, the **Can Be Intruded** setting is used if the call is connected.

Private Calls

This feature allows users to mark a call as being private.

When on, any subsequent calls cannot be intruded on until the user's private call status is switched off. The exception is Whisper Page which can be used to talk to a user on a private call.

Note that use of private calls is separate from the user's intrusion settings. If the user's **Cannot be Intruded** (User | Telephony | Supervisor Settings) setting is enabled, switching private calls off does not affect that status. To allow private calls to be used to fully control the user status, **Cannot be Intruded** (User | Telephony | Supervisor Settings) should be disabled for the user.

Use of private calls can be changed during a call. Enabling privacy during a call will stop any current recording, intrusion or monitoring. Privacy only applies to the speech part of the call. Call details are still recorded in the SMDR output and other system call status displays.

Button Programming The button programming action **Advanced | Call | Private Call** can be used to switch privacy on/off. Unlike the short code features it can be used during a call to apply or remove privacy from current calls rather than just subsequent calls. On suitable phones the button indicates the current status of the setting.

Short Codes A number of short code features are available for privacy.

- **Private Call** Short codes using this feature toggle private status on/off for the user's subsequent calls.
- **Private Call On** Short codes using this feature enable privacy for all the user's subsequent calls until privacy is turn off.
- **Private Call Off** Short codes using this feature switch off the user's privacy if on.

Call Waiting

Call waiting allows a user who is already on a call to be made aware of a second call waiting to be answered.

User Call Waiting

Call waiting is primarily a feature for analog extension users. The user hears a call waiting tone and depending on the phone type, information about the new caller may be displayed. The call waiting tone varies according to locale.

For Avaya feature phones with multiple call appearance buttons, call waiting settings are ignored as additional calls are indicated on a call appearance button if available.

To answer a call waiting, either end the current call or put the current call on hold, and then answer the new call. Hold can then be used to move between the calls.

Call waiting for a user can be enabled through the system configuration (User | Telephony | Call Settings | Call Waiting On) and through programmable phone buttons.

Call waiting can also be controlled using short codes. The following default short codes are available when using Call Waiting.

***15 - Call Waiting On** Enables call waiting for the user.

***16 - Call Waiting Off** Disables call waiting for the user.

***26 - Clear Call and Answer Call Waiting** Clear the current call and pick up the waiting call.

Hunt Group Call Waiting

Call waiting can also be provided for hunt group calls. The hunt group **Ring Mode** must be **Collective Call Waiting**.

On phones with call appearance buttons, the call waiting indication takes the form of an alert on the next available call appearance button. On other phones, call waiting indication is given by a tone in the speech path (the tone is locale specific).

The user's own **Call Waiting** setting is overridden when they are using a phone with call appearances. Otherwise the user's own **Call Waiting** setting is used in conjunction with the hunt group setting.

Message Waiting Indication

Message waiting indication (MWI) or a message lamp is supported for a wide variety of phones. It is used to provide the user with indication of when their voicemail mailbox contains new messages. It can also be configured to provide them with indication when selected hunt group mailboxes contain new messages.

Avaya digital and IP phones all have in-built message waiting lamps. Also for all phone users, the one-X Portal for IP Office application provides message waiting indication.

Related Links

Message Waiting Indication for Analog Phones on page 656
Message Waiting Indication for Analog Trunks on page 657

Message Waiting Indication for Analog Phones

For analog phones, the system supports a variety of analog message waiting indication (MWI) methods. The method used for an individual analog extension is set for the **Extn | Analog | Message Waiting Lamp Indication Type** field. Those methods are

- **101V**
- **51V Stepped**
- **81V**
- **Bellcore FSK**
- **Line Reversal A**
- **Line Reversal B**
- **None**
- **On**

The 101V method is only supported when using a Phone V2 expansion module.

81V is typically used in European countries. 51V Stepped is used in most other countries. However the actual method used for a particular model of analog phone should be confirmed with the phone manufacturer's documentation.

The **Message Waiting Lamp Indication Type** field also provides options for **None** (no MWI operation) and **On**. **On** selects a default message waiting indication method based on the system locale.

'On' Method	Locale
81V	Belgium, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Netherlands, Norway, Poland, Portugal, Russia, Saudi Arabia, Sweden, Switzerland, United Kingdom.
51V Stepped	Argentina, Australia, Brazil, Canada, Chile, China, Colombia, Japan, Korea, Mexico, New Zealand, Peru, South Africa, Spain, United States.

For the United Kingdom system locale (eng), the default Caller Display Type (UK) allows updates of an analog phone's ICLID display whilst the phone is idle. The system uses this facilities to display the number of new messages and total number of messages in the users own mailbox. This feature is not supported with other Caller Display Types.

Hunt Group Message Waiting Indication

By default no message waiting indication is provided for hunt group voicemail mailboxes. Message waiting indication can be configured by adding an **H** entry followed by the hunt groups name to the Source Numbers tab of the user requiring message waiting indication for that hunt group. For

example, for the hunt group Sales, add **HSales**. Hunt group message waiting indication does not require the user to be a member of the hunt group.

Related Links

Message Waiting Indication on page 655

Message Waiting Indication for Analog Trunks

IP Office can provide a MWI for analog trunks from the PSTN network that terminate on an ATM4U-V2 card. Multiple users can be configured to receive a MWI from a single analog line. Users can receive an MWI from multiple lines. Configuring a user for MWI includes configuraton of a button for automatically dialing the message center.

Note the following conditions.

- Only supported for analog trunks terminating on the ATM4U-V2 card.
- When Analog Trunk MWI is selected as the Voicemail Type, no other voicemail system is active. As a result, hunt group queue announcements are not supported, since they require Embedded Voice Mail or Voicemail Pro.
- All analog trunks configured for MWI must use the same message center number. Multiple message centers are not supported.
- Not supported in One-X Portal.
- No TAPI is provided for analog trunk MWI status.
- Not supported across multiple IP Office systems. If the analog line is on a different node than the user's phone, that phone cannot receive an MWI for the line.
- Mobile twinning is not supported. Analog trunk MWI is displayed only on the master set.
- Internal twinning is not supported automatically. However, the twinned set can be configured to receive the same analog trunk MWI as the master set.

Configuring MWI for an Analog Trunk

1. Go to **System | Voicemail**. In the **Voicemail** field, select **Analog Trunk MWI**.
2. In the **Destination** field, enter the message center telephone number.
3. Select the **Line** you want to configure for Analog MWI, and then select the **Analog Options** tab.
4. In the **MWI Standard field**, select **Bellcore FSK**.
5. Select the **User** you want to configure for MWI and then select the **Button Programming** tab.
6. Select the button you want to configure and then click **Edit**.
7. In the **Action** field click the browse (...) button and select **Advanced > Voicemail > Monitor Analog Trunk MWI**.
8. In the **Action Data** field, enter the line appearance ID of the analog line.

Related Links

Message Waiting Indication on page 655

System Phone Features

The user option **System Phone Rights** (User | User) can be used to designate a user as being a system phone user. System phone users can access a number of additional function not available to other phone users. Note that if the user has a login code set, they will be prompted to enter that code in order to access these features..

- **None** The user cannot access any system phone options.
- **Level 1** The user can access all system phone options supported on the type of phone they are using except system management and memory card commands.
- **Level 2** The user can access all system phone options supported on the type of phone they are using including system management and memory card commands. Due to the nature of the additional commands a login code should be set for the user to restrict access.

..

The following functions are supported:

- **MENU to set date/time** Restricted to 4412, 4424, 4612, 4624, 6408, 6416 and 6424 phones where supported by the system. Note 4612 and 4624 not support for 4.1+. On these phones, a system phone user can manually set the system date and time by pressing **Menu | Menu | Func | Setup**.
- **SoftConsole Send Message** If the system phone user is using SoftConsole, they can access the SoftConsole function **Send Message** to send a short text message (up to 16 characters) to a display phone. Refer to the SoftConsole documentation for details. Note that this is no longer required for 4.0+.

Change Login Code of Other Users Using a short code with the Change Login Code feature, system phone users can change the login code of other users on the system.

Outgoing Call Bar Off Using a short code with the Outgoing Call Bar Off feature, system phone users can switch off the outgoing call bar status of other users on the system. .

Edit System Directory Records ..Using a 1400, 1600, 9500 or 9600 Series phone, a system phone user can edit system directory records stored in the configuration of the system on which they are hosted. .They cannot edit LDAP and/or HTTP imported records.

The following commands are only supported using 1400, 1600, 9500 and 9600 Series phones. Due to the nature of the commands a login code should be set for the user to restrict access. The commands are accessed through the **Features | Phone User | System Administration** menu. For full details refer to the appropriate phone user guide or the IP Office Installation manual.

System Management (IP500 V2 only) Allows the user to invoke a system shutdown command.

Memory Card Management Allows the user to shutdown, startup memory cards and to perform actions to move files on and between memory cards.

System Alarms (IP500 V2 only) For certain events the system can display an **S** on the user's phone to indicate that there is a system alarm. The user can then view the full alarm text in the phone's Status menu. The possible alarms in order of priority from the highest first are:

1. Memory Card Failure.

2. Expansion Failure.
3. Voicemail Failure.
4. Voicemail Full.
5. Voicemail Almost Full.
6. License Key Failure.
7. System Boot Error.
8. Corrupt Date/Time.

The following functions are not supported on analog, T3, T3 IP and wireless phones.

Date/Time Programmable Button: Allows system phone users to manually set the system date and time through a programmable button (see Self Administer and Date and Time).

The 'No User' User

It is possible to have an extension which has no default associated user. This can occur for a number of reasons:

- The extension has no **Base Extension** setting associating it with a user who has the same setting as their **Extension** to indicate that they are the extension's default associated user.
- The extension's default associated user has logged in at another extension. Typically they will be automatically logged back in at their normal extension when they log out the other phone.
- The extension's default associated user cannot be automatically logged in as they are set to **Forced Login**.

Phones with no current user logged in are associated with the setting of the **NoUser** user in the system configuration. This user cannot be deleted and their Name and Extension setting cannot be edited. However their other settings can be edited to configure what functions are available at extensions with no currently associated user.

By default the **NoUser** user has **Outgoing Call Bar** enabled so that the extension cannot be used for external calls. The users first programmable button is set to the **Login** action.

Avaya 1100 Series, 1200 Series, M-Series and T-Series phones, when logged out as **No User**, the phones are restricted to logging in and dial emergency calls only.

NoUser Source Numbers

The **SourceNumbers** tab of the **NoUser** user is used to configure a number of special options. These are then applied to all users on the system. For details refer to the **User | Source Numbers** section.

Related Links

Suppressing the NoCallerId alarm on page 660

Suppressing the NoCallerId alarm

Use this procedure to suppress the NoCallerId alarm for all users on the system. Once the task is completed, the NoCallerID alarm is not raised in SysMonitor, SNMP traps, email notifications, SysLog or System Status.

Procedure

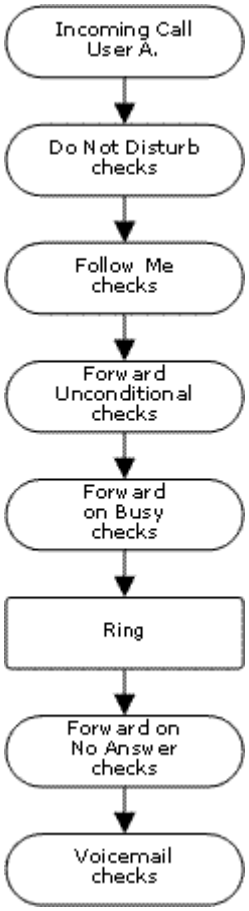
1. In Manager, in the navigation pane on the left, select **User**.
2. In the list of users, select **NoUser**.
3. In the details pane, select the **Source Numbers** tab.
4. Click **Add**.
5. In the **Source Number** field, enter **SUPPRESS_ALARM=1**.
6. Click **OK**.

Related Links

The 'No User' User on page 659

DND, Follow Me and Forwarding

This section contains topics looking at how users can have their calls automatically redirected. As illustrated, there is an order of priority in which the redirect methods are used.



Redirect priority

1. **Do Not Disturb (DND)** Redirect all calls to voicemail if available, otherwise return busy tone. DND overrides all the redirect method below unless the calling number is in the user's DND Exception Numbers List.
2. **Follow Me** Redirect all calls to another extension that the users is temporarily sharing. Follow Me overrides Forward Unconditional. The Follow Me destination is busy or does not answer, the user's Forward on Busy or Forward on No Answer options can be used if set.
3. **Forward Unconditional** Redirect the user's external calls to another number. That number can be any number the user can normally dial including external numbers. Forwarding of hunt group and internal calls is optional. Forward Unconditional overrides Forward on Busy and Forward on No Answer.

   If the destination is an internal user on the same system, they are able to transfer calls back to the user, overriding the Forward Unconditional.
4. **Forward on Busy** Redirects the user's external calls when the system sees the user as being busy. Uses the same number as Forward Unconditional unless a separate Forward on Busy Number is set. Forwarding internal calls is optional. Forward on Busy overrides Forward on No Answer.
5. **Forward on No Answer** Redirects the user's external calls when they ring for longer than the user's No Answer Time. Uses the same number as Forward Unconditional unless a separate Forward on Busy Number is set. Forwarding internal calls is optional.

Retrieving Externally Forwarded Calls:

Where a call is forwarded to an external destination and receives busy or is not answered within the forwarding user's **No Answer Time**, the system will attempt to retrieve the call. If forwarded on a trunk that does not indicate its state the call is assumed to have been answered, for example analog loop start trunks.

Off-Switch Forwarding Restrictions:

User forwarding is subject to the same restrictions as transferring calls. To bar a user from forwarding calls to an external number, the **Inhibit Off-Switch Forward/Transfers (User | Telephony | Supervisor Settings)** option. To bar all users from forwarding calls to external numbers the Inhibit **Off-Switch Forward/Transfers** option can be used.

When transferring a call to another extension that has forwarding enabled, the type of call being transferred is used. For example, if transferring an external call, if the transfer target has forwarding of external calls enabled then the forward is used.

Block Forwarding:

The Block Forwarding setting is used for enforcing predictable call routing, where the call should always go to the same destination. This setting was implemented for contact center applications.

Block Forwarding can be set for a user on the **User | Forwarding** page or as a user rights setting on the **User Rights | Forwarding** page.

Related Links

Do Not Disturb (DND) on page 662
Follow Me on page 664
Forward Unconditional on page 666
Forward on Busy on page 668
Forward on No Answer on page 670
Determining a User's Busy Status on page 672
Chaining on page 673

Do Not Disturb (DND)

Summary: Redirect all calls to busy tone or to voicemail if available except those in your DND exceptions list.

Do Not Disturb (DND) is intended for use when the user is present but for some reason does not want to be interrupted. Instead calls are sent to voicemail if available, otherwise they receive busy tone.

Exceptions Specific numbers can be added to the user's Do Not Disturb Exception List. Calls from those numbers override DND. N and X wildcards can be used at the end of exception numbers to match a range of numbers. For external numbers, this uses the incoming caller line ID (ICLID) received with the call.

Priority Enabling DND overrides any Follow Me or forwarding set for the user, except for calls in the user's Do Not Disturb Exception List.

Phone When enabled, the phone can still be used to make calls. An **N** is displayed on many Avaya phones. When a user has do not disturb in use, their normal extension will give alternate dialtone when off hook.

Applied to

Call Types Blocked		Call Treatment
Internal	✓	Voicemail if available, otherwise busy tone.
External	✓	Voicemail if available, otherwise busy tone.
Hunt Group	✓	Call not presented (DND exceptions are not used).
Page	✓	Call not presented.
Follow Me	✗	Rings.
Forwarded	✓	Busy.
VM Ringback	✗	Rings
Automatic Callback	✗	Rings
Transfer Return	✗	Rings.
Hold Return	✗	Rings.
Park Return	✗	Rings.
Twinning	✓	Voicemail if available, otherwise busy tone.

Do Not Disturb and Twinning

Mobile Twinning Selecting DND disables mobile twinning.

Internal Twinning

- Logging out or setting do not disturb at the primary stops twinned calls alerting at the secondary also.
- Logging out or setting do not disturb at the secondary only affects the secondary.

Do Not Disturb Exceptions List For both types of twinning, when DND is selected, calls from numbers entered in the user's Do Not Disturb Exception List are presented to both the primary and secondary phones.

Do Not Disturb Controls

Do Not Disturb	
Manager	A user's DND settings can be viewed and changed through the User | DND tab within the system configuration settings.
Controls	The following short code features/button programming actions can be used:

Table continues…

Voicemail	If voicemail is available, it is used instead of busy tone for callers not in the users exceptions list. For Voicemail Pro, the Play Configuration Menu action can be used to let callers switch DND on or off.
SoftConsole	A SoftConsole user can view and edit a user's DND settings except exception numbers. Through the directory, select the required user. Their current status including DND is shown. Double-click on the details to adjust DND on or off.

Feature/Action	Short Code	Default	Button
Do Not Disturb On	✓	*08	✓ - Toggles.
Do Not Disturb Off	✓	*09	✓
Do Not Disturb Exception Add	✓	*10*N#	✓
Do Not Disturb Exception Delete	✓	*11*N#	✓
Cancel All Forwarding	✓	*00	✓

Related Links

DND, Follow Me and Forwarding on page 660

Follow Me

Summary: Have your calls redirected to another user's extension, but use your coverage, forwarding and voicemail settings if the call receives busy tone or is not answered.

Follow Me is intended for use when a user is present to answer calls but for some reason is working at another extension such as temporarily sitting at a colleague's desk or in another office or meeting room. Typically you would use Follow Me if you don't have a Hot Desking log in code or if you don't want to interrupt your colleague from also receiving their own calls, ie. multiple users at one phone.

Priority Follow Me is overridden by DND except for callers in the user's DND Exception Numbers List. Follow Me overrides Forward Unconditional but can be followed by the user's Forward on Busy or Forward on No Answer based on the status of the Follow Me destination.

Destination The destination must be an internal user extension number. It cannot be a hunt group extension number or an external number.

Duration The Follow Me user's no answer timeout is used. If this expires, the call either follows their Forward on No Answer setting if applicable, or goes to voicemail is available. Otherwise the call continues to ring at the destination.

Phone When enabled, the phone can still be used to make calls. When a user has follow me in use, their normal extension will give alternate dialtone when off hook.

Exceptions

- The Follow Me destination extension can make and transfer calls to the follow me source.
- The call coverage settings of the user are applied to their Follow Me calls. The call coverage settings of the destination are not applied to Follow Me calls it receives.

Calls Forwarded

Call Types Redirected		
Internal	✓	Redirected.
External	✓	Redirected.
Hunt Group	✓	Redirected*.
Page	✓	Redirected.
Follow Me	✗	Not redirected.
Forwarded	✓	Redirected.
VM Ringback	✗	Not redirected.
Automatic Callback	✗	Not redirected.
Transfer Return	✗	Not redirected.
Hold Return	✗	Not redirected.
Park Return	✗	Not redirected.

*Except calls for "Longest Waiting" type hunt groups.

Follow Me Controls

Follow Me	
Manager	A user's Follow Me settings can be viewed and changed through the User | Forwarding tab within the system configuration settings. Note that on this tab, entering a Follow Me Number also enables Follow Me.
Controls	The following short code features/button programming actions can be used:
Voicemail	For calls initially targeted to the user but then redirected, when voicemail is invoked the mailbox of the user is used and not the mailbox of the destination. For Voicemail Pro, the Play Configuration Menu action can be used to let callers alter or set their current Follow Me destination.
SoftConsole	A SoftConsole user can view and edit a user's Follow Me settings. Through the directory, select the required user. Their current status including Follow Me is shown. Double-click on the details and select

Table continues…

	Forwarding to alter their forwarding settings including Follow Me.

Feature/Action	Short Code	Default	Button
Follow Me Here	✓	*12*N#	✓
Follow Me Here Cancel	✓	*13*N#	✓
Follow Me To	✓	*14*N#	✓
Cancel All Forwarding	✓	*00	✓

Related Links

DND, Follow Me and Forwarding on page 660

Forward Unconditional

Summary: Have your calls redirected immediately to another number including any external number that you can dial.

Priority This function is overridden by DND and or Follow Me if applied. **Forward Unconditional** overrides **Forward on Busy** and **Forward on No Answer**.

Destination The destination can be any number that the user can dial. If external and Inhibit Off-Switch Transfers is applied, the caller is directed to voicemail if available, otherwise they receive busy tone.

If the destination is an internal user on the same system, they are able to transfer calls back to the user, overriding the Forward Unconditional.

Duration The destination is rung using the forwarding user's No Answer Time. If this expires, the call goes to voicemail if available. Otherwise the call continues to ring at the destination.Calls to an external destination sent on trunks that do not signal their state are assumed to have been answered, for example analog loop start trunks.

Phone When enabled, the phone can still be used to make calls. An **D** is displayed on DS phones. When a user has forward unconditional in use, their normal extension will give alternate dialtone when off hook.

Calls Forwarded Once a call has been forwarded to an internal destination, it will ignore any further **Forward No Answer** or **Forward on Busy** settings but may follow additional **Forward Unconditional** settings.

Call Types Forwarded		
Internal	✓	Optional.
External	✓	Forwarded.
Hunt Group	✓	Optional.*
Page	✗	Not presented.

Table continues…

Follow Me	✗	Rings.
Forwarded	✓	Forwarded.
VM Ringback	✗	Rings.
Automatic Callback	✗	Rings.
Transfer Return	✗	Rings.
Hold Return	✗	Ring/hold cycle.
Park Return	✗	Rings.

*Optional only for calls targeting sequential and rotary type groups. Includes internal call to a hunt group regardless of the forward internal setting.

To Voicemail: Default = Off. If selected and forward unconditional is enabled, calls are forwarded to the user's voicemail mailbox. The **Forward Number** and **Forward Hunt Group Calls** settings are not used. This option is not available if the system's **Voicemail Type** is set to **None**. 1400, 1600, 9500 and 9600 Series phone users can select this setting through the phone menu. Note that if the user disables forward unconditional the **To Voicemail** setting is cleared.

Forward Unconditional Controls

Forward Unconditional	
Manager	A user's forwarding settings can be viewed and changed through the User | Forwarding tab within the system configuration settings.
Controls	The following short code features/button programming actions can be used:
Voicemail	For calls initially targeted to the user but then redirected, when voicemail is invoked the mailbox of the user is used and not the mailbox of the destination. For Voicemail Pro, the Play Configuration Menu action can be used to let callers set their current forwarding destination and switch Forwarding Unconditional on/off.
SoftConsole	A SoftConsole user can view and edit a user's forwarding settings. Through the directory, select the required user. Their current forwarding status is shown. Double-click on the details and select Forwarding to alter their forwarding settings.

Feature/Action	Short Code	Default	Button
Forward Number	✓	*07*N#	✓
Forward Unconditional On	✓	*01	✓ - Toggles.

Table continues…

Forward Unconditional Off	✓	*02	✓
Forward Hunt Group Calls On	✓	✗	✓ - Toggles.
Forward Hunt Group Calls Off	✓	✗	✓
Disable Internal Forwards	✓	✗	✗
Enable Internal Forwards	✓	✗	✗
Disable Internal Forwards Unconditional	✓	✗	✗
Enable Internal Forwards Unconditional	✓	✗	✗
Set No Answer Time	✓	✗	✓
Cancel All Forwarding	✓	*00	✓

Related Links

DND, Follow Me and Forwarding on page 660

Forward on Busy

Summary: Have your calls redirected when you are busy to another number including any external number that you can dial.

The method by which the system determines if a user is 'busy' to calls depends on factors such as whether they have multiple calls appearance buttons or Call Waiting and or Busy on Held set. See Busy.

Priority This function is overridden by DND and or Forward Unconditional if applied. It can be applied after a Follow Me attempt. It overrides Forward on No Answer.

Destination The destination can be any number that the user can dial. The Forward Unconditional destination number is used unless a separate number Forward on Busy Number is set. If Inhibit Off-Switch Transfers is applied, the caller is directed to voicemail if available, otherwise they receive busy tone.

Duration The destination is rung using the forwarding user's No Answer Time. If this expires, the call goes to voicemail is available. Calls to an external destination sent on trunks that do not signal their state are assumed to have been answered, for example analog loop start trunks.

Phone Forward on Busy is not indicated and normal dial tone is used.

Calls Forwarded Once a call has been forwarded to an internal destination, it will ignore any further **Forward No Answer** or **Forward on Busy** settings but may follow additional **Forward Unconditional** settings.

Call Types Forwarded		
Internal	✓	Optional.
External	✓	Forwarded.
Hunt Group	✗	Not presented.
Page	✗	Not presented.
Follow Me	✗	Rings.
Forwarded	✓	Forwarded.
VM Ringback	✗	Rings.
Automatic Callback	✗	Rings.
Transfer Return	✗	Rings.
Hold Return	✗	Ring/hold cycle.
Park Return	✗	Rings.

Forward on Busy Controls

Forward on Busy	
Software Level	A user's forwarding settings can be viewed and changed through the User | Forwarding tab within the system configuration settings.
Controls	The following short code features/button programming actions can be used:
Voicemail	For calls initially targeted to the user but then redirected, when voicemail is invoked the mailbox of the user is used and not the mailbox of the destination. For Voicemail Pro, the Play Configuration Menu action can be used to let callers set the forward destination.
SoftConsole	A SoftConsole user can view and edit a user's forwarding settings. Through the directory, select the required user. Their current forwarding status is shown. Double-click on the details and select Forwarding to alter their forwarding settings.

Feature/Action	Short Code	Default	Button
Forward Number	✓	*07*N#	✓
Forward on Busy Number	✓	*57*N#	✓
Forward on Busy On	✓	*03	✓ - Toggles.
Forward on Busy Off	✓	*04	✓

Table continues…

Disable Internal Forwards	✓	✗	✗
Enable Internal Forwards	✓	✗	✗
Disable Internal Forwards Busy or No Answer	✓	✗	✗
Enable Internal Forwards Busy or No Answer	✓	✗	✗
Set No Answer Time	✓	✗	✓
Cancel All Forwarding	✓	*00	✓

Related Links

DND, Follow Me and Forwarding on page 660

Forward on No Answer

Summary: Have your calls redirected another number if it rings without being answered.

Priority This function is overridden by DND and Forward on Busy if applied. It can be applied after a Follow Me attempt. Forward Unconditional overrides Forward on Busy and Forward on No Answer.

Destination The destination can be any number that the user can dial. The Forward Unconditional destination number is used unless a separate number Forward on Busy Number is set. If Inhibit Off-Switch Transfers is applied, the caller is directed to voicemail if available, otherwise they receive busy tone.

Duration The destination is rung using the forwarding user's No Answer Time. If this expires, the call goes to voicemail is available. Otherwise the call continues to ring at the destination. Calls to an external destination sent on trunks that do not signal their state are assumed to have been answered, for example analog loop start trunks.

Phone Forward on No Answer is not indicated and normal dial tone is used.

Calls Forwarded Once a call has been forwarded to an internal destination, it will ignore any further **Forward No Answer** or **Forward on Busy** settings but may follow additional **Forward Unconditional** settings.

Call Types Forwarded		
Internal	✓	Optional.
External	✓	Forwarded.
Hunt Group	✗	Not applicable.
Page	✗	Not applicable.
Follow Me	✗	Rings.
Forwarded	✓	Forwarded.

Table continues…

VM Ringback	✗	Rings.
Automatic Callback	✗	Rings.
Transfer Return	✗	Rings.
Hold Return	✗	Ring/hold cycle.
Park Return	✗	Rings.

Forward on No Answer Controls

Forward on No Answer	
Manager	A user's forwarding settings can be viewed and changed through the User | Forwarding tab within the system configuration settings.
Controls	The following short code features/button programming actions can be used:
Voicemail	For calls initially targeted to the user but then redirected, when voicemail is invoked the mailbox of the user is used and not the mailbox of the destination. For Voicemail Pro, the Play Configuration Menu action can be used to let callers set the forward destination. It cannot however be used to enable Forward on Busy or set a separate Forward on Busy number.
SoftConsole	A SoftConsole user can view and edit a user's forwarding settings. Through the directory, select the required user. Their current forwarding status is shown. Double-click on the details and select Forwarding to alter their forwarding settings.

Feature/Action	Short Code	Default	Button
Forward Number	✓	*07*N#	✓
Forward on Busy Number	✓	*57*N#	✓
Forward on No Answer On	✓	*05	✓ - Toggles.
Forward on No Answer Off	✓	*06	✓
Enable Internal Forwards	✓	✗	✗
Disable Internal Forwards	✓	✗	✗
Enable Internal Forwards Busy or No Answer	✓	✗	✗

Table continues…

Disable Internal Forwards Busy or No Answer	✓	✗	✗
Set No Answer Time	✓	✗	✓
Cancel All Forwarding	✓	*00	✓

Related Links

DND, Follow Me and Forwarding on page 660

Determining a User's Busy Status

Various system features allow users to handle more than one call at a time. Therefore the term "busy" has different meanings. To other users it means whether the user is indicated as being busy. To the system it means whether the user is not able to receive any further calls. The latter is used to trigger 'busy treatment', either using a user's **Forward on Busy** settings or redirecting calls to voicemail or just returning busy tone.

Busy Indication - In Use The user busy indication provided to programmable buttons and to user applications, is based on the monitored user's hook switch status. Whenever the user is off-hook, they will be indicated as being busy regardless of call waiting or call appearance settings.

Busy to Further Calls Whether a user can receive further calls is based on a number of factors as described below.

- **Logged In and Present** Is the user logged into an extension and is that extension physically connected to the system.
- **Busy on Held** If a user enables their Busy on Held setting, whenever they have a call on hold, they are no longer available to any further incoming calls.
- **Appearance Buttons** A user's call appearance button are used to receive incoming calls. Normally, whilst the user has any free call appearance buttons, they are available to receive further calls. Exceptions are:
  - **Reserve Last Appearance** Users with appearance buttons require a free call appearance button to initiate transfers or conferences. Therefore it is possible through the user's configuration settings to reserve their last call appearance button for outgoing calls only.
  - **Other Appearance Buttons** Calls may also be indicated on line, call coverage and bridged appearance buttons.

Call Waiting Users of phones without appearance buttons can use call waiting. This adds an audio tone, based on the system locale, when an additional call is waiting to be answered. Only one waiting call is supported, any further calls receive busy treatment.

Hunt Group Calls A user's availability to receive hunt group calls is subject to a range of other factors. See Member Availability.

Related Links

DND, Follow Me and Forwarding on page 660

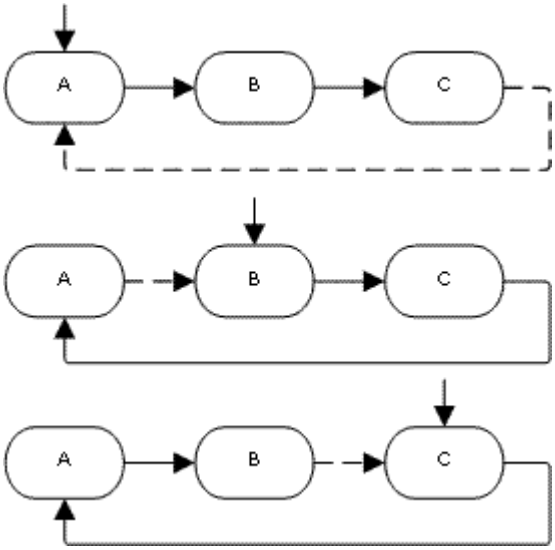
Chaining

Chaining is the process where a call forward to an internal user destination is further forwarded by that user's own forwarding settings.

Follow Me Calls Follow Me calls are not chained. They ignore the forwarding, Follow Me and Do Not Disturb settings of the Follow Me destination.

Voicemail If the call goes to voicemail, the mailbox of the initial call destination before forwarding is used.

Looping When a loop would be created by a forwarding chain, the last forward is not applied. For example the following are scenarios where A forwards to B, B forwards to C and C forwards to A. In each case the final forward is not used as the destination is already in the forwarding chain.



Hunt Group Loop If a user forwards a call to a hunt group of which they are a member, the group call is not presented to them but is presented to other members of the hunt group.

Maximum Number of Forwards A maximum of 10 forwarding hops are supported for any call.

Calls Forwarded Once a call has been forwarded to an internal destination, it will ignore any further **Forward No Answer** or **Forward on Busy** settings but may follow additional **Forward Unconditional** settings.

Related Links

DND, Follow Me and Forwarding on page 660

Transferring Calls

The following are some of the methods usable to transfer calls.

Supervised Transfer This is a transfer where the user waits for the transfer destination to answer and talks to that party before completing the transfer, this is referred to as a consultation call. They then either complete the transfer or drop the call and return to the held for transfer call. The call details, display, ringing and forwarding applied are appropriate to the type of call (internal or external) being transferred.

Unsupervised Transfer This is a transfer completed whilst the destination is still ringing.

Automatic Transfer - Forwarding The system allows users to automatically transfer calls using forwarding options such as Forward on Busy, Forward on No Answer and Forward Unconditional. For full details see DND, Follow Me and Forwarding.

Transfers to a Forwarded Extension When transferring a call to another extension that has forwarding enabled, the type of call being transferred is used. For example, if transferring an external call, if the transfer target has forwarding of external calls enabled then the forward is used.

Transfer Return Time (secs): Default = Blank (Off), Range 1 to 99999 seconds. Sets the delay after which any call transferred by the user, which remains unanswered, should return to the user. A return call will continue ringing and does not follow any forwards or go to voicemail.

Transfer return will occur if the user has an available call appearance button.

Transfer return is not applied if the transfer is to a hunt group that has queuing enabled.

Tool	Unsupervised Transfer	Supervised Transfer	Reclaim
Analog Phone/Single Line Phones	1. Press R. Note that broken dial tone is heard while a call is on hold. 2. Dial the transfer destination number. 3. Hang-up.	1. Press R. 2. Dial the transfer destination number. 3. If the destination answers and accepts the call, hang-up. 4. If the called party does not answer or does not want to accept the call, press Ragain. 5. To return to the original caller press R.	*46
Avaya DS Phone	1. Press **Transfer**. 2. Dial the transfer destination number. 3. Press **Transfer** again to complete the transfer.	1. Press **Transfer**. 2. Dial the transfer destination number. 3. If the destination answers and accepts the call, press **Transfer** again to complete the transfer. 4. If the called party does not answer or does not want to accept the call, press **Drop**.	*46

Table continues…

Tool	Unsupervised Transfer	Supervised Transfer	Reclaim
		5. To return to the original caller press it's call appearance button.	

Off-Switch Transfer Restrictions

Users cannot transfer calls to a destination that they cannot normally dial. This applies to manual transfers and also to automatic transfers (forwarding). In addition to call barring applied through short codes, the following system settings may restrict a users ability to transfer calls.

User Specific Controls

Outgoing Call Bar: Default = Off (User | Telephony | Supervisor Settings) When enabled, this setting stops a user from making any external calls. It therefore stops them making any external transfers or forwards.

Inhibit Off-Switch Forward/Transfer: Default = Off (User | Telephony | Supervisor Settings). When enabled, this setting stops the specific user from transferring or forwarding calls externally. This does not stop another user transferring the restricted users calls off-switch on their behalf.

When either system or user **Inhibit Off-Switch Forward/Transfer** is enabled, it affects the operation of the user's phone and applications. User attempts to set an external forward destination via a short code will receive error tone. User attempt to set an external forward destination via a programmable button on their phone will not have a Next option allowing the number to be saved.

Line Specific Control

Analog Trunk to Trunk Connection: Default = Off (Line | Analog Options) When not enabled, users cannot transfer or forward calls on one analog trunk back off-switch using another analog trunk.

System Wide Controls

Inhibit Off-Switch Forward/Transfer: Default = Off (System | Telephony | Telephony) When enabled, this setting stops any user from transferring or forwarding calls externally.

Restrict Network Interconnect: Default = Off (System | Telephony | Telephony). When this option is enabled, each trunk is provided with a Network Type option that can be configured as either **Public** or **Private**. The system will not allow calls on a Public trunk to be connected to a Private trunk and vice versa, returning busy indication instead.

Due to the nature of this feature, its use is not recommended on systems also using any of the following other system features: multi-site networks, VPNremote, application telecommuter mode.

Conference Control

Users can use conference controls to effectively transfer calls. This includes transferring an external call to another external number. The use of conferencing to effect off-switch transfers can be restricted using the Inhibit External Only Impromptu Conference setting (System | Telephony | Telephony).

Context Sensitive Transfer

Calls and Button Status Indication The status indication for a call on hold pending transfer has changed to differentiate such calls from standard held calls:

- On phones with both dual lamp buttons, both the green and red lamps fast flash (flutter) when the button represents a call on hold pending transfer.
- On phones with single lamp buttons or status icons, **Xfer**: is now shown in front of the caller ID information rather than the button name. For example **Xfer:Extn299** is shown rather than **a = Extn299**.
- The call status information shown when the button of a call on hold pending transfer is the currently highlight line is now prefixed with **On-Hold-Xfer** rather than **On-Hold**.

Switching Between Calls Switching from a connected call to an existing call on hold pending transfer puts the connected call on hold pending transfer. The following table is an example of the resulting operation .

Call or answer A	Connected to A
Press `Transfer`	A on hold pending transfer
Call or answer B	A on hold pending transfer. Connected to B.
Reconnect to A	Connected to A. B on hold pending transfer
Press `Transfer`or **Complete***.	A transferred to B.

Requirement for a Free Call Appearance Before Starting a Transfer When the user already has a call or calls on hold, they can now put their current call on hold pending transfer even if there are no free call appearances available. Previously an available call appearance was required in order to then make a consultation call to the potential transfer destination.

Conferencing Calls For these phone there have also been changes to which calls are conferenced in different scenarios including when there is a call on hold pending transfer. See Context Sensitive Conferencing.

Dial Tone Transfer

Release 5.0+: A user who is not able to make external calls to any or some external numbers, can be transferred to dial tone by a user who is able to make external calls.

- The restricted user wanting to make the external call, dials the unrestricted user and requests dial tone.
- The unrestricted user initiates a transfer and dials the prefix for an ARS form configured to provide secondary dial tone.

The prefix is a short code set up to access the required ARS form. While this can be a system short code, using a user or user rights short code will allow control over who can provide dial tone transfer for restricted users.

- When they hear the secondary dial tone, the unrestricted user completes the transfer.
- The restricted user now hears the secondary dial tone and is now able to make an external call.
- The restricted user is now able to make calls as permitted by the short codes in the ARS form.
- The restricted user is not able to transfer the dial tone to another user.

The ARS form being used can still contain short codes that restrict the dialing that can be attempted after the restricted user hears secondary dial tone. Other ARS features can also be used such as alternate routing or time profiles to provide out of hours routing. The ARS form timers are run from when the unrestricted caller dials the ARS form. They are not reset when the restricted user is transferred to the ARS form.

Multiple prefixes and ARS forms can be used if required to create more complex scenarios. For example, one where the unrestricted user can transfer the restricted users to an ARS forms that allows international calls or to an ARS form that only allows national dialing.

Example Configuration

The example below is a simple configuration that allows the unrestricted user to use 8 as a transfer destination that provides secondary dial tone.

Create an ARS Form for Secondary Dial Tone The ARS form needs to be created before short codes can be added to route callers to it.

- Enter a **Route Name** to identify the ARS form, for example **Dial Tone Trans**.
- Select **Secondary Dial Tone**.
- Select either **System Tone** (this matches locale specific normal dial tone) or **Network Tone** (this matches locale specific secondary dial tone). For some locales both tones are the same.
- Enter short codes that will take any digits dialed by the restricted user and process them for external dialing to an outgoing line group. For this example we will allow any digits dialed to be presented to the first trunk seized in outgoing line group 0.

Code	N
Telephone Number	N
Feature	Dial
Line Group ID	0

- Other short codes can be used to allow or bar the dialing of specific numbers or types of numbers.
- Configure the rest of the ARS form as required. For full details on ARS form configuration see ARS.

Create a Short Code for Dial Tone Transfer For this example we will allow the prefix 8 to be used to access an ARS form created above.

In the user short codes of the unrestricted user, create a short code that invokes the ARS form created above. For example:

Code	8
Telephone Number	
Feature	Dial
Line Group ID	51 Dial Tone Trans

- It is important that the short code does not pass any digits to the ARS form. Once the ARS form receives any digits, it starts short code matching and ends secondary dial tone.
- The short code could also be setup as a system or user rights short code.

The unrestricted user is now able to provide secondary dial tone to other users by on request by pressing **Transfer**, dialing **8** and then pressing **Transfer** again.

Account and Authorization Codes

If the restricted user enters an account or authorization code while calling the unrestricted user to request dial tone, that value is not carried forward with their external call once they have been provided with secondary dial tone.

If the unrestricted user enters an account or authorization code while dialing the ARS form, that value remains associated with the call made by the restricted user.

If the ARS form short code used to route the restricted users call requires an account or authorization code, the value already entered is used, otherwise the restricted user is prompted to enter a value.

Call Logging

The restricted user's outgoing call log will include the call to the unrestricted user and the outgoing external call they subsequently make. The outgoing external call record will include the prefix dialed by the unrestricted user to access the ARS form.

The unrestricted users call log will include just an incoming call from the restricted user.

Within the SMDR output, the calls by the restricted user are included. The call by the unrestricted user is not included.

Handsfree Announced Transfers

This feature allows the enquiry call part of a supervised transfer to be answered handsfree. In addition the system can be optionally configured to allow both the enquiry call and completed transfer call to be auto-answered.

Example

1. User 201 answers a call that they then want to transfer to user 203.
2. They press TRANSFERto put the call on hold pending transfer.
3. They then press a **Dial Direct** button and dial 203.

4. The transfer enquiry call is auto answered by User 203's phone. User 201 is able to announce the pending transfer and hear if User 203 wants to accept the call.

The auto-answer only occurs if the target user's extension is idle. If the target is already connected to a call, the transfer enquiry will be presented as normal call.

If the transfer is accepted, User 201 can press TRANSFERagain to complete the transfer process.

The transferred call will then ring at the target. However, if required the system can be configured to also auto-answer the completed transfer.

Configuration

Handsfree announced transfers are supported when using one of the following features after having pressed **TRANSFER**.

Button Features	Short Code Features
Dial Direct Automatic Intercom Dial Intercom	Dial Direct

User Button Usability Following the use of any of the buttons above, if the button has not been programmed with a specific target, a User button can be used to indicate the target for the enquiry call. This gives the advantage of being able to see the target user's status before attempting the transfer.

- For **Automatic Intercom** and **Dial Intercom** buttons without a pre-specified target, the **User** button must be on a button module.
- For **Dial Direct** buttons without a pre-specified target, the **User** button can be on the phone or button module. Due to this and the support for **Dial Direct** across a network of systems, we recommend that a **Dial Direct** button is used for handsfree announced transfers.

Phone Support

Handsfree announced transfer is supported for calls being transferred to the following phones:

Full Support	Partial Support	Not Supported
The following system phones support full announced transfer operation. **1603, 1608, 1616, 2410, 2420, 5410, 5420, 4610, 4621, 4625, 5610, 5620, 5621.** **All T3 phones**. **Analog Off-Hook Stations** (See notes below).	The following phone can auto-answer announced transfers but require the user to use the handset to respond. **2402, 4601, 4602, 5402, 5601, 5602**.	Announced transfer is not supported for any phones not listed in the other column. On unsupported phones the transfer eqnuiry consultation call will be presented as a normal call.

Notes

On supported phones, if the target user's phone is not idle when the enquiry call attempt is made, the enquiry call is turned into a normal transfer attempt, eg. alerting on an available call appearance.

Enabling the extension specific setting Disable Speakerphone will turn all auto-answer calls, including handsfree announced transfers to the extension, into normal calls.

Off-Hook Station Analog Phones Analog phone extensions configured as Off-Hook Station can auto-answer transfers when off-hook and idle.

Headset Users The following applies to users on supported phones with a dedicated **HEADSET** button. These users, when in headset mode and idle will auto-answer the announced transfer enquiry call through the headset after hearing 3 beeps. The transfer completion will require them to press the appropriate call appearance unless they are set to Headset Force Feed.

Twinning Handsfree announced transfer calls to users with twinning enabled will be turned into normal calls.

Multi-site network Support Dial Direct is supported to targets across a multi-site network, therefore allowing handsfree announced transfers to remote users.

Full Handsfree Transfer Operation

If required the system can be configured to allow the full handsfree announced transfer process, ie. both the enquiry call and the transfer, to be auto-answered on supported phones. This is done by entering **FORCE_HANDSFREE_TRANSFER** into the Source Numbers of the NoUser user and rebooting the system

One Touch Transferring

This feature allows selected users to transfer calls to each other using a reduced number of key presses.

With this option, a call can be transferred by simply selecting the transfer destination and then hanging up (or pressing **Transfer** if working handsfree).

Without this option the normal sequence is to press `Transfer`, dial the destination and then hanging up (or pressing **Transfer** if working handsfree).

For one touch transfer the transfer destination number must be selected using a button programmed to one of the following features:

- **User**
- **Dial**
- **Abbreviated Dial**
- **Automatic Intercom**
- **Dial Intercom**
- **Dial Direct**

This feature is enabled on a per user basis by adding **Enable_OTT** to the user's Source Number settings. This feature is supported on all Avaya phones that support the programmable button features above except T3 phones.

Centrex Transfer

Centrex Transfer is a feature provided by some line providers on external analog lines. It allows the recipient of a calls on such a line to transferred that call to another external number. The transfer is then performed by the line provider and the line is freed. Without Centrex Transfer, transferring an external call to another external number would occupy both a incoming and outgoing line for the duration of the call.

The following are the supported controls and usages for Centrex Transfer:

- **Centrex Transfer Button Operation** The action **Flash Hook** (**Advanced | Miscellaneous | Flash Hook**) can be assigned to programmable buttons on DS and IP phones. This button can be configured with or without a telephone number for an automatic or manual transfer respectively.
  - **Manual Transfer** If the programmable button is setup as a Flash Hook button without a target telephone number, pressing the button returns dial tone to the user. They can then dial the required transfer number and when they hear ringing or an answer, hang up to complete the Centrex Transfer.
  - **Automatic Transfer** If the programmable button is setup as a Flash Hook button with a target telephone number, pressing the button performs the Centrex Transfer to the numbers as a single action.
- **Centrex Transfer Short Code Operation** The short code feature Flash Hook can be used with system short codes. It can be setup with or without a telephone number in the same way as a Flash Hook programmable button detailed above. The line group must be the group of analog lines from the Centrex service line provider.
  - **Centrex Transfer Operation for Analog Extensions** Most analog phones have a button that performs the action of sending a hook flash signal. The marking of the button will vary and for example may be any of R, H, Recall or Hold. For system analog extensions, pressing this button sends a hook flash to the system to hold any current call and return dial tone.
    - To perform a Centrex Transfer, pressing the analog extension's hook flash button should be followed by the dialing of a Flash Hook short code.
    - For analog extension users with Call Waiting enabled, pressing the hook flash button during a call will hold the current call and connect any call waiting. Therefore it is recommend that analog extension users wanting to use Centrex Transfer should not also have Call Waiting enabled.
  - **Transfer from Voicemail/Auto-Attendant** This operation is only supported through Voicemail Pro using an Assisted Transfer action with the destination set to a Flash Hook short code.

Additional Notes

Addition Prefix Dialing In some cases the Centrex service provider may require a prefix for the transfer number. If that is the case, that prefix must be inserted in the button programming or the short code used for the Centrex Transfer.

Application Transfers Centrex Transfer is not supported for calls being held and transferred through applications such as SoftConsole.

Conference Calls Centrex Transfer is not supported with conference calls.

Hot Desking

Hot desking allows users to log in at another phone. Their incoming calls are rerouted to that phone and their user settings are applied to that phone. There are a number of setting and features which affect logging in and out of system phones.

In order to hot desk, a user must be assigned a Login Code (User | Telephony | Supervisor Settings) in the system configuration.

By default, each system extension has an **Base Extension** setting. This associates the extension with the user who has the matching **Extension** settings as being that extension's default associated user.

- By leaving the **Base Extension** setting for an extension blank, it is possible to have an extension with no default associated user. All extensions in this state use the settings of a special user named **NoUser**. On suitable phones the display may show **NoUser**.
- You can create users whose Extension directory number is not associated with any physical extension. These users must have a log in code in order to log in at a phone when they need to make or receive calls. In this way the system can support more users than it has physical extensions.

When another user logs in at an extension, they take control of that phone. Any existing user, including the default associated user, is logged out that phone.

- Any user settings not applicable to the type of phone on which the user has logged in become inaccessible. For example some programmable button features will become inaccessible if the phone at which a user logs in does not have a sufficient number of programmable buttons.
- Note that settings that are stored by the phone rather than by the system remain with the phone and do not move when a user hot desks.

1400 Series, 1600 Series, 9500 Series, 9600 Series, M-Series and T-Series telephones all use the centralized call log and centralized personal directory features that move those settings with the user as they hot desk.

Other Avaya H.323 IP telephones can be configured to backup and restore user settings to a file server when a user hot desks between phones. The range of settings supported depends on the particular phone model. Refer to the IP Office H.323 IP Telephone Installation Manual.

For all other features and phone types, it must be assumed that any settings and data shown by the phone is stored by the phone and are still accessible after logging off.

When a user logs off or is logged out by someone else logging in, they are automatically logged back in at the extension for which they are the default associated user if no one else is logged in at that extension. However this does not happen for users set to **Forced Login** (User | Telephony | Supervisor Settings).

For each user, you can configure how long the extension at which they are logged in can remain idle before they are automatically logged out. This is done using the Login Idle Period option. This option should only be used in conjunction with Force Login.

Logged in users who are members of a hunt group can be automatically logged out if they do not answer hunt group calls presented to them. This is done by selecting **Logged Off** as the user's **Status on No Answer** (User | Telephony | Supervisor Settings) setting.

Calls to a logged out user are treated as if the user is busy until the user logs in.

Logging in and out at a phone can be done either using system short codes or programmable buttons.

- The default system short code for logging in, is ***35*N#** where the user replaces N with their extension number and then log in code separated by a *****. This uses the short code feature ExtnLogin. If the user dials just a log in code as N, it is checked against the user with the same extension number as the extension's base extension number.
- The default system short code for logging out is ***36**. This uses the short code feature ExtLogout.
- The ExtnLogin and ExtnLogout features can be assigned to programmable buttons on suitable Avaya phones. The **ExtnLogin** button will then prompt the user to enter their details.

Related Links

Remote Hot Desking on page 683
Call Center Agents on page 684
Hot Desking Examples on page 684
Automatic Log Out on page 686

Remote Hot Desking

The system supports hot desking between systems within a network.

In the descriptions below, the system on which the user is configured is termed their 'home' system, all other systems are 'remote' systems.

When a user logs in to a remote system:

- The user's incoming calls are rerouted to that system.
- The user's outgoing calls uses the settings of the remote system.
- The user's license privileges move with them, for example their user profile setting is retained. The host system does not need to be licensed for the user.

- The user's own settings are transferred. However, some settings may become unusable or may operate differently.
- User rights are not transferred to the remote system but the name of any user rights associated with the user are transferred. If user rights with the same name exist on the remote system, then they will be used. The same applies for user rights applied by time profiles, if time profiles with the same name exist on the remote system .
- Appearance buttons configured for users on the home system will no longer operate.
- Various other settings may either no longer work or may work differently depending on the configuration of the remote system at which the user has logged in. For example: For T3 phones, the personal directory is not transferred with the user.
- The rights granted to the user by their **Profile** settings are retained by the user. There is no requirement for the remote system to have the appropriate licenses for the **Profile**.

If the user's home system is disconnected while the user is remotely hot desked, the user will remain remotely hot desked. They can remain in that state unless the current host system is restarted. They retain their license privileges as if they were on their home system. Note however that when the user's home system is reconnected, the user may be automatically logged back onto that system.

Break Out Dialing In some scenarios a hot desking user logged in at a remote system will want to dial a number using the system short codes of another system. This can be done using either short codes with the **Break Out** feature or a programmable button set to **Break Out**. This feature can be used by any user within the multi-site network but is of most use to remote hot deskers.

Related Links

Hot Desking on page 682

Call Center Agents

On systems with a call center application such as Compact Contact Center (CCC) or Compact Business Center (CBC), logging in and logging out is a key part of tracking and reporting on call center agents. It also controls call distribution as, until the agent logs in, their hunt group membership is seen as disabled.

For CCC, CBC and Delta Server, an agent is defined as being a user with a Login Code and set to Forced Login. Those users consume a CCC agent license.

Related Links

Hot Desking on page 682

Hot Desking Examples

The following are example of different ways that the hot desking settings can be used.

Related Links

Hot Desking on page 682

Scenario 1: Occasional Hot Desking

About this task

In this scenario, a particular user, for this example extension 204, needs to occasionally work at other locations within the building.

Procedure

1. A **Login Code** is added to the user's configuration settings, for this example **1234**.
2. The user can now log in when needed at any other phone by dialing ***35*204*1234#**.

   The phone's default associated user is logged out by this and their calls get busy treatment. User 204 is also logged out their normal phone and their calls now rerouted to the phone at which they have logged in.
3. When finished, the user can dial ***36** to log out.
4. This logs the phone's normal default user back on.

   Its also logs the hot desking user back on at their normal extension.

Scenario 2: Regular Hot Desking

About this task

This scenario is very similar to the one above. However, the user doesn't want to be automatically logged back in on their normal phone until they return to its location.

Procedure

1. A **Login Code** is added to the user's configuration settings, for this example **1234**.
2. The Forced Login option is selected.
3. When the user logs out of the phone that they are currently using, they are no longer automatically logged in on their normal extension.

   When they return to it they must dial ***35*204*1234#** to log in.
4. Whilst not logged in anywhere, calls to the user receive busy treatment.

Scenario 3: Full Hot Desking

About this task

Similar to the scenarios above but this time the user doesn't have a regular phone extension that they use. In order to make and receive calls they must find a phone at which they can log in.

Procedure

1. The user is given an Extension directory number that is not matched by the extension directory number setting of any existing extension.
2. They are also given a **Login Code** and a **Login Idle Period** is set, for this example 3600 seconds (an hour).

Forced Login isn't required as the user has no default extension at which they might be automatically logged in by the system.

3. The user can now log in at any available phone when needed.
4. If at the end of the business day they forget to log out, the Login Idle Period will eventually log them off automatically.

Scenario 4: Call Center Hot Desking

About this task

In this scenario, the phone extensions have no default extension number. Several phones set like this might be used in a call center where the agents use whichever desk is available at the start of their shift. Alternatively a set of desks with such phones might be provided for staff that are normally on the road but occasionally return to the office and need a temporary desk area to complete paper work.

Procedure

1. For the extensions, the Extension setting is left blank.

   This means that those phones will be associated with the NoUser user's settings and display **NOT LOGGED ON**.

2. The call center agents or road-warrior users are configured with Extension directory numbers that also don't match any existing physical extensions.

   They are all given Login Code numbers.

3. The users can log in at any of the extensions when required.

   When they log out or log in elsewhere, the extensions return to the NoUser setting.

Automatic Log Out

Normally a user can either log themselves out or be logged out by another user logging in. The following methods can be used by the system to automatically log out a user. A remote hot desking user whose home system can no longer be seen by the remote system at which they are logged in is automatically logged out after 24 hours.

The following methods only apply to users with a **Login Code** and set to **Forced Login**.

Idle Timeout

The user Login Idle Period (User | Telephony | Supervisor Settings) can be used to automatically log out the user after a set period of phone inactivity. The period can be set between 1 to 99999 seconds and is based on call inactivity other than ringing calls.

Unanswered Calls

Users who are members of hunt groups are presented with hunt group calls when they are logged in and not already on a call. If the user is logged in but not actually present they will continue to be presented with hunt group calls. In this scenario it can be useful to log the user off.

For the hunt group On the Hunt Group | Hunt Group tab, use the Agent's Status on No Answer Applies to setting to select which types of unanswered hunt group calls should change the user's status. The options are:

None.

Any Calls.

External Inbound Calls Only.

For the user The Status on No Answer (User | Telephony | Supervisor Settings) can be used. This sets what the user's status should be changed to if they do not answer a hunt group call. The options are:

Logged In If this option is selected, the user's status is not changed.

Busy Wrap-Up If this option is selected the user's membership status of the hunt group triggering the action is changed to disabled. The user can still make and receive calls and will still continue to receive calls from other hunt groups to which they belong.

Busy Not Available If this option is selected the user's status is changed to do not disturb. This is the equivalent of DND and will affect all calls to the user.

Logged Off If this option is selected the users status is changed to logged out. In that state the cannot make calls and cannot receive calls. Hunt group calls go to the next available agent and personal calls treat the user as being busy.

Related Links

Hot Desking on page 682

Chapter 15: Configuring the Avaya Session Border Controller for IP Office Remote Workers

Related Links

Overview on page 688
Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Overview

The Avaya Session Border Controller for Enterprise (SBCE) delivers security to a SIP-based Unified Communications network. This document describes how to configure the SBCE for IP Office Remote Workers.

Related Links

Configuring the Avaya Session Border Controller for IP Office Remote Workers on page 688
Remote access on page 688
Licencing on page 689
Remote Worker best practices on page 689
Provisioning SIP Phones on page 690

Remote access

When the SBCE is in an IP OFFICE Solution registration and remote access to the SBCE is done jointly with IP Office. Remote access is thru the SSL VPN on the IP OFFICE and hopping to the SBCE. For more information, see the document “ASBCE GRT Registration and Remote Connectivity via IP Office SSL/VPN NAPT” on support.avaya.com.

Related Links

Overview on page 688

Licencing

Licensing takes place once the SBCE is on the network and in the Commissioned state. Retrieval and activation of licensing for Avaya SBCE is done via Avaya's PLDS (Product Licensing and Distribution System). Access to PLDS is via the Avaya Support Portal at the URL `https://plds.avaya.com`.

For the SBCE, the SBCE EMS element is its own license hst for licensing specific to the SBCE. Licensing is managed for SBCE within PLDS by a user-defined host name and the MAC address of the management interface. ecide on a user defined license host name for the SBCE at the physical site. This will be the license host name used to activate SBCE licenses in PLDS.

On the SBCE, run the command `ifconfig` to determine the MAC address of the management network interface.

- The MAC address of the management interface of the Portwell CAD is the Eth5 port.
- For a single Dell server deployment, the management interface MAC address is the Eth 5 port.

The license file for the SBCE must be uploaded so that Avaya Services can provide support for what the customer is licensed for. Customers are still under the EULA for their license just like in prior releases. After activating the license on PLDS and getting the XML file via emal, use the SBCE management interface to upload and install the license.

To install the license:

1. Log in to the SBCE management interface.
2. In the navigation tree on the left, select **System Management** and then click **Install**.
3. In the Install License window, click Browse and navigate to the license file.
4. You can **Append** the license or **Overwrite**. Only overwrite if required.
5. You can **Group By Product** or **License File**.

Related Links

Overview on page 688

Remote Worker best practices

- For all non SIP and media related traffic, or any specific IP Office or endpoint configuration and requirements see *Administering Avaya Communicator on IP Office* and *Administering Avaya one-X® Mobile for IP Office*.

  For example, XMPP will go direct from endpoint to One-X portal through the firewall and not through the SBCE.
- For security best practices, see the ASBCE Security Configuration Guide.
- For SBCE configuration see *Administering Avaya Session Border Controller for Enterprise*.

- Use encryption with endpoints that are capable. The following table summarizes device specific support.

Client type	Uses to the external interface of the SBCE		
	TLS	SRTP Audio	SRTP Video
Avaya Communicator for Windows	Y	Y	N
Avaya Communicator for iPad	Y	Y	N
one-X Mobile Preferred VoIP client for Android	Y	N	N
one-X Mobile Preferred VoIP client for iOS	N	N	N

- If Media or Signaling QoS are required, they must be configured on the SBCE as the SBCE does not pass through.
- Customer firewall configuration requires forwarding of video/audio signaling and media ports. SIP ALG's should be disabled on any firewalls.
- For troubleshooting the best rules to follow are to look at Alarms/Incidents and take a packet capture to determine if the issue is on the SBCE. If further debugging is required, enable debug logs and get the appropriate elogs.
- If doing remote worker and trunking on the same SBCE, you use a second set of IP addresses on the SBCE for trunking. See the SBCE documentation and application notes on configuring SBCE for trunking.
- Review SBCE, IP Office, and endpoint release notes for fixes, limitations, and workarounds.

Related Links

Overview on page 688

Provisioning SIP Phones

The desired way to provision for Remote Workers in an IP Office and Session Boarder Controler Enterprise (SBCE) deployment is to have HTTP/HTTPS traffic relayed by the SBCE between Remote Workers and the IP Office. 11xx, 12xx, and E129 SIP sets must first be provisioned locally on the IP Office. Then, those sets are moved to the remote location on the SBCE public side. The administrator must manually configure the provisioning IP address and set it to the SBCE public HTTP/S reverse-proxy IP address using the following NoUser User Source Numbers (See **User | User Source Numbers**).

- RW_SBC_REG=<SBC-B1-public-SIP-IPaddr>
- RW_SBC_PROV=<SBC-B1-private-HTTP/S-IPaddr>
- RW_SBC_TLS=<SBC-public-TLS-port>
- RW_SBC_TCP=<SBC-public-TCP-port>
- RW_SBC_UDP=<SBC-public-UDP-port>

Those IDs are applicable only to SBCE Remote Worker SIP sets. If RW_SBC_REG_IP and RW_SBC_PROV_IP are not entered, the other source number are ignored. One of three SBCE ports (RW_SBC_TLS/RW_SBC_TCP/RW_SBC_UDP) port must be entered. The recommendation is to enter all relevant SBCE ports.

- For 11xx and 12xx sets, all ports are sent to the set and the set chooses the protocol to register to SBC in the following rpiority: tls,tcp,udp.
- For E129 sets, IP Office chooses the SBCE TLS port if configured.
- If SBCE TLS is not configured, IP Office chooses SBCE TCP port if configured.
- If SBCE TCP port is not configured, IP Office chooses SBCE UDP port.

Therefore, you can choose different combinations of Source Number IDs depending on the desired SBCE configuration. IP Office checks whether the SIP set provisioning HTTP/HTTPS requests are coming from the RW_SBC_PROV_IP address. In that case, IPO will send RW_SBC_REG_IP to the set as a SIP Server for E129 (or S1/S2 for 11xx and 12xx). For E129 sets, the outbound-proxy filed is used to provide RW_SBC_REG_IP. In addition, Config path, Provisioning path and Phonebook path are removed from the cfg.xml file for IPO SBC RWs since those must be manually configured before moving E129 sets to the remote location on SBCE public side.

The recommended configuration is to use homogeneous protocols:

- If TLS is used between Remote Workers and SBCE, then TLS should be used between SBCE and IP Office.
- If TCP is used between Remote Workers and SBCE, then TCP should be used between SBCE and IP Office.
- If UDP is used between Remote Workers and SBCE, then UDP should be used between SBCE and IP Office.
- If SRTP is used between Remote Workers and SBCE, then SRTP should be used between SBCE and IP Office.
- If RTP is used between Remote Workers and SBCE, then RTP should be used between SBCE and IP Office.

Related Links

Overview on page 688

Configuring Session Border Controller Enterprise for IP Office Remote Workers

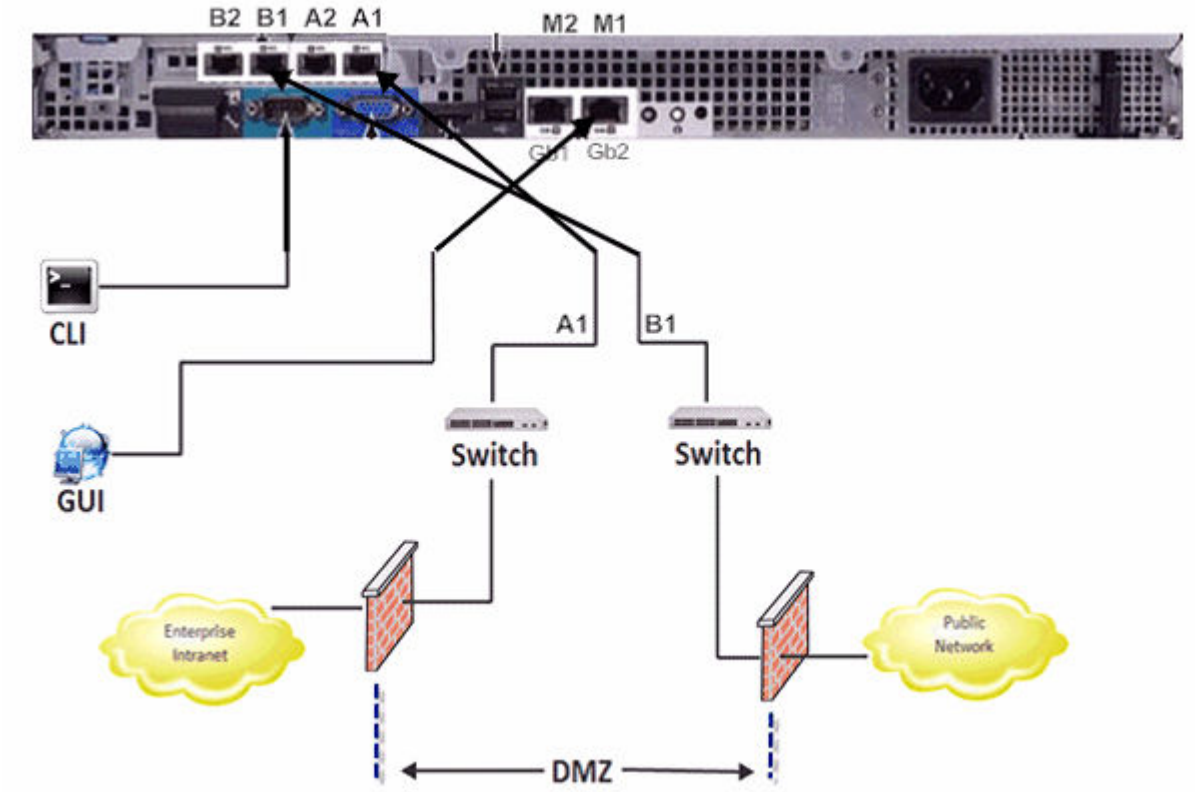
Related Links

Configuring the Avaya Session Border Controller for IP Office Remote Workers on page 688
Network interfaces on page 692
Creating a backup on page 693
Configuring network address translation on page 694
Enabling interfaces on page 694
Configuring media interfaces on page 695

Network interfaces

The example below shows a two wire deployment of a Dell Session Border Controller for Enterprise (SBCE) in a demilitarized zone (DMZ). It is common to have only an external firewall, but it is possible to have a firewall on both sides of the DMZ. For a description of the distinction between one and two wire deployments, see *Avaya Session Border Controller for Enterprise Overview and Specification*.

Single server deployment



The following requirements apply to a single server two wire deployment.

- M1 is used for management.
- A1 is used to communicate with IP Office.
- B1 is used to communicate with the endpoints.
- M1, A1, and B1 all require an IP address. M1 cannot be on the same subnet as A1 or B1.
- If A1 and B1 are on same subnet, you can do a one-wire deployment and use A1 only for data. M1 is still required for management.
-
- Since the Portwell CAD has fewer interfaces, M2 or B2 are not listed on the back. M1, A1, and B1 are the ports used on Portwell SBC hardware as well. All network interfaces on the SBC are auto negotiate, so the switch or router ports that the SBC connects to must also be set to auto negotiate.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Creating a backup

Backup the empty SBCE configuration. This enables you to start again from scratch.

Procedure

1. Login to the SBCE Control Center as `Admin`.
2. In the navigation tree on the left, select **Backup/Restore** and then select the **Snapshots** tab.
3. Click Create Snapshot.
4. Enter a description and then click Create.
5. Click Download and save the file locally.

Next steps

When you have finished the configuration, create another snapshot. See *Administering Avaya Session Border Controller for Enterprise* for a procedure to configure automatic backup to an SFTP server.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Configuring network address translation

If you have a firewall in front or behind the SBCE and are natting the SBCE IP address, you must perform this procedure.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Network Management**.
3. Select the **Network Configuration** tab.
4. Enter the IP address you are natting in the **Public IP** field.

   The SBC will nat the SIP messages with the IP address.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Enabling interfaces

Enable the interfaces A1, internal to the IP Office, and B1, external to the phones, that were configured during installation. If configuring a one-wire deployment, you will only enable A1. For Portwell CAD hardware, B2 and M2 do not exist.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Network Management**.
3. Select the **Interface Configuration** tab.
4. Enable the required interfaces.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Configuring media interfaces

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Media Interfaces**.
3. Click **Add**.
4. Enter the name for internal interface and then select the A1 IP address from the pull down menu.
5. Enter the media port range and click **Finish**.

   The default port range used is 35000-40000.
6. Click **Add**.
7. Enter the name for external interface and then select the B1 IP address from the pull down menu.
8. Enter the media port range and click **Finish**.

   The default port range used is 35000-40000.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Configuring signalling interfaces

Procedure

1. Login to the SBCE Control Center as `Admin`.
2. In the navigation tree on the left, expand **System Management**.
3. Select **Device Specific Settings** and then **Signalling Interfaces**.
4. Click **Add**.
5. Enter the name for internal interface and the select the A1 IP address from the pull down menu.
6. For the transport to be used on that interface, put in the port in the chosen transport field or fields and click Finish.

   TCP port 5060 is the required transport for remote workers on IP Office.
7. Click **Add**.
8. Enter the name for external interface and the select the B1 IP address from the pull down menu.
9. For the transport to be used on that interface, put in the port in the chosen transport field or fields and click Finish.

   TCP port 5060 is the required transport for remote workers on IP Office.
10. TLS port 5061 is the preferred transport for remote worker towards the Avaya endpoints if the endpoint supports it. If using TLS, select the default Avaya TLS server profile on the external interface. If the endpoint doesn't support TLS, then use TCP and look at the IP Office remote worker guides for Avaya Communicator and one-X Mobile clients for information on protocols to use.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Configuring server interworking profiles

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Global Profiles**.
3. Select **Server Interworking**.
4. The profile used for remote workers on the IP Office is **avaya-ru** server interworking. Highlight the **avaya-ru** profile.
5. Click **Clone**.

6. Enter a name for the profile and click **Finish**.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Configuring phone interworking profiles

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Global Profiles**.
3. Select **Phone Interworking**.
4. Select the **avaya-ru** profile and click **Clone**.
5. Enter a name for the profile and click **Finish**.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Configuring the call server

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Global Profiles**.
3. Select **Server Configuration**.
4. Click **Add**.
5. Enter a name.
6. In the **Server Type** field, select **Call Server** from the pull down menu.
7. In the **IP Addresses** field, the IP Office IP address.
8. Check the **Supported Transports** you want to use.

   TCP is required for remote worker but you may have UDP if you are also using the SBC for SIP trunks.
9. In the **Transport Port** fields enter the port to be used (for example port 5060).

10. Click Next three times.
11. Do not enable **Grooming**. IP Office uses different TCP connections to each endpoint.
12. For the interworking profile, choose **avaya-ru** or a cloned version of it.
13. Click **Finish**.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Configuring routing profiles

Routing profiles define packet routing criteria in order to route them to the right destination. Routing profiles are "applied" to Endpoint Flows. Clone an existing routing profile as a starting point or create a new one. Do not change the default profile.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Global Profiles**.
3. Select **Routing**.
4. Click **Add**.
5. Enter a name for the profile.
6. Click **Next**.
7. In the **Next Hop Server 1** field, enter the IP Office IP address.

   You can use the IP Office fully qualified domain name (FQDN).

   If using a non default port of 5060, you must put the IP colon port in the **Next Hop** field. For example 10.3.3.3:5070.
8. Click on the appropriate **Outgoing Transport** to be used for IP Office.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Configuring topology hiding

Topology Hiding is an SBCE security feature which allows you to change key SIP message parameters to mask how your enterprise network may appear to an unauthorized or malicious user. If required, Topology Hiding is applied to flows. The server flow points towards IP Office and the subscriber flow points towards the endpoints.

Note that if you want to pass what you get from the endpoints, then a Topology Hiding profile is not required.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Global Profiles**.
3. Select **Topology Hiding**.
4. Click on the default profile and then click **Clone**.
5. Enter a name and click **Finish**.
6. The profile just created is highlighted. Click **Edit**.
   - If IP Office is configured to accept a specific domain then in the **From, To, and Request-Line** field, select **Overwrite**, enter the domain name and click **Finish**.
   - If IP Office is configured to accept a specific domain then in the **From, To, and Request-Line** field, select **Destination IP**and click **Finish**.
   - If no special criteria is required, leave everything as **Auto** and click **Finish**.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Configuring endpoint policy groups

Create a new endpoint policy group. Do not change the default group.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Domain Policies** and then **End Point Policy Groups**.
3. Click **Add** and enter a name for the IP Office server flow.
4. Click **Next**.
5. Choose the appropriate **Rules** and click **Finish**.
6. Click **Add** and enter a name for the subscriber flow.
7. Click **Next**.
8. Choose the appropriate **Rules** and click **Finish**.

Next steps

The following three procedures for end point policy groups show changing the application rule for max sessions, the media rule for QoS and RTP or SRTP, and the signaling rule for QoS. See *Administering Avaya Session Border Controller for Enterprise* for additional information on domain polices.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Configuring endpoint policy groups application rules

Clone an existing application rule as a starting point or create a new one. Do not change the default.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Domain Policies** and then **Application Rules**.
3. Click **Add** and enter a name for the one to be used by the IP Office End Point Policy Group.
4. Click **Next**.
5. Check **In and Out for Voice**and put in the amount of concurrent sessions required for the license. Put the same value for **Max Concurrent Sessions** and **Max Sessions Per Endpoint**.

   It is best practice to put more than the license as this is not counted one or one with license session. For example, if they have license of 300 concurrent sessions put 500 for each box.

   If you need video, you must do the same for video. If you clone the default, Audio is already enabled you only need to adjust the values and then enable video.
6. Click **Finish**.
7. Repeat to create a rule used by the Subscriber Flow End Point Policy Group. For the subscriber flow rule, put the **Max Concurrent Sessions** higher than the license. However, for **Max Sessions Per Endpoint**, the recommended value is 10. You can use a higher value if required.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Configuring endpoint policy groups media rules

Clone an existing media rule as a starting point or create a new one. Do not change the default.

Media rules are defined under **System Management** > **Domain Policies** > **Media Rules**. The requirements for media rules are as follows.

- It is recommended to clone a profile like the default-low-med profile. The default Media Rule has the **Media QoS** setting of **DSCP EF** enabled.
- When you create a new media rule, the default is . This must be changed tor another option that meets the current requirements.
- On the Media Encryption tab, set the SBC to RTP or SRTP to an endpoint or IP Office. For Media Encryption, set the preferred Audio Format as RTP in the rule for IP Office. Towards the endpoints, the rule used can be set to SRTP if the endpoint supports it. Otherwise use RTP. Ensure Encrypted RTCP is unchecked and Interworking is checked. For Video ensure RTP is selected.
- For all other tabs, use the default settings.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Configuring endpoint policy groups signalling rules

Clone an existing media rule as a starting point or create a new one. Do not change the default.

Media rules are defined under **System Management** > **Domain Policies** > **Signalling Rules**. The requirements for signalling rules are as follows.

- It is recommended to clone a profile like the default-low-med profile. The default Media Rule has the **Signalling QoS** setting of **DSCP AF41** enabled.
- When you create a new signalling rule, the default is **TOS**. This must be changed to **DSCP AF41** or another option that meets the current requirements.
- For all other tabs, use the default settings.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Configuring server flows

A server flow is required for the IP Office.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

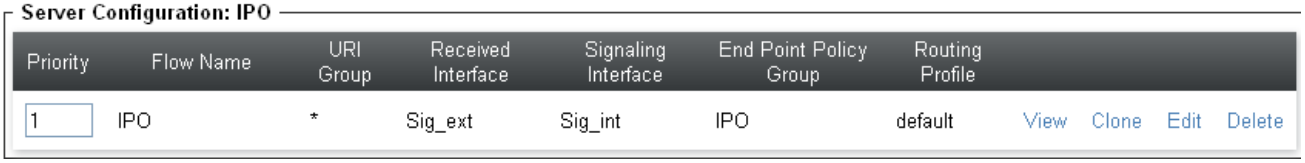
1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **End Point Flow**.
3. Select **Server Flow**.

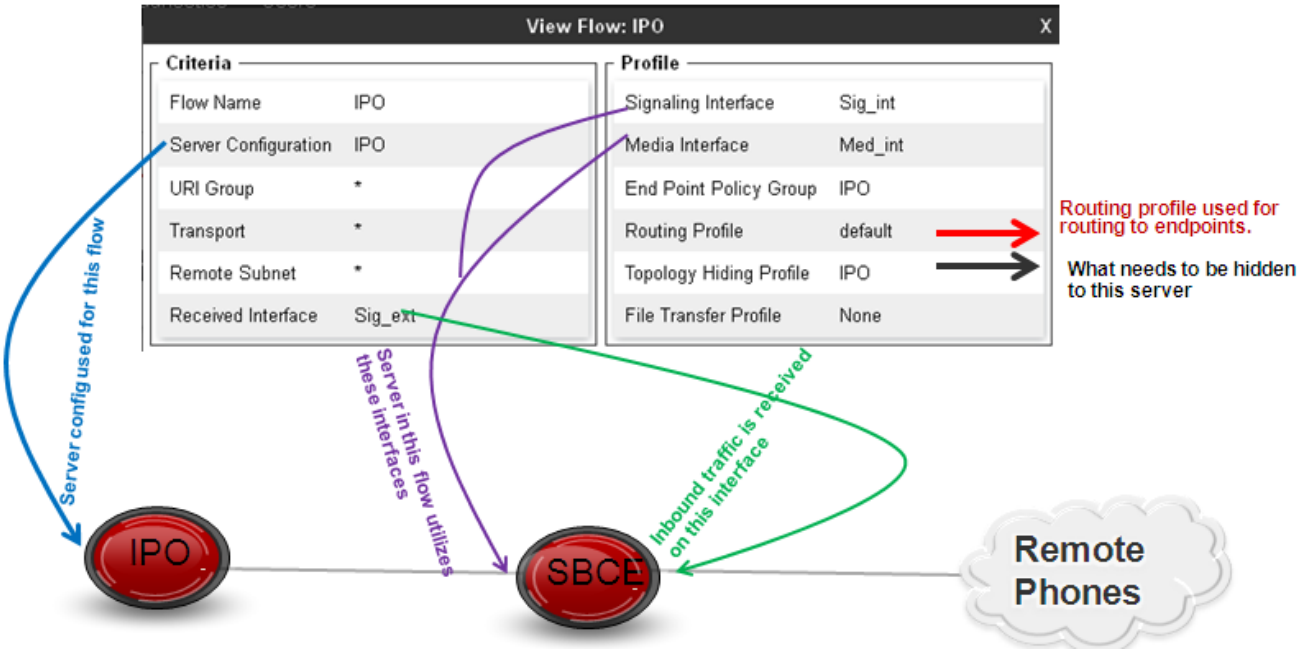
4. Click **Add**.
5. Enter a name for the IP Office flow.
6. In the **Server Configuration** field, select the IP Office server configuration.
7. In the **Received Interface** field, select the external signaling interface.
8. In the **Media Interface** field, select the IP Office interface.
9. In the **Signaling Interface** field, select the IP Office interface.
10. In the **End Point Policy** field, select the policy group created for IP Office.
11. In the **Routing Profile** field, select the default routing profile.
12. If required, in the **Topology Hiding Profile**, select profile created for IP Office.
13. Click **Finish**.

Example IP Office server flow

Note:

If doing remote worker and trunking to the same SM you will have two SM server flows. One with the remote worker received interface and the default routing profile and the other with the trunk received interface and the to_trunk routing profile





Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Configuring user agent profiles

User Agent profiles can be created using what the endpoints send in the user agent header. When these profiles are put in a subscriber flow, only phones that match that User Agent are allowed to send registration or other messages through the SBCE.

Before you begin

You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Global Parameters** and then **User Agents.**.
3. Click **Add**.
4. Enter a description then put in the type of user agent the endpoint you want to allow using regular expression. You can use one type per policy or you can put multiple types in one user agent profile.
5. Click **Finish**.
6. You can add the user agent header to a subscriber flow during the flow configuration or by editing an existing flow. In the subscriber flow **User Agent** field, select the user agent profile.

Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Configuring subscriber flows

Subscriber flows are required to route registrations and calls from the phones to and from the IP Office.

Before you begin

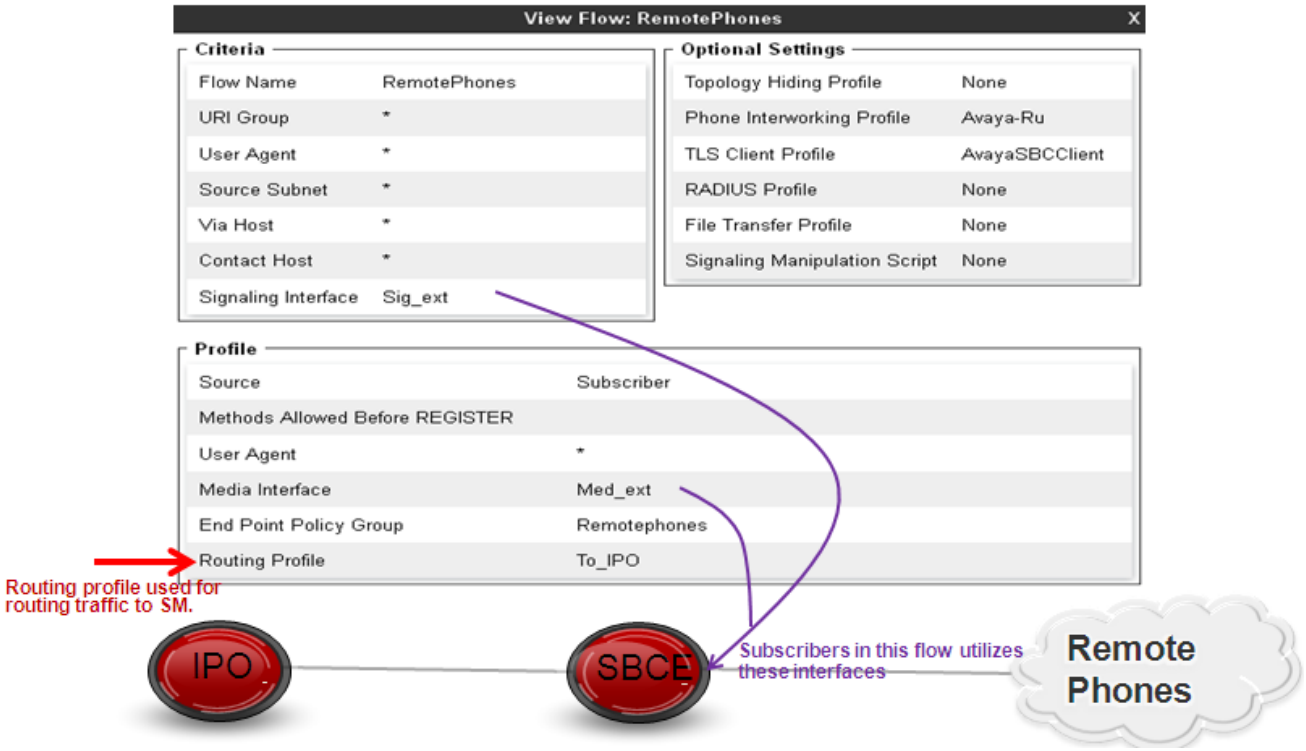
You must be logged into the SBCE Control Center as `Admin`.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **End Point Flow**.
3. Select **Subscriber Flow**.
4. Click **Add**.
5. Enter a name for the end point flow.

6. The **URI Group** and **User Agent** fields can be used to only allow certain DID's or phone types to use that flow.
7. In the Signaling Interface field, select the external signaling interface.
8. Click Next.
9. In the **Media Interface** field, select the external media interface.
10. In the **End Point Policy Group** field, select the policy group created for the endpoints.
11. In the **Routing Profile** field, select the profile to route to the IP Office.
12. The **Topology Hiding** field can be used if you want to send something specific to the phones. It can be left blank.
13. In the **Phone Interworking Profile** field, select **avaya-ru** or the recommended cloned copy of **avaya-ru**.
14. If using TLS, put in the default **TLS Client Profile** called **AvayaSBCClient**.
15. Click **Finish**.

Example subscriber flow



Related Links

Configuring Session Border Controller Enterprise for IP Office Remote Workers on page 691

Chapter 16: Configuring SIP Trunks

Related Links

Overview

A growing number of service providers now offer PSTN access to businesses via public SIP trunk connections, either to extend their reach beyond their typical copper based network coverage areas, or so that multiple services (voice and internet access) can be bundled into a single network connection. Although detailed public SIP trunk service offerings vary depending on the exact nature of the offer from the specific service provider, SIP trunks can potentially provide several advantages compared to traditional analog or digital trunks. These advantages include:

- cost savings resulting from reduced long distance charges, more efficient allocation of trunks, and operational savings associated with managing a consolidated network
- simplified dialing plans and number portability
- geographic transparency for local accessibility creating a virtual presence for incoming calls
- trunk diversity and redundancy
- multi-media ready to roll out future SIP enabled applications
- fewer hardware interfaces to purchase and manage, reducing cost and complexity
- faster and easier provisioning

IP Office delivers functionality that enhances its ability to be deployed in multi-vendor SIP-based VoIP networks. While this functionality is primarily based on the evolving SIP standards, there is no guarantee that all vendors, interpret and implement the standards in the same way. To help the SIP service provider, Avaya operates a comprehensive SIP Compliance Testing Program referred to as GSSCP. Avaya's DevConnect program validates the operation of the IP Office solution with the service provider’s SIP trunk offering.

Related Links

Configuring SIP Trunks on page 705

Configuring a SIP Trunk

This procedure provides the basic steps for configuring a SIP trunk. To view the configuration field descriptions for SIP trunks, go to SIP Line on page 336.

Before you begin

- You must know the IP address of both ends of the trunk.
- You must have valid licenses on both IP Office systems.
- On Server Edition, make sure you have a non-zero value in the **Maximum SIP Sessions** field on the **System | Telephony | Telephony** tab. If you do not, you will see Monitor messages about insufficient licenses.

Procedure

1. In the Manager navigation pane, right click **Line** and select **New** > **SIP Line**.
2. On the **SIP Line** tab, record the **Line Number** value for use later.
3. In the **ITSP Domain Name** field, enter the domain name required by the far end.

   If nothing is configured in this field, then IP Office inserts the far end's **ITSP Proxy Address** from the **Transport** tab as the ITSP domain in the SIP messaging.
4. Use the default values for the remaining fields.
5. Select the **Transport** tab.
6. In the **ITSP Proxy Address** field, enter the IP Address of the far end.
7. Select the **SIP URI** tab.
8. Click **Add**.
9. Enter values for the **Incoming Group** and **Outgoing Group** fields.

   You can use the **Line Number** from the **SIP Line** tab for both values.
10. In the Manager navigation page, select **Incoming Call Route**.
11. On the **Standard** tab, in the **Line Group ID** field, enter the **Line Number** from the **SIP Line** tab.
12. Select the **Destinations** tab.
13. In the **Destination** column, replace the value with a period (“.”).
14. In the Manager navigation pane, select **Short Code**.
15. Add a short code to dial the trunk you have just added.
16. One end of the trunk is now configured. Save the configuration to the IP Office.

17. Using Manager, open the configuration for the IP Office at the other end of the SIP trunk and repeat the steps.

Related Links

Configuring SIP Trunks on page 705

SIP Line Requirements

Use of SIP requires the following:

- **SIP Service Account** An account or accounts with a SIP internet service provider (ITSP). The method of operation and the information provided will vary. The key requirement is a SIP URI, a web address of the form **name@example.com**. This is the equivalent of a SIP telephone number for making and receiving calls via SIP.
- **Voice Compression Channels** SIP calls use system voice compression channels in the same way as used for standard IP trunks and extensions. For an IP500 V2system, these are provided by the installation of VCM modules within the control unit. RTP relay is applied to SIP calls where applicable.
- **Licensing** SIP trunks require licenses in the system configuration. These set the maximum number of simultaneous SIP calls supported by the system.
- **Firewall Traversal** Routing traditional H.323 VoIP calls through firewalls often fails due to the effects of NAT (Network Address Translation). For SIP a number of ways to ensure successful firewall traversal can be used. The system does not apply any firewall between LAN1 and LAN2 to SIP calls.
  - **STUN (Simple Traverse of UDP NAT)** UDP SIP can use a mechanism called STUN to cross firewalls between the switch and the ITSP. This requires the ITSP to provide the IP address of their STUN server and the system to then select from various STUN methods how to connect to that server. The system can attempt to auto-detect the required settings to successfully connect. To use STUN, the line must be linked to the Network Topology settings of a LAN interface using the line's Use Network Topology Info setting.
  - **TURN (Traversal Using Relay NAT)** TCP SIP can use a mechanism called TURN (Traversal Using Relay NAT). This is not currently supported.
  - **Session Border Control** STUN is not required is the ITSP if a Session Border Controller (SBC) is used between the system and the ITSP. The system does not perform its own SBC.
- **SIP Trunks** These trunks are manually added to the system configuration. Typically a SIP trunk is required for each SIP ITSP being used. As the configuration provides methods for multiple URI's from that ITSP to use the same trunk. For each trunk at least one SIP URI entry is required, up to 150 SIP URI's are supported on the same trunk. Amongst other things this sets the incoming and outgoing groups for call routing.
- **Outgoing Call Routing** The initial routing uses any standard short code with a dial feature. The short code's Line Group ID should be set to match the Outgoing Group ID of the SIP URI

channels to use. However the short code must also change the number dialed into a destination SIP URI suitable for routing by the ITSP. In most cases, if the destination is a public telephone network number, a URI of the form **123456789@example.com** is suitable. For example:

- **Code**: 9N#
- **Feature**: Dial
- **Telephone Number**: N"@example.com"
- **Line Group ID**: 100

- **Incoming Call Routing** Incoming SIP calls are routed in the same way as other incoming external calls. The caller and called information in the SIP call header can be used to match Incoming CLI and Incoming Number settings in normal system Incoming Call Route records.
- **DiffServ Marking** DiffServ marking is applied to calls using the DiffServer Settings on the System | LAN | VoIP tab of the LAN interface as set by the line's **Use Network Topology Info** setting.

SIP URIs

Calls across SIP require URI's (Uniform Resource Identifiers), one for the source and one for the destination. Each SIP URI consists of two parts, the user part (for example **name**) and the domain part (for example **example.com**) to form a full URI (in this case **name@example.com**). SIP URI's can take several forms:

- name@117.53.22.2
- name@example.com
- 012345678@example.com

Typically each account with a SIP service provider will include a SIP URI or a set of URI's. The domain part is then used for the SIP trunk configured for routing calls to that provider. The user part can be assigned either to an individual user if you have one URI per user for that ITSP, or it can also be configured against the line for use by all users who have calls routed via that line.

If the wildcard * is used in the SIP trunk's **Local URI**, **Contact** and **Display** fields, that SIP trunk will accept any incoming SIP call. The incoming call routing is still performed by the system incoming call routes based on matching the values received with the call or the URI's incoming group setting. For outgoing calls using this SIP URI, all valid short code CLI manipulations are used (transforming calling party number to ISDN will be ignored).

Resource Limitation

A number of limits can affect the number of SIP calls. When one of these limits is reached the following occurs: any further outgoing SIP calls are blocked unless some alternate route is available using ARS; any incoming SIP calls are queued until the required resource becomes available. Limiting factors are:

- the number of licensed SIP channels.
- the number of SIP channels configured for a SIP URI.
- the number of voice compression channels.
- **SIP Line Call to/from Non-IP Devices** Voice compression channel required.

- **Outgoing SIP Line Call from IP Device** No voice compression channel required.
- **Incoming SIP Line Call to IP Device** If using the same codec, voice compression channel reserved until call connected. If using differing codecs then 2 channels used.

SIP Information Display

The full from and to SIP URI will be recorded for use by SMDR, CBC and CCC. For all other applications and for telephone devices, the SIP URI is put through system directory matching the same as for incoming CLI matching. First a match against the full URI is attempted, then a match against the user part of the URI. Directory wildcards can also be used for the URI matching.

Related Links

Configuring SIP Trunks on page 705

SIP Incoming Call Routing

Incoming SIP calls are routed using Incoming Call Routes in the same way as call arriving on other external trunks. The following **Incoming Call Route** fields are used to determine which route is the best match for a call.

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.

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 entry can be used to achieve the match, records being read from left to right. For IP addresses only full entry matching is supported.

The fields **Bearer Capability** and **Incoming Sub Address** are not used for matching of incoming SIP calls. The remain **Incoming Call Route** fields, including those voice recording, as used as for all call types.

If the wildcard * is used in the SIP trunk's **Local URI**, **Contact** and **Display** fields, that SIP trunk will accept any incoming SIP call. The incoming call routing is still performed by the system incoming call routes based on matching the values received with the call or the URI's incoming group setting. For outgoing calls using this SIP URI, all valid short code CLI manipulations are used (transforming calling party number to ISDN will be ignored).

Related Links

Configuring SIP Trunks on page 705

SIP Prefix Operation

The prefix fields **Prefix**, **National Prefix**, **Country Code** and **International Prefix** are available with the SIP Line settings. These fields are used in the following order:

1. If an incoming number (called or calling) starts with the + symbol, the + is replaced with the **International Prefix**.
2. If the **Country Code** has been set and an incoming number begins with that **Country Code** or with the **International Prefix** and **Country Code**, they are replaced with the **National Prefix**.
3. If the **Country Code** has been set and the incoming number does not start with the **National Prefix** or **International Prefix**, the **International Prefix** is added.
4. If the incoming number does not begin with either the **National Prefix** or **International Prefix**, then the **Prefix** is added.

For example, if the SIP Line is configured with prefixes as follows:

- **Line Prefix**: 9
- **National Prefix**: 90
- **International Prefix**: 900
- **Country Code**: 44

Number Received	Processing	Resulting Number
+441707362200	Following rule 1 above, the + is replace with the **International Prefix** (900), resulting in 900441707362200. The number now matches the **International Prefix** (900) and **Country Code** (44).Following rule 2 above they are replace with the **National Prefix** (90).	**901707362200**
00441707362200	Following rule 2 above the **International Prefix** (900) and the **Country Code** (44) are replaced with the **National Prefix** (90).	**90107362200**
441707362200	Following rule 2 above, the **Country Code** (44) is replace with the **National Prefix** (90).	**901707362200**
6494770557	Following rule 3 above the **International Prefix** (900) is added.	**9006494770557**

OPTIONS Operation

Options are not sent only when active SIP registration is present. In all other cases, OPTIONS are sent.

The interval is determined as follows.

- If no **User | Source Numbers | SIP_OPTIONS_PERIOD** parameter is defined and the **LAN1 | Network Topology | Binding Refresh Time** is 0, then the default value of 300 seconds is used.
- To establish a period less than 300 seconds, do not define a **SIP_OPTIONS_PERIOD** parameter and set the **Binding Refresh Time** to a value less than 300 seconds. The OPTIONS message period will be equal to the **Binding Refresh Time**.
- To establish a period greater than 300 seconds, a **SIP_OPTIONS_PERIOD** parameter must be defined. The **Binding Refresh Time** must be set to a value greater than 300 seconds. The OPTIONS message period will be the smaller of the **Binding Refresh Time** and the **SIP_OPTIONS_PERIOD**.

Related Links

Configuring SIP Trunks on page 705

SIP messaging

SIP trunk prerequisites

Before any calls can be made, the system must have sufficient SIP trunk licenses for the maximum number of simultaneous SIP trunk calls expected.

On Server Edition systems, the **System | Telephony | Telephony | Maximum SIP Sessions** value must match the total number of SIP set and trunk calls that can occur at the same time.

Related Links

Configuring SIP Trunks on page 705
Outgoing call message details on page 711
Incoming call message details on page 716
Codec selection on page 721
DTMF transmission on page 722
Fax over SIP on page 722
Hold scenarios on page 722
SIP REFER on page 724

Outgoing call message details

Related Links

SIP messaging on page 711
Destination URI on page 712
From field content on page 712
To field content on page 713
Contact field content on page 713

P-Asserted Identity field content on page 713
Typical outgoing call scenarios on page 714

Destination URI

The destination URI in an INVITE message has the general format of an e-mail address. Specific rules have been defined for expressing telephone numbers in this format. These rules are defined in RFC 2806 and RFC 3261 (section 19.1.6). A sample URI for a call on a SIP trunk is:

```
sip: 12125551234@ITSP_Domain SIP/2.0
```

The **ITSP_Domain** in the following headers is taken from the **SIP Line | ITSP Domain Name** field. If that is empty, the IP Address of the IP Office LAN interface is used or the public address of that interface if topology discovery is used.

Related Links

Outgoing call message details on page 711

From field content

If the call is originated from an IP Office endpoint, the settings on the **SIP line | SIP URI** tab determine whether the information should be taken from the trunk's SIP credentials, or from the **User | SIP** tab.

- If the channel's Local URI is set to ***** then the extension number of the set will be used for the User part of the identity.

  ```
  From: "SipDisplayNameAlice" <sip: 311@ITSP_Domain>;tag=8a9fed65b
  ```

- If the channel's Local URI is set to 'Use Internal Data' then the **User | SIP | SIP Name** will be used for the User part of the identity, and the ITSP Domain for the host part.

  ```
  From: "SipDisplayNameAlice" <sip: SipName@ITSP_Domain>;tag=8a9fed65b
  ```

- If the SIP Name field also contains a domain (indicated by the presence of @) then that domain will be used.

  ```
  From: "SipDisplayNameAlice" <sip: SipName@USER_Domain>;tag=8a9fed65b
  ```

- If Call-ID is blocked either by short code or if the **User | SIP | Anonymous** checkbox is checked then the From: header will be anonymous, unless the **SIP Line | Send From in Clear** checkbox is checked.

  ```
  From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=8a9fed65b
  ```

- If the channel's **Local URI** is set to **Use Credentials …** then there must first be at least one set of SIP Credentials defined, and that account selected in the channel's **Registration** dropdown selection box. The corresponding field from the **SIP Line | SIP Credentials** tab will be used for the User part of the identity.

  ```
  From: "Line17Cred2" <sip:Line17Cred2@ITSP_Domain>;tag=8a9fed65b
  ```

- The contact identity is populated similarly to the **From:** header. If Call-Id blocking is invoked: via **W** in a short code, or by checking the **User | SIP | Anonymous** checkbox then the **Contact:** field becomes semi-anonymous:

```
Contact: <sip:anonymous@135.55.86.70:5060;transport=udp
```

Related Links

Outgoing call message details on page 711

To field content

Since the identity of the called party is not known at the time of the initial INVITE, the **To:** field shows only the information necessary to route the call, which is the dialed digits after any short code and ARS manipulation, prefix manipulation, and removal of any end-of-dial digits (# in North America).

```
To: <sip: 12125551234@ITSP_Domain>
```

Related Links

Outgoing call message details on page 711

Contact field content

The contact identity is populated similarly to the **From:** header. If Call-Id blocking is invoked: via **W** in a short code, or by checking the **User | SIP | Anonymous** checkbox then the **Contact:** field becomes semi-anonymous:

```
Contact: <sip:anonymous@135.55.86.70:5060;transport=udp
```

Related Links

Outgoing call message details on page 711

P-Asserted Identity field content

Without Call-Id blocking, this field essentially mirrors the **From:** field.

P-Asserted-Identity: " SipDisplayName " <sip: SipName@ITSP_Domain>

Note:

You can enter the wildcard character “*”. Entering this value populates the SIP PAI header with the caller information available to IP Office.

Call-Id blocking: using **W** in a short code, or by checking the **User | SIP | Anonymous** checkbox results in the **P-Asserted** field being the only header that carries the calling party information, and so is unchanged from the non-blocked case above.

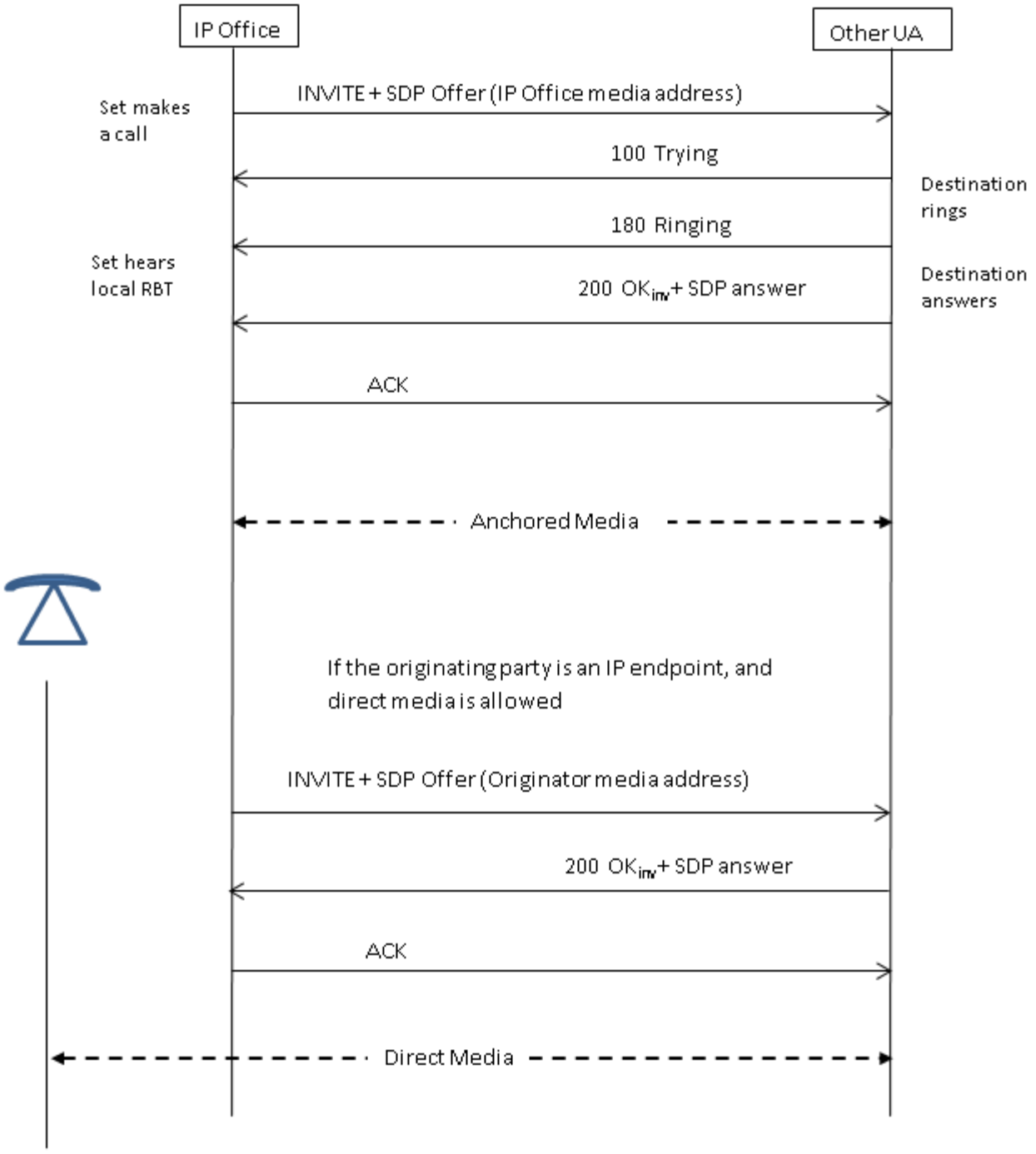
```
P-Asserted-Identity: " SipDisplayName" <sip:SipName@ITSP_Domain>
```

Related Links

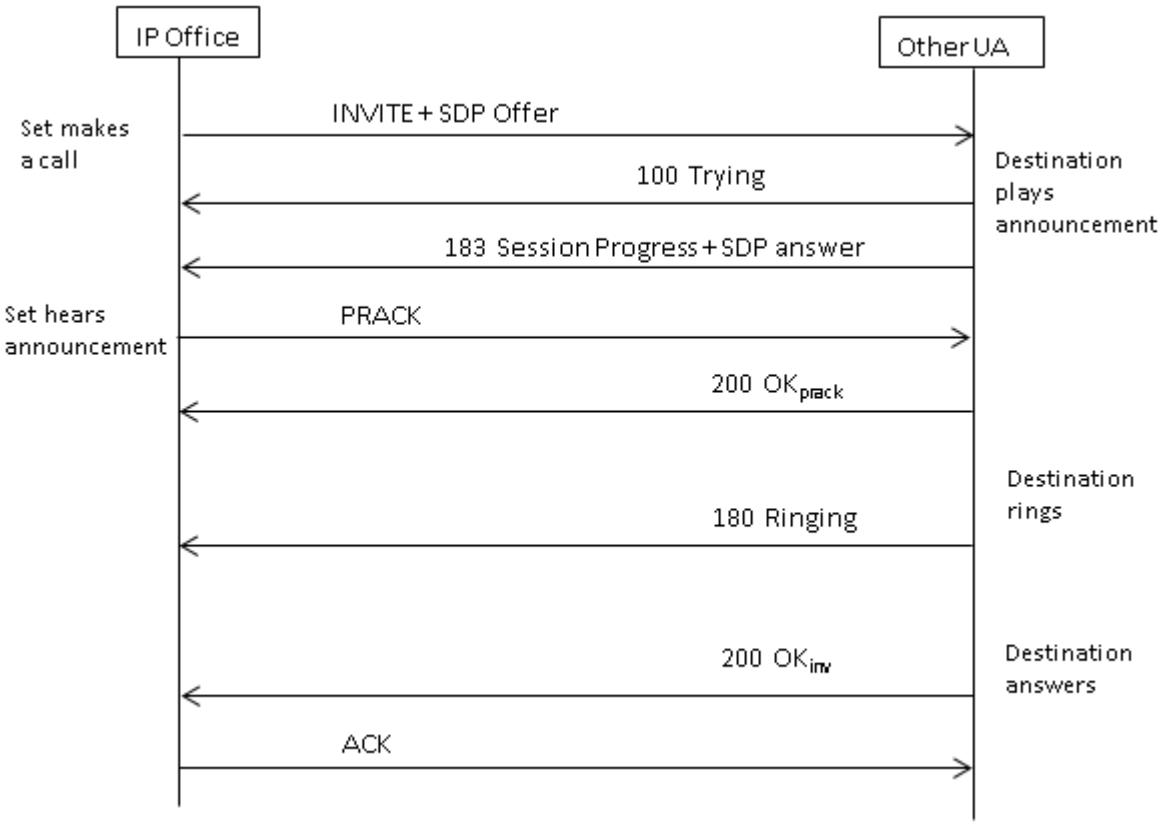
Outgoing call message details on page 711

Typical outgoing call scenarios

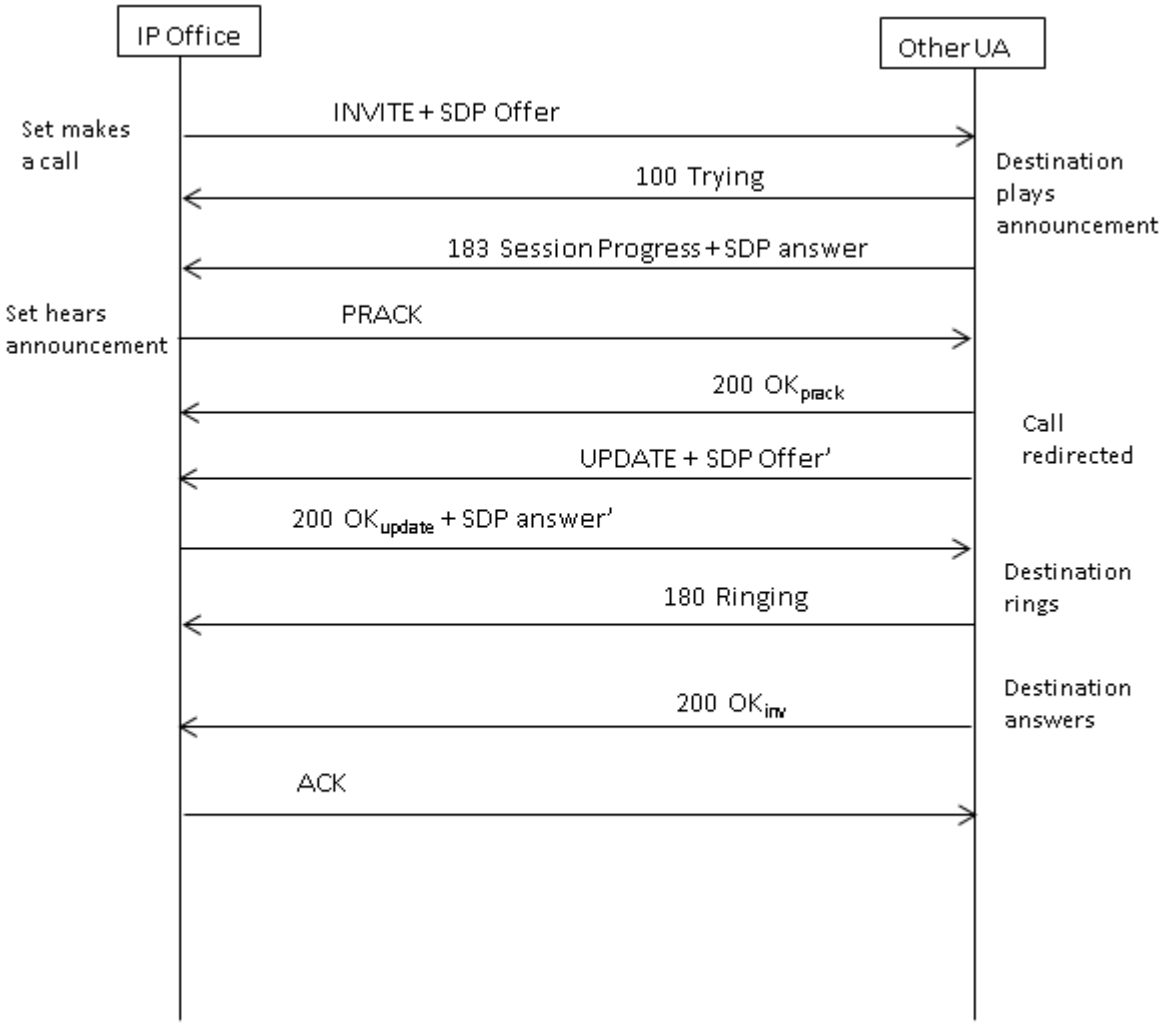
INVITE with SDP, local ringback



INVITE with SDP, early media



INVITE with SDP, early media re-directed by destination



Related Links

Outgoing call message details on page 711

Incoming call message details

Related Links

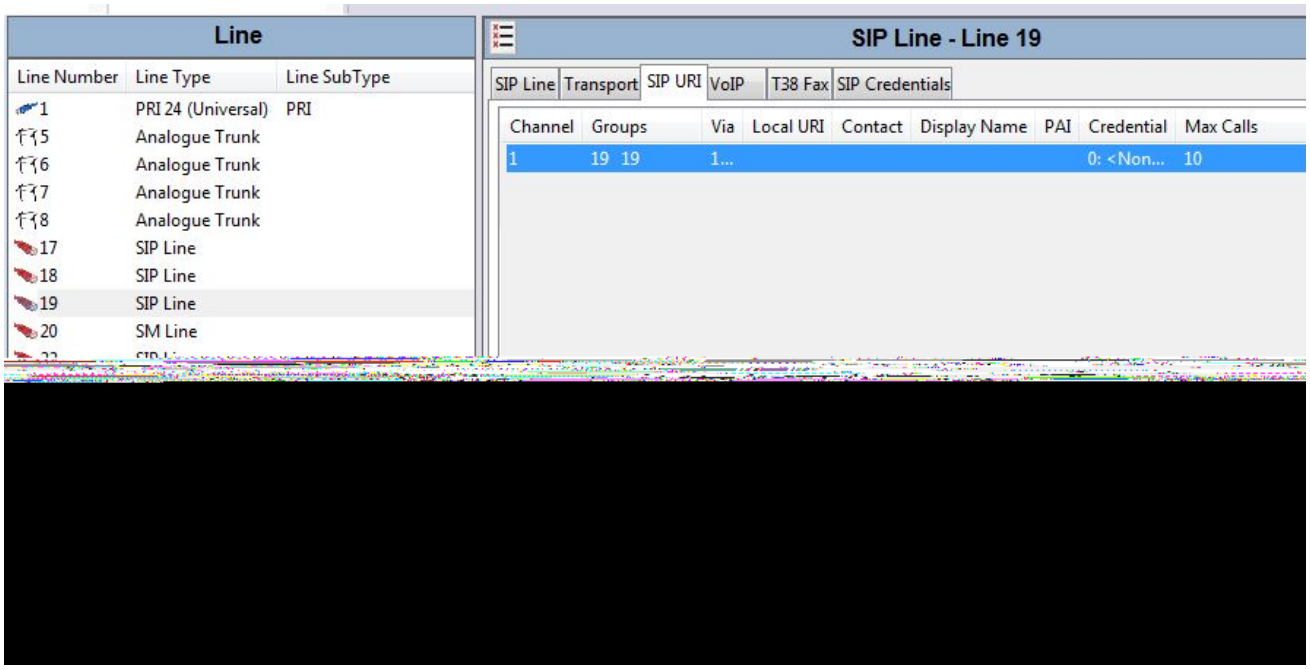
SIP messaging on page 711
Incoming call routing on page 716
Media path connection on page 717
Typical incoming call scenarios on page 718

Incoming call routing

When a SIP INVITE is received by IP Office, its origin is compared to the known IP addresses of the SIP lines configured. If a match is not found, then the INVITE is presented internally to the set

interface to determine if it matches any of the registered terminals. SIP messages from unknown endpoints are discarded, and solicit no response from IP Office.

SIP lines have incoming and outgoing groups associated with them, which are configured on the **SIP line | SIP URI** tab. In the example below, the incoming and outgoing groups are both 19, and the **Local URI** specifies **Use Internal Data**. With this **Local URI** setting, to route a call to a user, the **User | SIP | SIP Name** field is used to match against the incoming digits.



The incoming group indicates the identity of an **Incoming Call Route**, which is used to match the incoming digits in the Request-URI to a target. That target could be a set, a hunt group, another trunk, or an ARS entry.

Due to this grouping, calls incoming to several different trunks or trunk types can use the same **Incoming Call Route**, but in order for this to work,the **Local URI** must be manually set to <*>.

Incoming Call Routes are identified by the **Line Group ID** or optionally, an **Incoming Number** may be specified to match against in the received digits. Then a **Destination** specified, which may be a specific target, or may contain only a <.> to indicate that the digits are to be matched against known system targets.

Related Links

Incoming call message details on page 716

Media path connection

IP Office does not provide in-band ringback to incoming SIP trunk calls. This is different from what is done for H.323. The only scenario in which an incoming SIP trunk call will hear in-band ringback occurs when the call terminates on an analog trunk. With analog trunks, the media path is cut through immediately because IP Office has no way of determining the state (ringing, busy, answered) of the trunk.

IP Office connects “early” media before the call is answered by sending a 183 Session Progress response only if the following two conditions are met:

- A PROGRESS (in-band tone indication OR 183 Session Progress with SDP) message is received from the destination (this can only happen in a SIP-to-PRI or SIP-to-SIP tandem scenario).
- The INVITE message contains SDP.

IP Office does not attempt to connect early media on PROGRESS when there is no SDP in the initial INVITE, since this is unlikely to succeed. The reason there is no SDP in INVITE is probably that the originating system does not know the originator’s media address yet. A typical scenario where this is the case occurs when the call on the originating system comes from an H.323 SlowStart trunk.

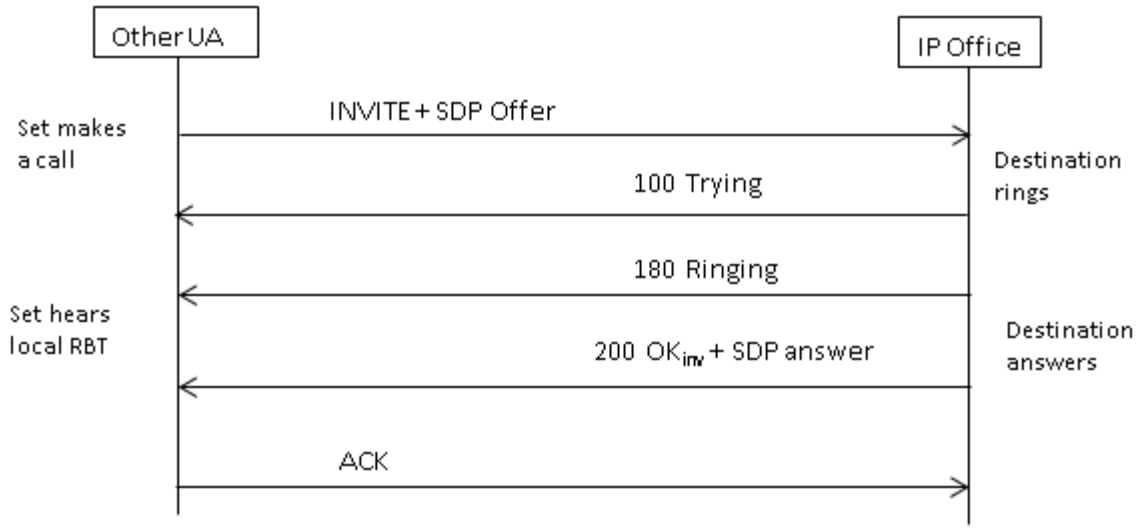
Related Links

Incoming call message details on page 716

Typical incoming call scenarios

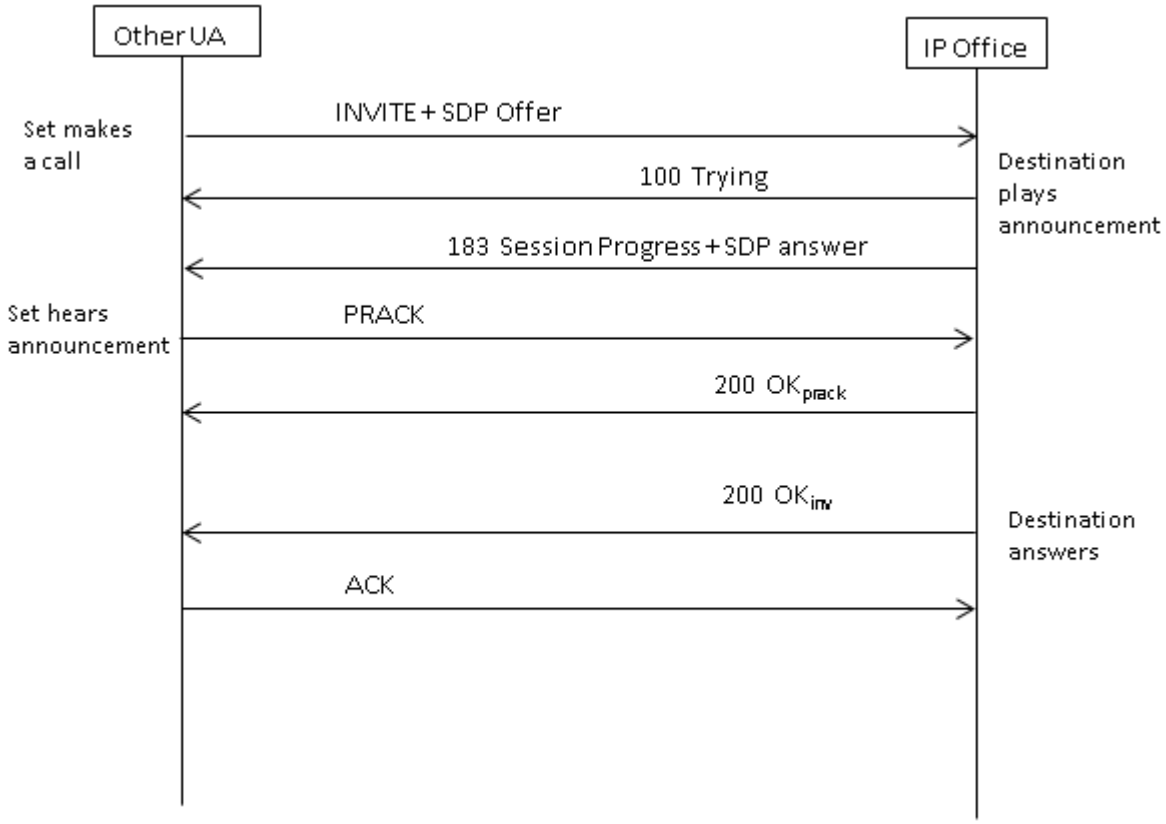
INVITE with SDP, local ringback

If the destination is an analog trunk, the 180 Ringing will be replaced with a 183 Progress with SDP followed immediately by a “fake” answer in order that the media will be connected right away so that the originator hears whatever in-band tones are present on the analog trunk (ringback or busy). If the target is a set that is unconditionally call forwarded over an analog trunk, then there will be a 180 Ringing without SDP, followed immediately by the “fake” answer.



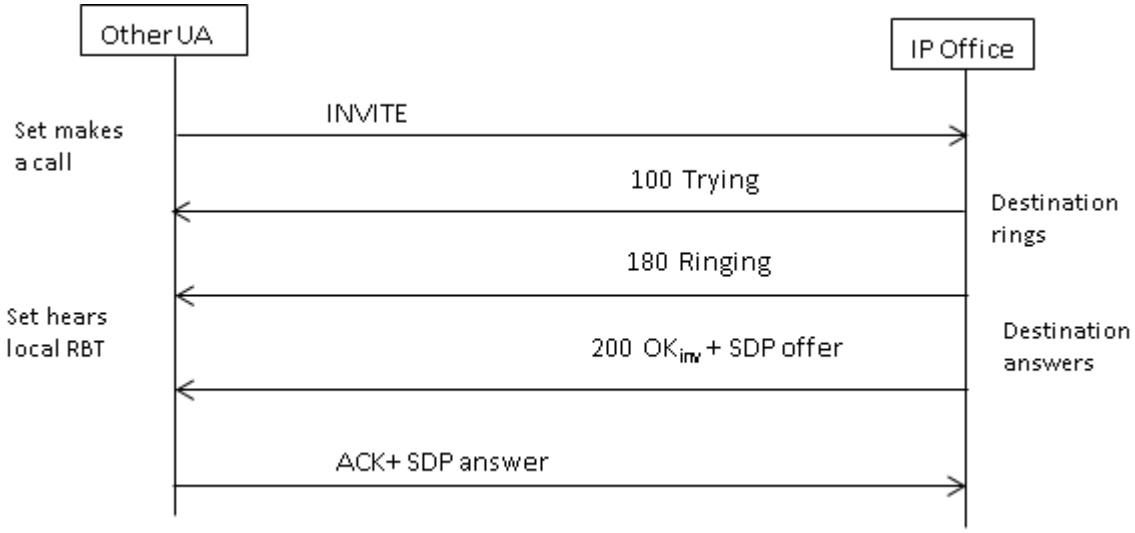
INVITE with SDP, early media

If the SIP Trunk receives a FAR_PROGRESS (in-band) message from its peer in the core (e.g. from a tandem PRI or SIP trunk), it sends a 183 Session Progress message with SDP to the far end. IP Office will connect the media on receipt of 180 or 183 with SDP.



INVITE without SDP, local ring back

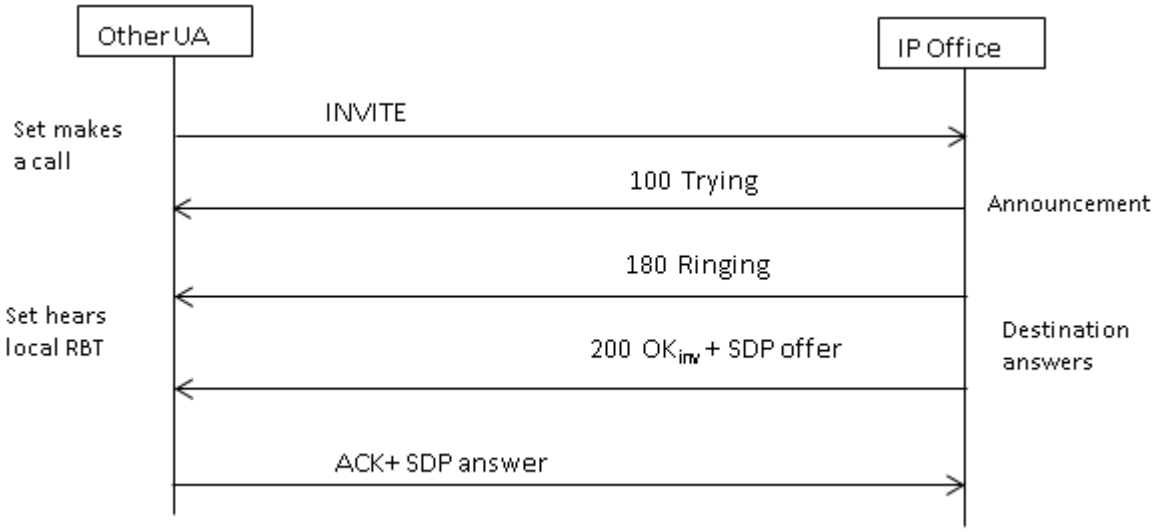
IP Office does not attempt to send early media in this scenario.



INVITE without SDP, early media

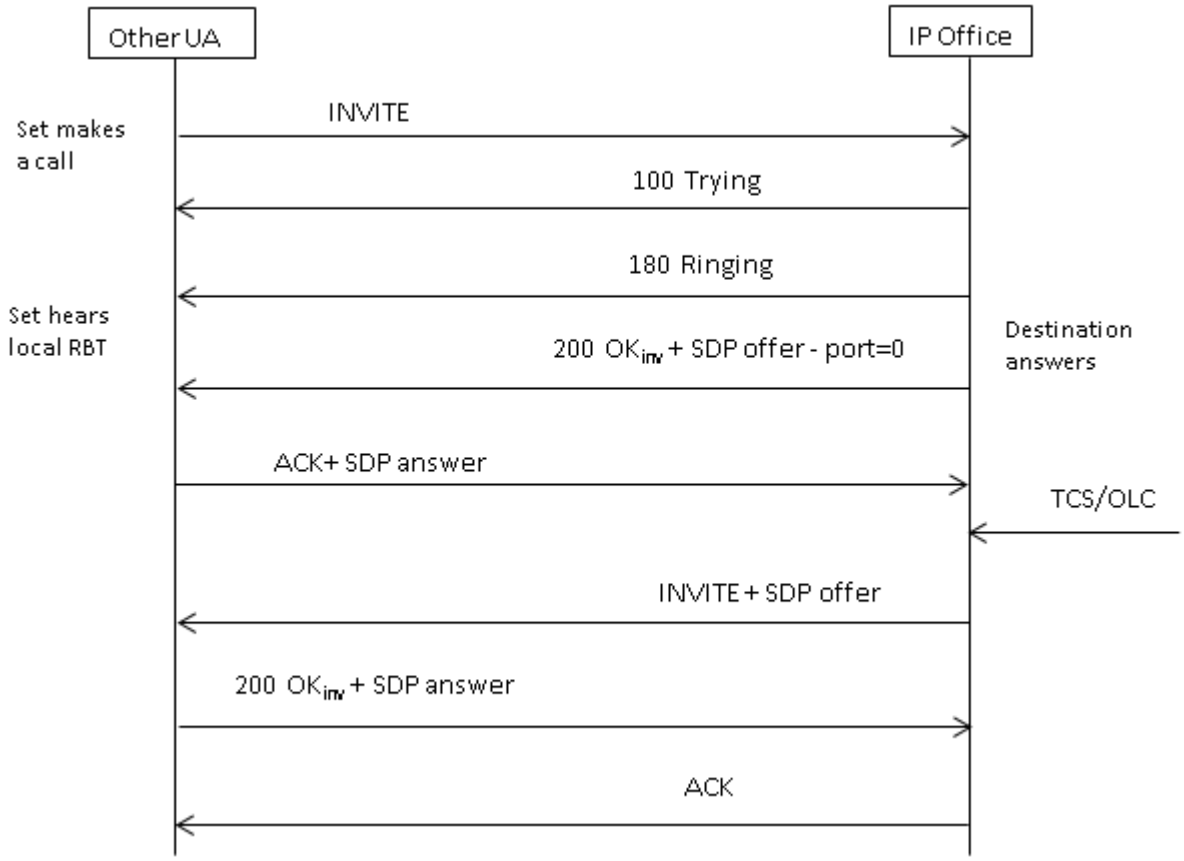
In this scenario, the far end attempts to connect media before the call is answered. IP Office does not provide early media when receiving an empty INVITE, but rather 180 Ringing instead. There is

no requirement to provide an SDP in the 180 Ringing provisional response, as that response is not sent reliably using the PRACK mechanism.



INVITE without SDP, call terminates on H.323 endpoint

If the destination of the call is an H.323 trunk, the destination media address is not known when the call is answered. Therefore, the SDP offer in 200 OK will contain a null port number (and IP address). Once the logical channels are opened on the H.323 side, IP Office sends a re-INVITE using the real media address.



Related Links

Incoming call message details on page 716

Codec selection

Codec selection is based on the Offer/Answer model specified in RFC 3264. The endpoint that issues the offer includes the list of codecs that it supports. IP Office offers the codecs set on the **SIP line | VoIP** tab, not those that are set on the extension.

The other endpoint sends an answer that should normally contain a single codec. If there are multiple codecs in the answer, IP Office only considers the first codec. If the SIP Line is configured to do Codec Lockdown (Re-Invite Supported is a prerequisite) then it will send another INVITE with the single chosen codec.

Related Links

SIP messaging on page 711

DTMF transmission

DTMF over RTP (RFC 2833) can be used in IP Office. Asymmetric dynamic payload negotiation is supported when it is necessary to bridge multiple SIP endpoints that do not support payload negotiation. The value used for an initial offer is configured on the **System | Codecs** tab. The default value is 101. Upon receipt of an offer with an RFC2833 payload type, IP Office will automatically use the proposed value rather than its own configured value. This helps to support networks that do not negotiate payload types.

There are cases in which direct media is desirable between SIP trunks and endpoints that do not support RFC2833. To allow for this, if key presses are indicated from the set, the IP Office will 'shuffle' the media in. This connects its own media engine to the endpoint and to the SIP trunk, and injects the digits in-band using the negotiated dynamic payload. After fifteen seconds of no key presses, the media will be shuffled back out to re-establish a direct connection again.

Related Links

SIP messaging on page 711

Fax over SIP

T.38 Fax over SIP is supported on the IP500 v2 platform deployed as standalone or as an expansion gateway. G.711 fax is also supported, and is supported on Linux servers. For networks that do or do not support T.38, IP Office allows both G3 and Super G3 fax machines to interoperate.

There are configuration parameters that control the behavior in different networks. If T.38 is supported in a network, then it may make sense to select T.38 as the Fax Transport preference in order to make use the inherent quality provided by the redundancy mechanisms. On the other hand, if all of the fax machines in the network are Super G3 capable, there may be a need to take advantage of the increased speed that this encoding provides. Since T.38 is not capable of encoding Super G3, G.711 may be a better choice for the Fax Transport. In either case, IP Office will accept codec change requests from the far SIP endpoint to switch to T.38 or to G.711.

T.38 Fax Transport and Direct Media are mutually exclusive on a given SIP Line. IP Office keeps itself in the media path so that it can detect fax tones to make the switch to T.38.

Related Links

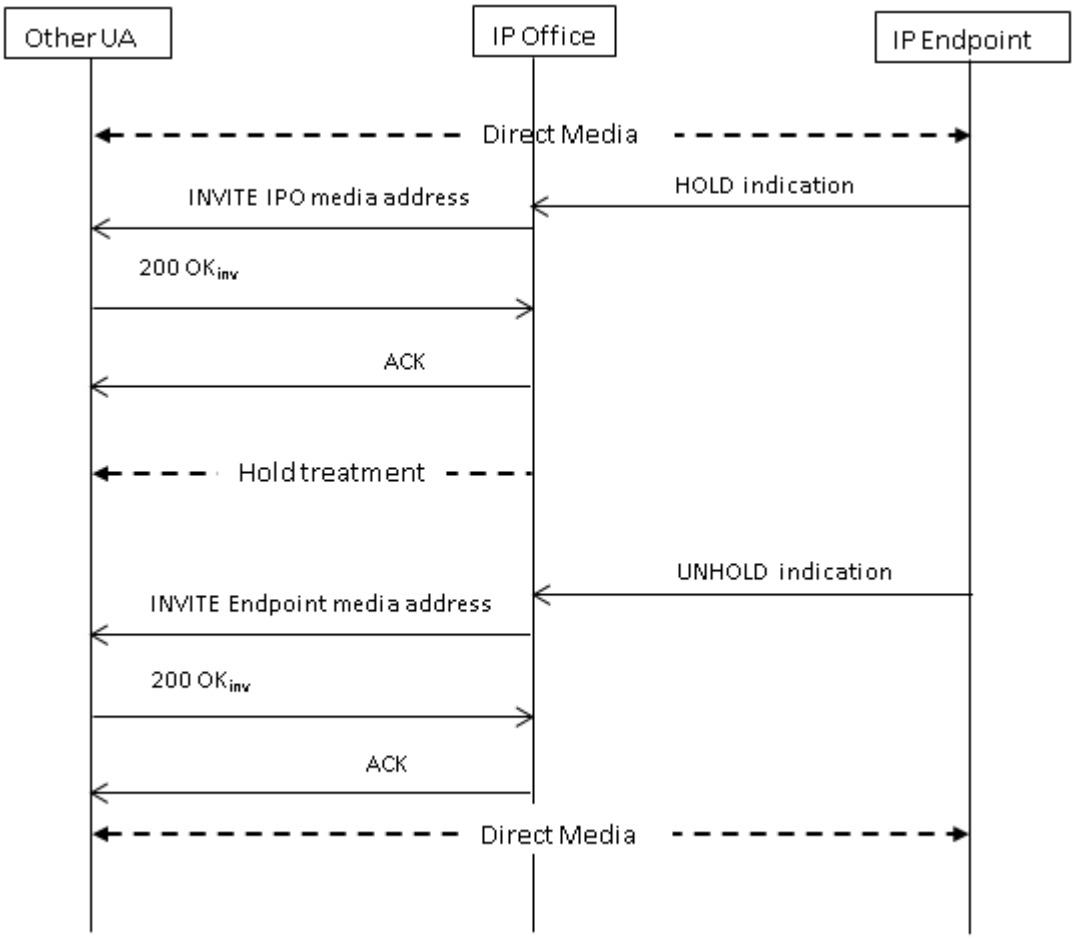
SIP messaging on page 711

Hold scenarios

Hold originated by IP Office

When an IP Office DS set or non-IP trunk puts a SIP trunk on hold, there is no indication to the network. The voice path is merely switched in the TDM domain to the appropriate hold treatment source, be it tones, silence or music. For IP sets and trunks, be they H.323 or SIP, if the call uses direct media, there will be a re-INVITE sent to redirect the media source from the set or trunk

endpoint to a port on the IP Office in order to connect hold treatment. When the call is then unheld, another INVITE will go out to connect the set with the far end.



Hold originated by far end

The far end of a SIP trunk can put the IP Office on hold by sending it re-INVITE with an SDP Offer containing:

- A **sendonly** attribute. IP Office replies with an SDP Answer containing the **recvonly**attribute.
- An "**inactive**" attribute. IP Office replies with **inactive**.
- A zero media connection address (c=0.0.0.0). IP Office replies with **inactive**.

Unhold

A held call is unheld by means of an SDP Offer with the **sendrecv** attribute (or no direction attribute, since **sendrecv** is assumed if not specified).

Unhold from mutual hold

Either end can un-hold the other end, i.e., allow it to transmit again, by sending a new Offer with the **sendrecv** or **recvonly**attribute. The other end replies with **sendonly** if the call is still on hold at its end.

Related Links

SIP messaging on page 711

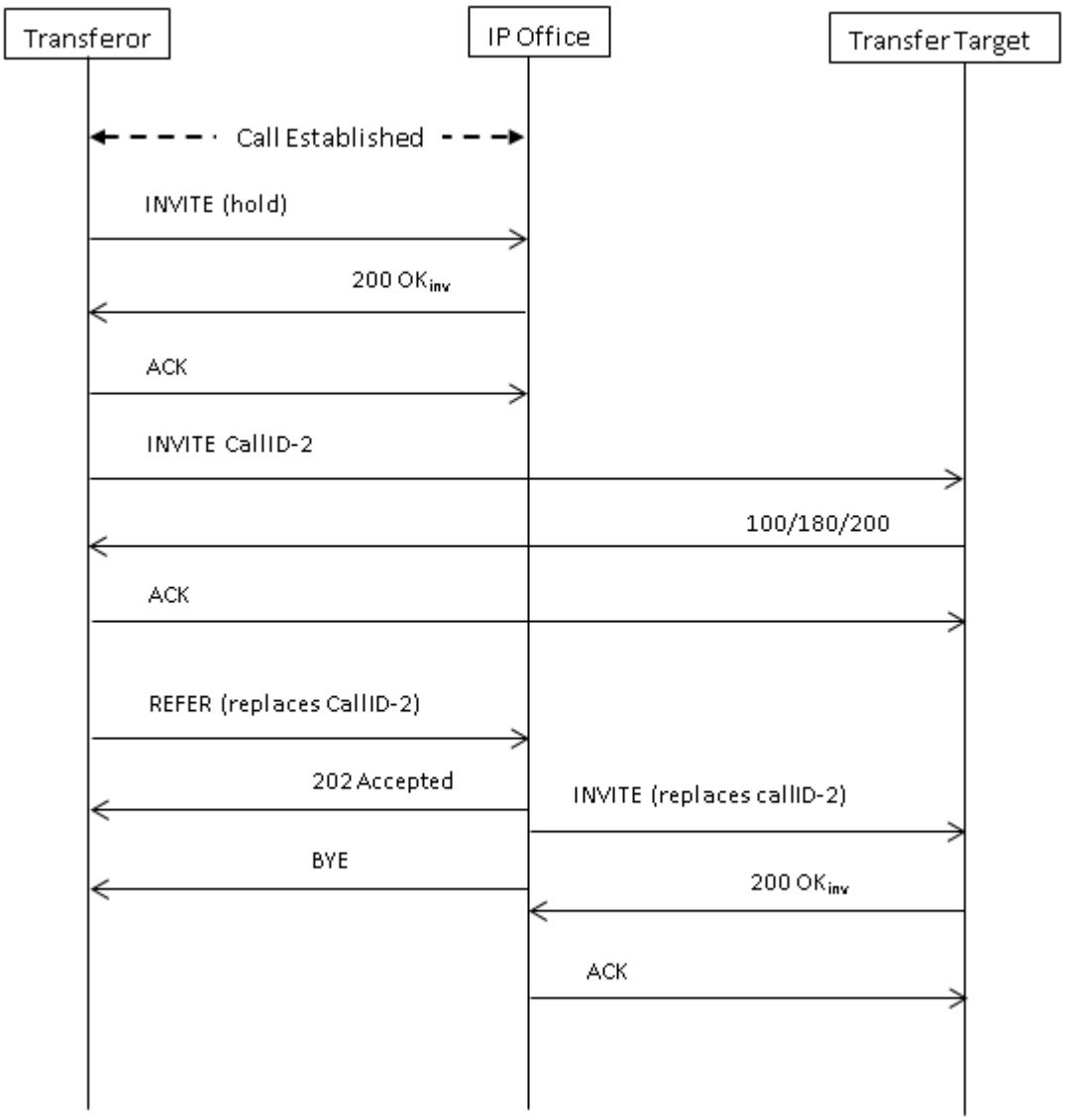
SIP REFER

After a SIP call has been established between two parties (the “Primary call), the SIP REFER method is used by the **TransferOR** end of the call to transfer the **TransferEE** end to a **Transfer Target**. The REFER message provides the Transfer Target’s contact information in the Refer-To header. This causes the TransferEE to establish the Secondary call to the Transfer Target, thus completing the transfer.

For public SIP trunks, IP Office supports only consultative call transfer using REFER. Consultative transfer is also known as Attended. With consultative transfer, the TransferOR puts the Primary call on hold and establishes a **Consult** call to another party. After the consultation, the TransferOR completes the transfer, causing the TransferEE to connect to the Transfer Target, thereby replacing the Transfer Target’s call with the TransferOR.

REFER can be configured to accept incoming, reject incoming, or decide based on the presence of REFER in the **Allow:** header in responses to OPTIONS messages. Similarly, there is the same configuration for outgoing REFER.

Although the TransferOR and TransferEE must be SIP endpoints, the Transfer Target may be a TDM, PRI, H.323 or SIP terminal on the same IP Office, or an endpoint reachable over the same SIP line as the REFER request is received from.



Related Links

SIP messaging on page 711

IP Office SIP trunk specifications

This section outlines the SIP trunk capabilities supported by IP Office.

Related Links

Configuring SIP Trunks on page 705
RFCs on page 726
Transport protocols on page 727

Request methods on page 727
Response methods on page 727
Headers on page 728

RFCs

- ITU-T T.38 Annex D, Procedures for real-time Group 3 facsimile communication over IP networks
- RFC 1889 - RTP: A Transport Protocol for Real-Time Applications
- RFC 2327 - SDP: Session Description Protocol
- RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication
- RFC 2833/RFC 4733 - RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 2976 - The SIP INFO Method
- RFC 3087 - Control of Service Context using SIP Request-URI
- RFC 3261 - Session Initiation Protocol
- RFC 3262 - Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3263 - Session Initiation Protocol (SIP): Locating SIP Servers
- RFC 3264 - An Offer/Answer Model with the Session Description Protocol (SDP)
- RFC 3311 - The Session Initiation Protocol (SIP) UPDATE Method
- RFC 3323 - A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3325 - Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted
- RFC 3326 - The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3398 - Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping
- RFC 3407 - Session Description Protocol (SDP) Simple Capability
- RFC 3515 – The Session Initiation Protocol (SIP) Refer method
- RFC 3550 - RTP: A Transport Protocol for Real-Time Applications
- RFC 3551 - RTP Profile for Audio and Video Conferences with Minimal Control
- RFC 3665 - Session Initiation Protocol Basic Call Flow Examples
- RFC 3666 - Session Initiation Protocol PSTN Call Flows
- RFC 3725 - Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)
- RFC 3824 - Using E.164 numbers with the Session Initiation Protocol (SIP)
- RFC 3842 - A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol
- RFC 3891 - The Session Initiation Protocol (SIP) "Replaces" Header
- RFC 3960 - Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
- RFC 4028 - Session Timers in the Session Initiation Protocol (SIP)
- RFC 4566 - SDP: Session Description Protocol
- RFC 5359 - Session Initiation Protocol Service Examples
- RFC 5379 - Guidelines for Using the Privacy Mechanism for SIP
- RFC 5806 - Diversion Indication in SIP
- RFC 5876 - Updates to Asserted Identity in the Session Initiation Protocol (SIP)
- RFC 6337 - Session Initiation Protocol (SIP) Usage of the Offer/Answer Model

- RFC 3489 - STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 6432 - Carrying Q.850 Codes in Reason Header Fields in SIP (Session Initiation Protocol) Responses

Related Links

IP Office SIP trunk specifications on page 725

Transport protocols

- UDP
- TCP
- RTP
- RTCP

Related Links

IP Office SIP trunk specifications on page 725

Request methods

- INVITE
- ACK
- BYE
- CANCEL
- INFO
- REFER
- REGISTER
- SUBSCRIBE
- NOTIFY
- PRACK
- OPTIONS
- UPDATE
- PUBLISH
- MESSAGE
- PING

Related Links

IP Office SIP trunk specifications on page 725

Response methods

- 100 Trying
- 180 Ringing
- 181 Call Is Being Forwarded
- 182 Call Queued
- 183 Session progress
- 202 ACCEPTED
- 3XX
- 4XX
- 5XX
- 6XX

- 200 OK

Related Links

IP Office SIP trunk specifications on page 725

Headers

- Accept
- Alert-Info
- Allow
- Allow-Event
- Authorization
- Call-ID
- Contact
- Content-Length
- Content-Type
- CSeq
- Diversion
- From
- History-Info
- Max-Forwards
- P-Asserted-Identity
- P-Early-Media
- P-Preferred-Identity
- Privacy
- Proxy-Authenticate
- Proxy-Authorization
- Proxy-Require
- Require
- Remote-Party-ID
- Server
- Session-Timers
- Supported
- To
- User-Agent
- Via
- WWW-Authenticate

Related Links

IP Office SIP trunk specifications on page 725

Chapter 17: Configuring Small Community Networking

Systems linked by IP Office Line IP trunks can enable voice networking across those trunks to form a multi-site network. Within a multi-site network, the separate systems automatically learn each other's extension numbers and user names. This allows calls between systems and support for a range of internal call features, see Supported Small Community Network Features.

Capacity

The following are the supported capacity limits for a Small Community Network system.

Maximum Number of Systems	32
Maximum Number of Users	1000
Maximum H.323 Line Hops Between Systems	5
Star H.323 Line Layout	✓
Serial H.323 Line Layout	✓
Mesh H.323 Line Layout	✓

Configuration Summary

To set up a Small Community Network, the following are required:

A working IP Office Line trunk between the systems, that has been tested for correct voice and data traffic routing.

- The arrangement the IP Office Line trunks must meet the requirements detailed in Supported Small Community Network Layouts.
- Within a particular system, all SCN trunks should be on the same LAN interface.
- VCM channels are required in all systems.
- The extension, user and group numbering on each system must be unique.
- The user and group names on each system must be unique.
- We also recommend that all names and numbers (line, services, etc) on the separate systems are kept unique. This will reduce potential maintenance confusion.
- The **Outgoing Group ID** on the Small Community Network lines should be changed to a number other than the default **0**.
- All systems should use the same set of telephony timers, especially the **Default No Answer Time**.

- Only one system should have its **Voicemail Type** set to **Voicemail Pro/Lite**. All other systems must be set to either **Centralized Voicemail** or **Distributed Voicemail**. No other settings are supported.

Software Level Interoperation

Small Community Networks is supported between systems with the same major software level or one level of difference in major software level. For example between 9.1 and 9.0 (same major level) and between 8.0 and 9.0 (one major level of difference).

This option is intended mainly to allow the phased upgrading of sites within a Small Community Network. It is still recommended that all systems within a network are upgraded to the same level where possible. Within a Small Community Network including differing levels of software, the network features and capacity will be based on the lowest level of software within the network.

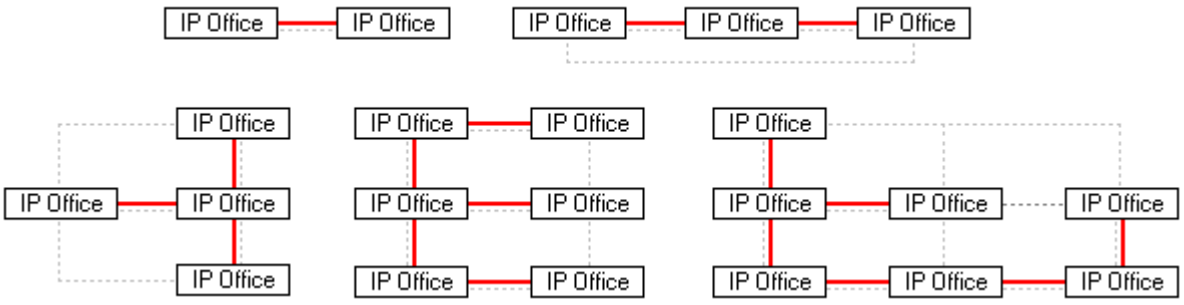
Related Links

Supported Small Community Network Network Layouts on page 730
Telephone Features Supported Across Server Edition and SCN Networks on page 123
Voicemail Support on page 733
Enabling Small Community Networking on page 733
Small Community Network Management on page 735
Small Community Network Remote Hotdesking on page 744
Small Community Network Fallback on page 745
SCN Short Code Programming on page 747

Supported Small Community Network Network Layouts

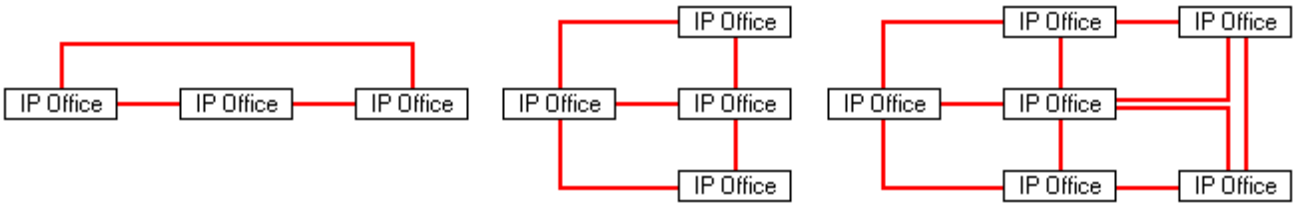
The allowed arrangement of IP Office Lines between the systems depends on the lowest software level of any system in the network. Note that we are referring to IP Office Lines configured in the system configurations. The actual IP network configuration, including IP routes in the system configurations, can differ as per the customer network requirements.

Star/Serial Layouts The following are examples of star and serial layouts.



---- = IP network, | = IP Office Line.

Mesh Layout A mesh layout is one where there is more than one possible IP Office Line route between any two systems. The following are examples of mesh layouts. Mesh, star and serial layouts can be combined.



Small Community Network Signalling Small Community Network uses a signalling similar to RIP is order to update each other of there presence. This traffic can be seen in the System Monitor application as AVRIP packets. This traffic is is sent to port 50795 on which each system listens.

Each system in the Small Community Network transmits an update every 30 seconds. Additionally BLF updates are transmitted when applicable up to a maximum of every 0.5 seconds. Typically the volume is less than 1Kbps per system.

Related Links

Configuring Small Community Networking on page 729

Telephone Features Supported Across Server Edition and SCN Networks

Each system running IP Office in a multi-site network acts as a self-contained IP Office telephone system. In addition to the remote systems sharing knowledge of user and hunt group extension numbers, the following additional telephony features are supported between systems in a multi-site network. Features not listed are not supported across the multi-site network.

Absence Text

Advertised Hunt Groups Hunt groups set to advertised can be dialed by users on other systems

Anti-tromboning Calls routed across the multi-site network and back to the originating system are turned back into internal calls on the originating system only.

Break Out Dialing

Call Park / Unpark Call

Call Pick-up Extension

Call Tagging

Callback When Free

Centralized Call Log

Centralized Personal Directory

Conference

Distributed Hunt Groups

Distributed Voicemail Server Support When using Vociemail Pro, each system can support its own Voicemail Pro server. See the Voicemail Pro Installation Manual.

Enable ARS / Disable ARS

Extension Dialing Each system automatically learns the user extension numbers available on other systems and routes calls to those numbers.

Fallback Server Edition Fallback SCN Fallback

Fax Relay

Follow Me Here / Follow Me To

Forwarding

Hold Held calls are signalled across the network.

Internal Twining

Intrusion Features

Mobile Call Control Licensed mobile call control users who remote hot desk to another system take their licensed status with them.

Music On Hold Source Selection

Relay On / Relay Off / Relay Pulse

Remote Hot Desking

Set Hunt Group Out of Service / Clear Hunt Group Out of Service

Transfer Calls can be transferred to network extensions.

User DSS/BLF Monitoring of user status only. The ability to use additional features such as call pickup via a USER button will differ depending on whether the monitored user is local or remote. Indication of new voicemail messages provided by SoftConsole user speed dial icon is not supported.

User Profile Resilence When a user hot desks to another system, they retain their Profile settings and rights.

Related Links

Working with the Server Edition Manager User Interface on page 92
Configuring Small Community Networking on page 729

Voicemail Support

Within a Small Community Network, a single Voicemail Pro can be used to provide voicemail services for all the systems. For full details of installation and setup refer to the Voicemail Pro documentation. The Voicemail Pro is licensed and hosted by a chosen central system and provides full operation for that system. The voicemail features supported for the other remote systems are listed below:

The use of additional Voicemail Pro servers is supported. The distributed severs provide call recording and auto attendant functions to their local system. The central Voice Pro server is still used as the message store for all messages. Refer to the Voicemail Pro documentation.

- **User mailboxes**.
- **Call recording.** Recording of incoming call routes is only supported for destinations on the same system, not for remote Small Community Network destinations.
- **Dial by Name**.
- **Auto Attendants**.
- **Breakout** Requires that the numbers used are routable by the system hosting the voicemail server.
- **Announcements**
- **UMS Web Services** Users for UMS Web Services (IMAP and or web voicemail) are licensed through the **UMS Web Services** license on their host system. This applies even if the user remote hot desks to another system in the Small Community Network.

Related Links

Configuring Small Community Networking on page 729

Enabling Small Community Networking

The process below adds an IP Office Line to the system configuration. It is assumed that data routing between the systems has already been configured and tested. Adding Small Community Network connections between systems can also be done using Manager's Small Community Network Management mode.

Related Links

Configuring Small Community Networking on page 729

Setup the VoIP Line from System A to System B

About this task

Receive the system configuration for System A. Prepare the system for addition to the Small Community Network:

Procedure

1. Change all extensions numbers and names to values that will be unique within the multi-site network.
   - For users and extensions this can be done using the **Extension Renumber** tool. That will adjust all users and extension and all items using those numbers, for example hunt group memberships and incoming call routes.
   - For hunt groups, each hunt group must be change individually.
2. Click **Line** to display a list of existing lines.
3. Right-click on the displayed list and select **New** and then **IP Office Line**.
4. Select the **Line** tab and set the following:
   - In the **Transport Type** field, select **Proprietary**.
   - In the **Networking Level** field, select **SCN**.
   - In the **Description** field, enter a description of the link. For example **System B Small Community Network**.
   - Set the **Outgoing Group ID** to a unique value. For example match the automatically assigned **Line Number** value.
5. Under **Gateway**, set the following:
   - For the **Gateway IP Address**, enter the IP address of the remote System B.
   - Use of **IP Office SCN - Fallback** is detailed in Small Community Network Fallback.
6. Click the **VoIP Settings** tab.
   -
   - Select the preferred **Compression Mode**. The same mode must be used by all VoIP lines and extensions within the network.
   - The other option can be configured as required but must be matched by the other IP Office Lines in the network. For example the Silence Suppression settings on all the network trunks must match.
7. Select **System | Voicemail**.
   a. Only one system should have its **Voicemail Type** set to **Voicemail Pro/Lite**.

      The **Voicemail IP Address** will be the IP address of the central voicemail server PC.

   b. Any other system with its own Voicemail Pro server PC should have its **Voicemail Type** set to **Distributed Voicemail**.

      The **Voicemail IP Address** should be the IP address of the distributed voicemail server PC. The **Voicemail Destination** should be set to the **Outgoing Group ID** used for the Small Community Network line to the system that is set as **Voicemail Pro/Lite**.

   c. All other systems should have their Voicemail Type set to Centralized Voicemail.

The **Voicemail Destination** should be set to the **Outgoing Group ID** used for the Small Community Network line to the system that is set as **Voicemail Pro/Lite**.

8. Save the configuration and reboot System A.

Next steps

Set up the IP Office Line from B to A.

Setup the VoIP Line from System B to System A

Procedure

1. On the remote system, repeat the previous steps to create an IP Office Line to System A. As stated above, where possible the line settings, especially the VoIP settings, must match those used for other IP Office Lines in the network.
2. Load the configuration and reboot the remote system.

Next steps

Test by making calls between extensions on the different systems

Small Community Network Management

Manager supports the ability to load and manage the configurations of the systems in a Small Community Network at the same time. Manager must be enabled for Small Community Network discovery.

When the configurations of the systems in a Small Community Network are loaded, Manager switched to Small Community Network management mode. This differs from normal system configuration mode in a number of ways:

- A network viewer is available. In addition to giving a graphical view of the Small Community Network, the view can be used to add and remove links between the systems in the Small Community Network.
- In the configuration tree, the records for users and hunt groups on all systems are grouped together.
- Time Profiles and User Right common to all systems are grouped together.
- The configuration settings for each system in the Small Community Network can be accessed and edited.

Related Links

Configuring Small Community Networking on page 729
Enabling SCN Discovery on page 736
Creating a Common Admin Account on page 736
Loading a Small Community Network Configuration on page 737

Editing a Small Community Network Configuration on page 738
Using the Network Viewer on page 739
System Inventory on page 744

Enabling SCN Discovery

About this task

In order for the **Select IP Office** menu to groups systems in a Small Community Network and allow loading of all the Small Community Network configurations, Manager must be enabled for SCN discovery.

Procedure

1. Select **File | Preferences**.
2. Select the **Discovery** tab.
3. Select the SCN Discovery option.
4. Check that the other discovery setting are sufficient to discover all the systems in the Small Community Network.
5. Click **OK**.

Related Links

Small Community Network Management on page 735

Creating a Common Admin Account

About this task

When managing multiple systems, it may be useful to create a common user name and password on all the systems for configuration access. This tool can be used to create a new service user account, **SCN_Admin**, for configuration access.

This process requires you to have a user name and password for security configuration access to each of the systems.

Select **Tools | SCN Service User Management**.

The option is not shown if a Basic Mode system configuration is loaded. If no configuration is loaded, and the option is not shown, select **View | Advanced View**.

Procedure

1. The **Select IP Office** menu displays the list of discovered systems.
2. Select the systems for which you want to create a common configuration account.

   Click **OK**.
3. A user name and password for security configuration access to each system is requested.

Enter the values and click **OK**. If the same values can be used for all systems enter those values, select **Use above credentials for all remaining, selected IPOs**. If each system requires a different security user names and password, deselect **Use above credentials for all remaining, selected IPOs**.

4. The systems will be listed and whether they already have an **SCN_Admin** account is shown.
5. To create the **SCN_Admin** account on each system and set the password for those account click on **Create Service User**.
6. Enter the common password and click **OK**.
7. The password can be changed in future using the Change Password option.
8. Click **Close**.

Related Links

Small Community Network Management on page 735

Loading a Small Community Network Configuration

About this task

If Manager is configured with SCN Discovery enabled, the **Select IP Office** menu will display any SCNs it discovers.

Procedure

1. With no configuration loaded, click on  or select **File | Open Configuration**.
2. The **Select IP Office** menu is displayed.

   Any systems in a Small Community Network will be grouped together.
3. To load the configuration of all the systems in the network, click the check box next to the network name and then click **OK**.

   If a  warning icon is displayed next to the **SCN** check box, it indicates that not all the systems known to be in the Small Community Network were discovered. Hovering the cursor over the icon will display details of the missing systems. Loading the network configuration at this time would not include the configuration of the missing system or systems. The missing systems:

   - May be disconnected
   - The discovery settings for the Manager PC may be incorrect.
   - The data routing between the Manager PC and the missing systems may be incorrect or blocked.
4. Enter the name and password for configuration access to each system.

   If the systems all have a common user name and password (see Common Administrator Access below), select **Use above credentials for all remaining selected IPOs**. Click **OK**.

5. Manager will load and display the combined configurations in Small Community Network Management mode.

Related Links

Small Community Network Management on page 735

Editing a Small Community Network Configuration

When the configuration of a Small Community Network is loaded, Manager displays the configuration in a different way from when the configuration of a single system is loaded. The main differences are in how configuration records are grouped in the configuration tree.

Clicking on the  Small Community Network icon displays the Network Viewer which shows the lines between the systems in the Small Community Network.

Small Community Network Configuration Records Certain records from each of the systems in the Small Community Network are grouped together in the configuration tree differently from when just a single system configuration is loaded. There are two types, unique Small Community Network records and shared Small Community Network records:

Unique Records They can be edited here and the system to which they belong is indicated in the group pane and in the title bar of the details pane. However, to add or delete these types of record must be done within the configuration records of the particular system that will host the entry's configuration details.

- All user in the Small Community Network are shown under the  **User** icon.
- All hunt groups in the Small Community Network are shown under the  **Hunt Group** icon.

Shared Records Shared records are configuration items that exist on all systems in the Small Community Network, having the same name and settings on each system. Editing the shared record updates the matching copy in the configuration of each system. Similarly, adding or deleting a shared record adds or deletes from the individual system configurations. If the copy of the shared record within an individual configuration is edited, it is no longer a shared record for the Small Community Network though the individual records on other system will remain. Changing the individual records back to matching will turn the records back into a shared record.

- Shared time profiles are shown under the  **Time Profile** icon.
- Shared user rights are shown under the  **User Rights** icon.

Individual System Configurations  The full configuration for each system in the Small Community Network can be accessed and edited as required. It is possible to copy and paste configuration records between systems using the configuration tree.

Saving Changes

When the save icon or **File | Save Configuration** is selected, the menu for multiple configuration saves is displayed. It provides similar options are for a normal single configuration save. Note that when working in Small Community NetworkManagement mode, after saving configuration changes the Manager will always close the displayed configuration.

Change Mode If Manager thinks the changes made to the configuration settings are mergeable, it will select **Merge** by default, otherwise it will select **Reboot**.

- **Merge** Send the configuration settings without rebooting the system. This mode should only be used with settings that are mergeable. Refer to Mergeable Settings.
- **Reboot** Send the configuration and then immediately reboot the system.
- **Reboot When Free** Send the configuration and reboot the system when there are no calls in progress. This mode can be combined with the **Call Barring** options.
- **Timed** The same as When Free but waits for a specific time after which it then wait for there to be no calls in progress. The time is specified by the **Reboot Time**. This mode can be combined with the **Call Barring** options.

Reboot Time This setting is used when the reboot mode **Timed** is selected. It sets the time for the system reboot. If the time is after midnight, the system's normal daily backup is canceled.

Call Barring These settings can be used when the reboot mode **Reboot When Free** is selected. They bar the sending or receiving of any new calls.

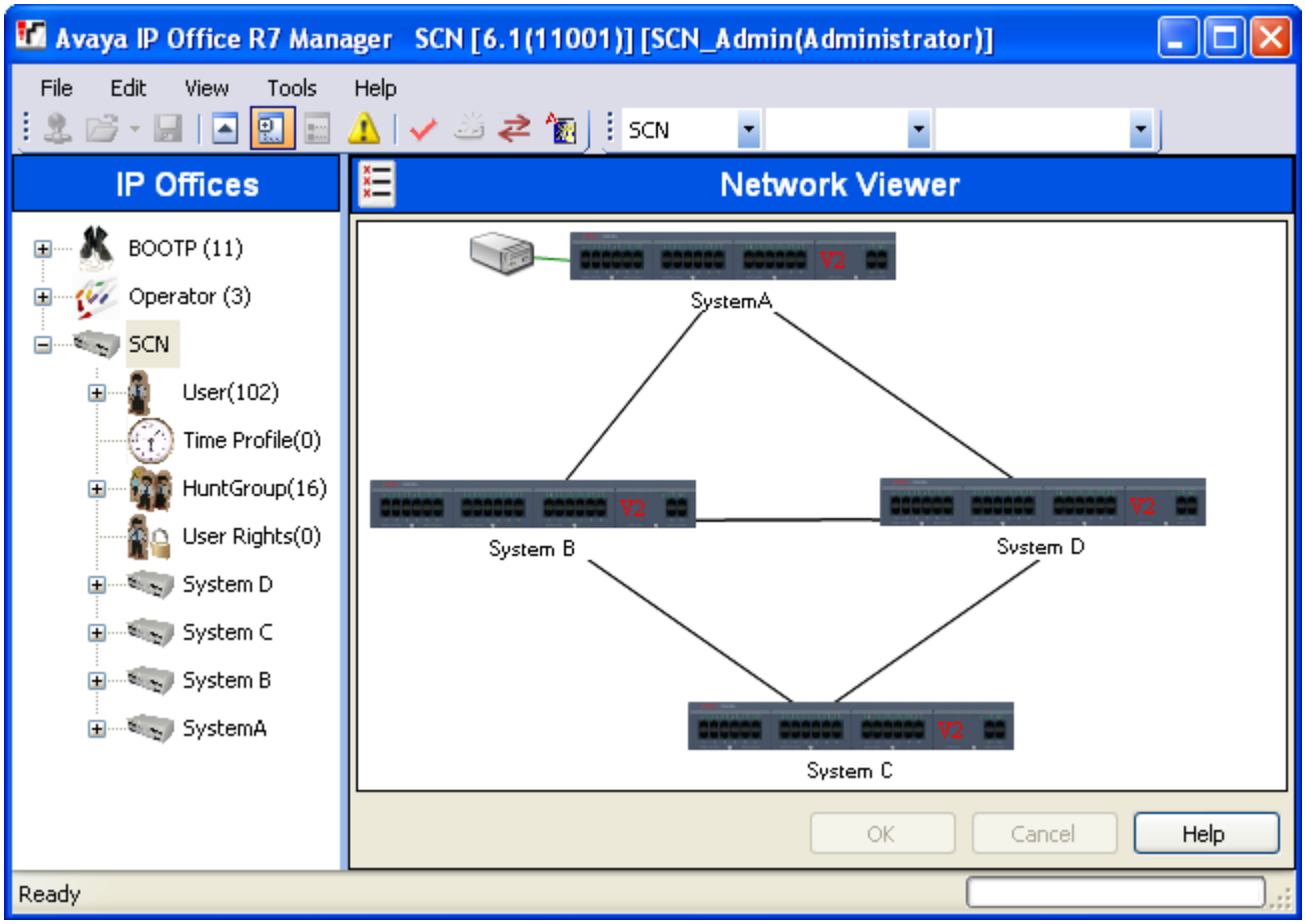
Error Status The warning will appear if the configuration being sent contains any validation errors indicated by a icon in the error pane. The configuration can still be sent if required.

Related Links

Small Community Network Management on page 735

Using the Network Viewer

Clicking on Small Community Network in the configuration tree displays the Network Viewer. This shows each of the systems in the Small Community Network and the links between each of the systems. Systems with attached Voicemail Pro servers are also indicated.



Green System with Voicemail Pro system.

Black Small Community Network line between two systems.

Red Incorrect Small Community Network line between systems (probably one-way connection). Right-click on the line and select **Repair**.

You can use the Network Viewer to perform a range of functions:

- Arrange the View
- Launch System Status
- Launch Voicemail Pro
- Add an IP Office Line
- Add a system
- Remove an IP Office Line
- Remove a system from the Small Community Network
- Repairing an IP Office Line
- Add a Background Image

Related Links

Small Community Network Management on page 735

Arranging the View

About this task
Procedure

You can click and drag items around in order to position them where required.

Alternatively if you right click on the view you can select Auto Arrange.

Note:

The position of elements in the network view are stored as part of the system configuration. Therefore changes to the view will require the configuration to be saved.

Adding a Line Within the Small Community Network

About this task

You can use the network viewer to add a Small Community Network link between two systems in the Small Community Network that are currently linked. This process will add new H.323 Small Community Network line records to the configurations of each of the systems.

Note:

Adding a line between systems will require those systems to reboot when the changes are saved.

Procedure

1. Right click on the starting system for the link.

   Select **Connect To** and select the name of the other system in the Small Community Network to which you want to link.

2. Select the type of line, **IP Office SCN** or **IP Office SCN-Fallback**.
3. Click **OK**.

   If Small Community Network-Fallback is selected, the actual backup function still need to be configured.

   a. The newly added line is displayed in the network viewer.

   b. Click **OK**.

Repairing a Line Within the Small Community Network

About this task

A red line in the network viewer indicates a incorrectly configured line between two systems in the Small Community Network. Typically this will be a line configured in one of the systems but not matched by a line configured in the other system. The network viewer can be used to correct this error.

Procedure

1. Note that adding a line between systems will require those systems to reboot when the changes are saved.
2. Right click on the red line and select **Repair Line**.
3. The line is changed to black.
4. Click **OK**.

Adding a System to the Small Community Network

About this task

You can use the network viewer to add a Small Community Network line to a system not yet in the Small Community Network. This process will add new H.323 Small Community Network line records to the configurations of each of the systems.

Procedure

1. Note that adding a line between systems will require those systems to reboot when the changes are saved.
2. Right click on the starting system for the link.

   Select **Connect To** and select **Discovery**.
3. The **Select IP Office** menu will display any discoverable systems not already in the Small Community Network.

   If the discovery includes systems already in another Small Community Network it will not indicate such. If you want to add such a system in order to join the SCNs you can do so. However after adding the system, you should immediately save the configuration and reload the Small Community Network.

   a. Select the required system and click **OK**.
   b. Enter the name and password for configuration access to the selected system and click **OK**.
   c. The newly added system is displayed in the network viewer.
   d. Click **OK**.

      The configuration of the newly added system is now included in the configuration tree.
   e. If the **Error List** is visible (**View | Error Pane**), check that none of the error are Small Community Network specific errors, for example duplicate names or extension numbers.

Removing a Small Community Network Line

About this task

You can use the network viewer to remove the Small Community Network lines between two systems in the Small Community Network.

Procedure

1. Note that removing a link between systems will require those systems to reboot when the changes are saved.
2. Right click on the link and select **Delete** Line.
3. The line is removed from the network viewer.
4. Click **OK**.

Removing a System

About this task

You can use the network viewer to remove a system from the Small Community Network.

Procedure

1. Note that removing a system will require previous linked systems to reboot when the changes are saved.
2. Right click on the system and select **Remove From Small Community Network**.
3. Any lines to other system in the Small Community Network are removed.
4. Click **OK**.

Start System Status

About this task

If the System Status Application is also installed on the Manager PC, you can start it for a particular system.

Procedure

1. Right click on the system and select **System Status**.
2. The application is started and the login form pre filled with the IP address of the system.

Start Voicemail Pro

About this task

If the Voicemail Pro client is also installed on the Manager PC, you can start it for the any system with an associated Voicemail Pro server.

Procedure

Right click on the voicemail server icon and select **Launch VMPro Client**.

Add a Background Image

About this task

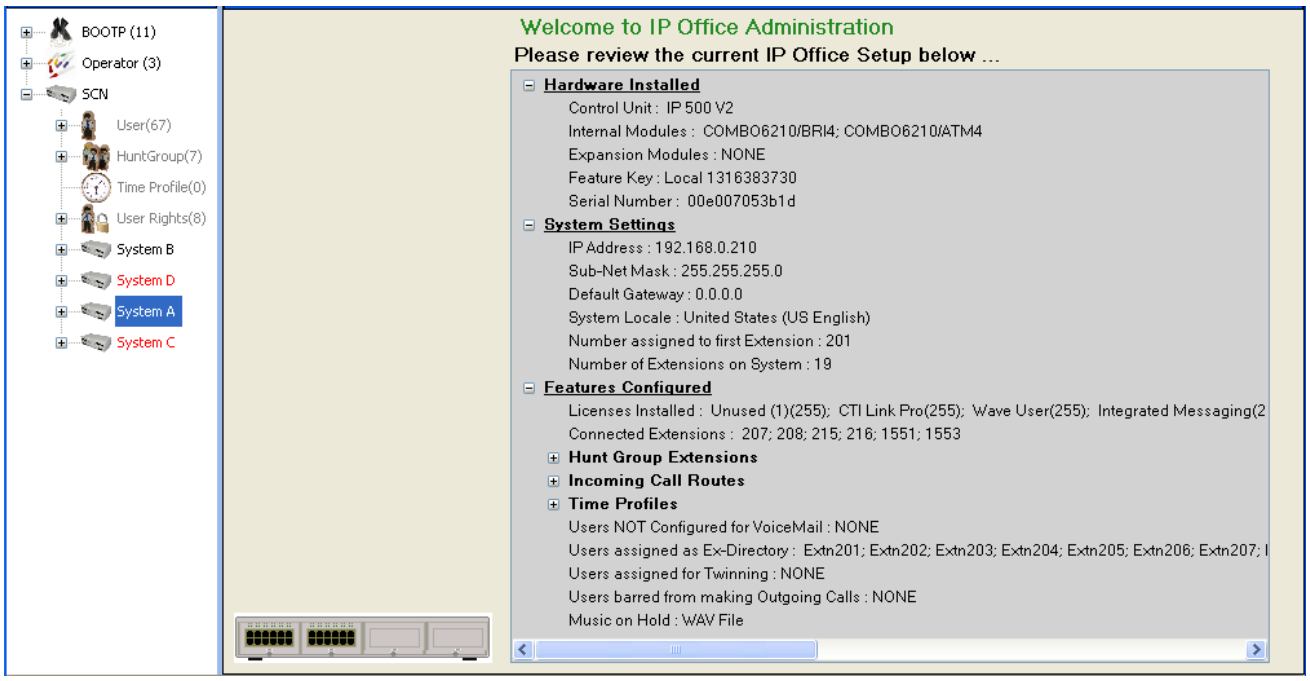
You can select an image file to be displayed in the background of the Network Viewer display. This file is not saved as part of the configuration in any way, ie. if the image file is moved or deleted it is not longer used by Manager.

Procedure

1. Right click on the general background area of the network viewer and select **Background Image**.
2. Select **Set Background Image** to browse to the location of the file to be used.
3. The Visible option can be used to switch the display of the background image on or off.

System Inventory

When working in Small Community Network Management mode, clicking on the **System** icon for a particular system displays a system inventory page for that system.



Related Links

Small Community Network Management on page 735

Small Community Network Remote Hotdesking

The system supports hot desking between systems within a network.

In the descriptions below, the system on which the user is configured is termed their 'home' system, all other systems are 'remote' systems.

When a user logs in to a remote system:

- The user's incoming calls are rerouted to that system.
- The user's outgoing calls uses the settings of the remote system.
- The user's license privileges move with them, for example their user profile setting is retained. The host system does not need to be licensed for the user.
- The user's own settings are transferred. However, some settings may become unusable or may operate differently.
- User rights are not transferred to the remote system but the name of any user rights associated with the user are transferred. If user rights with the same name exist on the remote system, then they will be used. The same applies for user rights applied by time profiles, if time profiles with the same name exist on the remote system .
- Appearance buttons configured for users on the home system will no longer operate.
- Various other settings may either no longer work or may work differently depending on the configuration of the remote system at which the user has logged in. For example: For T3 phones, the personal directory is not transferred with the user.
- The rights granted to the user by their **Profile** settings are retained by the user. There is no requirement for the remote system to have the appropriate licenses for the **Profile**.

If the user's home system is disconnected while the user is remotely hot desked, the user will remain remotely hot desked. They can remain in that state unless the current host system is restarted. They retain their license privileges as if they were on their home system. Note however that when the user's home system is reconnected, the user may be automatically logged back onto that system.

Break Out Dialing In some scenarios a hot desking user logged in at a remote system will want to dial a number using the system short codes of another system. This can be done using either short codes with the **Break Out** feature or a programmable button set to **Break Out**. This feature can be used by any user within the multi-site network but is of most use to remote hot deskers.

Related Links

Configuring Small Community Networking on page 729

Small Community Network Fallback

Each system in the Small Community Network can include one IP Office Line where the **SCN Backup Options** is set to **Supports Fallback**. The system to which the IP Office Line connects is then requested to provide fallback support for selected options for the local system.

- Note that both ends of the SCN trunk connection must be set to fallback.
- On the system requesting backup, the required **SCN Backup Options** are selected, indicating that it is requesting backup. A single system can only request backup from one other system.
- A system providing backup can provide backup for up to 7 other systems.

Important:

Fallback handover takes approximately 3 minutes. This ensure that fallback is not invoked when it is not required, for example when the local system is simply being rebooted to complete a non-mergeable configuration change.

Fallback is only intended to provide basic call functionality while the cause of fallback occurring is investigated and resolved. If users make changes to their settings while in fallback, for example changing their DND mode, those changes will not apply after fallback.

If the fallback system is rebooted while it is providing fallback services, the fallback services are lost.

Fallback features require that the IP devices local to each system are still able to route data to the fallback system when the local system is not available. This will typically require each system site to be using a separate data router from the system.

When an IP Phone re-registers to a secondary IP Office on the failure of the primary control unit, the second system will allow it to operate indefinitely as a “guest”, but only until the system resets. Licenses will never be consumed for a guest IP phone.

Remote hot desking users on H323 extensions are automatically logged out.

Fallback Options

Once a line is set to **Supports Fallback**, the following options are available:

Backs up my IP Phones: Default = On. This option is used for Avaya 1600, 4600, 5600 and 9600 Series phones registered with the system. When selected, it will share information about the registered phones and users on those phones with the other system.

- If the local system is no longer visible to the phones, the phones will reregister with the other system. The users who were currently on those phones will appear on the other system as if they had hot desked.
- When phones have registered with the other system, they will show an **R** on their display.

If using resilience backup to support Avaya IP phones, **Auto-create Extn** and **Auto-create User** should not be left enabled after initial configuration or any subsequent addition of new extensions and users. Leaving auto-create options enabled on a system that is a failover target may cause duplicate extension/user records on the multi-site network under multiple failure scenarios.

Backs up my Hunt Groups: Default = On. When selected, any hunt groups the local system is advertising to the network are advertised from the other system when fallback is required. The trigger for this occurring is Avaya H.323 phones registered with the local system registering with the other system, ie. **Backs up my IP Phones** above must also be enabled. In a Server Edition network this option is only available on the H.323 trunk from the Primary Server to the Secondary Server.

When used, the only hunt group members that will be available are as follows:

- If the group was a distributed hunt group, those members who were remote members on other systems still visible within the network.
- Any local members who have hot desked to another system still visible within the network.

When the local system becomes visible to the other system again, the groups will return to be advertised from the local system.

Backs up my Voicemail: Default = On. This option can be used if the local system is hosting the Voicemail Pro server being used by the network. If selected, when the local system is no longer visible to the voicemail server, the other system will act as host for the voicemail server. In a Server Edition network this option is only available on the H.323 trunk from the Primary Server to the Secondary Server. It is assumed as being on an is automatically set by the Resilience Administration tool.

Backs up my IP DECT phones: Default = On.

This option is only available when **Transport Type** is set to **Proprietary**.

This option is used for Avaya IP DECT phones registered with the system. When selected, it will share information about the registered phones and users on those phones with the other system.

If the local system is no longer visible to the phones, the phones will reregister with the other system. The users who were currently on those phones will appear on the other system as if they had hot desked. Note that when the local system is restored to the network, the phones will not automatically re-register with it. A phone reset via either a phone power cycle or using the System Status Application is required. When phones have registered with the other system, they will show an **R** on their display.

Related Links

Configuring Small Community Networking on page 729

SCN Short Code Programming

In a multi-site network, the systems automatically learn each others extension numbers and route calls appropriately. However the same does not apply to dialing of other numbers. Using short codes it is possible to have the dialing of numbers on one system to be redirected to another system and dialed there. The dialing is then matched against the short codes available on the remote system.

Scenario

We want a short code on System A which will correctly route any 3000 range number to System B. This will allow System B group numbers to be dialed from System A. To achieve the above scenario, we will add a new system short code. By using a system short code it becomes available to all users.

Example Short Code

In the configuration for System A.

1. Click **Short code**to display a list of existing system short codes.
2. Right-click on the displayed list and select **New**.
3. Enter the short code settings as follows:

- **Short Code**: 3XXX This will match any four-digit number beginning with 3.
- **Telephone Number**: . The . indicates that the short code should output the digits as dialed.

- **Line Group ID**: 99999 This should match the Outgoing Group ID given to the IP Office Line connected to System B.
- **Feature**: Dial

Click **OK**.

A similar system short code can be added to System B's configuration to route 2XXX dialing to System A.

Related Links

Configuring Small Community Networking on page 729

Chapter 18: Short Code Overview

The system uses short codes to match the number dialed to an action. The number dialed or part of the number dialed can be used as parameter for the feature.

This section provides an overview of short codes and information on configuration. For details on each short code, see *Avaya IP Office™ Platform Short Code and Button Action Reference*.

⚠ Warning:

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

The short method for describing short codes in this manual, for example **9N/Dial/./0**, indicates the settings of the following fields of a short code: **Code/Feature/Telephone Number/Line Group ID**. For a description of the individual fields see Short Code.

Examples The method of detailing a short codes settings lists the short code fields separated by a /.

***17/VoicemailCollect/?U** A user dialing ***17** is connected to voicemail.

***14*N#/FollowMeTo/N** If a user dials ***14*210#** at their own extension, their calls are redirected to extension 210.

Dialing Short Codes The following types of short code applied to on-switch dialing. The result may be an action to be performed by the system, a change to the user's settings or a number to be dialed. The order below is the order of priority in which they are used when applied to user dialing.

User Short Codes These are usable by the specific user only. User short codes are applied to numbers dialled by that user and to calls forwarded via the user.

User Rights Short Codes These are usable by any users associated with the user rights in which they are set. User Rights short codes are only applied to numbers dialed by that user. For example they are not applied to calls forwarded via the user.

System Short Codes These are available to all users on the system. They can be overridden by user or user rights short codes.

Post-Dialing Short Codes When any the short code above result in a number to be dialed, further short code can be applied to that number to be dialed. This is done using the following types of short codes.

ARS (Alternate Route Selection) Short Codes The short code that matches dialing can specify that the resulting number should be passed to an ARS form. The ARS form can specify which routes should be used for the call by using further short code matches and also provide option to use other ARS forms based on other factors such as time and availability of routes.

Transit Network Selection (TNS) Short Codes Used on T1 ISDN trunks set to use AT&T as the Provider. Applied to the digits presented following any other short code processing.

Incoming Number Short Codes On certain types of trunks short codes can be applied to the incoming digits received with calls.

Line Short Codes These short codes are used to translate incoming digits received with calls. The stage at which they are applied varies between different line types and may be overridden by an extension number match.

Related Links

Short Code Characters on page 750
User Dialing on page 753
Application Dialing on page 755
Secondary Dial Tone on page 756
? Short Codes on page 757
Short Code Matching Examples on page 758
Default System Short Code List on page 762

Short Code Characters

Each short code, regardless of its type, has the following fields:

- **Short Code**: Default =Blank. Range = Up to 31 characters. The digits which if matched trigger use of the short code. Characters can also be used to create short codes which cannot be dialed from a phone but can be dialed from application speed dials. However some characters have special meaning, see the table below.
- **Telephone Number**: Default = Blank. Range = Up to 32 characters. The number output by the short code. When necessary, this is used as parameter for the selected short code Feature. See the table below for the special characters that can be used here.
- **Line Group ID**: Default = 0 This field is used for short codes that result in a number to be dialed.It acts as a drop-down from which either an outgoing line group or an ARS form can be selected.
- **Feature**: Default = Dial This sets the action performed by the short code when used. See Short Code Features.
- **Locale**: Default = Blank Features that transfer the caller to voicemail can indicate the language locale required for prompts. This is subject to the language being supported and installed on the voicemail server.

When the system routes a call to the voicemail server it indicates the locale for which matching prompts should be provided if available. The locale sent to the voicemail server by the system is determined as show below. If the required set of prompts is not available, the voicemail will fallback

to another appropriate language and finally to English (refer to the appropriate voicemail installation manual for details).

- **Short Code Locale**: The short code locale, if set, is used if the call is routed to voicemail using the short code.
- **Incoming Call Route Locale**: The incoming call route locale, if set, is used if caller is external.
- **User Locale**: The user locale, if set, is used if the caller is internal.
- **System Locale**: If no user or incoming call route locale is set, the system locale is used unless overridden by a short code locale.

Systems using Embedded Voicemail, if the required set of upgraded language prompts to match the locale is not present on the system SD card, Manager will display an error. The required prompt set can be uploaded from Manager using the Add/Display VM Locales option.

Force Account Code: Default = Off When selected, for short codes that result in the dialing of a number, the user is prompted to enter a valid account code before the call is allowed to continue.

Short Code Field Characters

? - Default Match This character can be used on its own to create a short code match in the absence of any other short code match. See ? Short Codes.

?D - Default Number Dialing This character combination makes a call to the defined phone number as soon as the user goes off-hook. See ? Short Codes.

N - Match Any Digits Matches any dialed digits (including none). The Dial Delay Time or a following matching character is used to resolve when dialing is complete.

X - Match a Digit Matches a single digit. When a group of X's is used, the short code matches against the total number of X's.

[ ] - Secondary Dial Tone Trigger For pre-4.0 IP Office systems used to trigger secondary dial tone. Not used for Release 4.0+. See Secondary Dial Tone.

; - Receive Sending Complete When used this must be the last character in the short code string. If the **Dial Delay Count** is **0**, a **;** instructs the system to wait for the number to be fully dialed, using the **Dial Delay Time** or the user dialing **#**, to indicate completion and then acting on the short code. If the **Dial Delay Count** is not zero, the dialing is only evaluated when **#** is pressed.

The majority of North-American telephony services use en-bloc dialing. Therefore the use of a ; is recommended at the end of all dialing short codes that use an N before routing those calls to a trunk or ARS. This is also recommended for all dialing where secondary dial tone short codes are being used.

Telephone Number Field Characters

A - Allow Outgoing CLI Allow the calling party number sent with the call to be used. This character may be required by service providers in some locales.

C - Use Called Number Field Place any following digits in the outgoing call's Called number field rather than the Keypad field.

D - Wait for Connect Wait for a connect message before sending any following digits as DTMF.

E - Extension Number Replace with the extension number of the dialing user. Note that if a call is forwarded this will be replaced with the extension number of the forwarding user.

h - Hold Music Source When used as part of the short code telephone number field, this character allows the source for music on hold to be selected. Enter h(X) where **X** is 1 to 4 indicating the required hold music source if available. This overrides any previous hold music selection that may have been applied to the call. When used with ParkCall shortcodes, the **h(X)** should be entered before the park slot number part of the telephone number.

I - Use Information Packet Send data in an Information Packet rather than Set-up Packet.

K - Use Keypad Field Place any following digits in the outgoing call's Keypad field rather than the Called Number field. Only supported on ISDN and QSIG.

l - Last Number Dialed (lower case L) Use the last number dialed.

L - Last Number Received Use the last number received.

N - Dialed Digit Wildcard Match Substitute with the digits used for the **N** or **X** character match in the Short Code number field.

p - Priority The priority of a call is normally assigned by the Incoming Call Route or else is **1-Low** for all other calls. Dial Extn short codes can use **p(x)** as a suffix to the **Telephone Number** to change the priority of a call. Allowable values for **x** are **1**, **2** or **3** for low, medium or high priority respectively.

In situations where calls are queued, high priority calls are placed before calls of a lower priority. This has a number of effects:

- Mixing calls of different priority is not recommended for destinations where Voicemail Pro is being used to provided queue ETA and queue position messages to callers since those values will no longer be accurate when a higher priority call is placed into the queue. Note also that Voicemail Pro will not allow a value already announced to an existing caller to increase.
- If the addition of a higher priority call causes the queue length to exceed the hunt group's Queue Length Limit, the limit is temporarily raised by 1. This means that calls already queued are not rerouted by the addition of a higher priority call into the queue.

S - Calling Number Place any following digits into the outgoing call's calling number field. Using S does not alter any allow or withhold CLI setting associated with the call, the short code characters **A** or **W** should be used respectively. Note that for SIP trunks, the SIP URI configuration options override this setting.

Outgoing CLI Warning Changing the outgoing CLI for calls requires the line provider to support that function. You must consult with your line provider before attempting to change the outgoing CLI, failure to do so may result in loss of service. If changing the outgoing CLI is allowed, most line providers required that the outgoing CLI used matches a number valid for return calls on the same trunks. Use of any other number may cause calls to be dropped or the outgoing CLI to be replaced with a valid number.

On mobile twinned calls, if the original party information is used or a specific calling party information CLI is set, that number overrides setting the outgoing CLI using short codes.

SS - Pass Through Calling Number Pass through the Calling Party Number. For example, to provide the incoming ICLID at the far end of a VoIP connection, a short code **?** with telephone number **.SS** should be added to the IP line.

i - National Both the **S** and **SS** characters can be followed by an **i**, that is **Si** and **SSi**. Doing this sets the calling party number plan to ISDN and number type to National. This may be required for some network providers.

t - Allowed Call Duration Set the maximum duration in minutes for a call plus or minus a minute. Follow the character with the number of minutes in brackets, for example **t(5)**.

U - User Name Replace with the User Name of the dialing user. Used with voicemail.

W - Withhold Outgoing CLI Withhold the sending of calling ID number. Operation is service provider dependent.

Y - Wait for Call Progress Message Wait for a Call Progress or Call Proceeding message before sending any following digits as DTMF. For example, the Y character would be necessary at a site where they have signed up with their telephone service provider to withhold international dialing until a DTMF pin/account number is entered that initiates the call progress/proceeding message.

Z - Calling Party Name This option can be used with trunks that support the sending of name information. The **Z** character should be followed by the name enclosed in **" "** quotation marks. Note that their may be name length restrictions that vary between line providers. The changing of name information on calls being forwarded or twinned may also not be supported by the line provider.

@ - Use Sub Address Field Enter any following digits into the sub-address field.

. - Dialed Digits Replace with the full set of dialed digits that triggered the short code match.

, - One Second Pause Add a one second pause in DTMF dialing.

; - Receive Sending Complete When used this must be the last character in the short code string. If the **Dial Delay Count** is **0**, a **;** instructs the system to wait for the number to be fully dialed, using the **Dial Delay Time** or the user dialing **#**, to indicate completion and then acting on the short code. If the **Dial Delay Count** is not zero, the dialing is only evaluated when **#** is pressed.

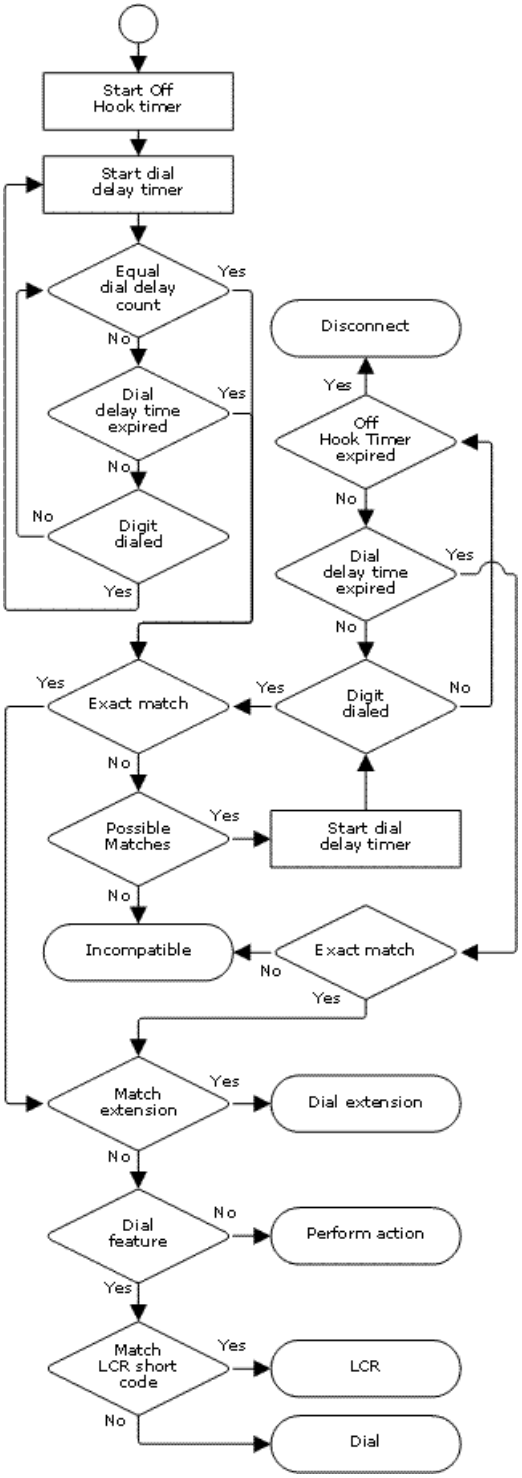
" " - Non Short Code Characters Use to enclose any characters that should not be interpreted as possible short code special characters by the system. For example characters being passed to the voicemail server.

Related Links

Short Code Overview on page 749

User Dialing

Summary: Looks at how the system looks for possible short code matches to user dialing.



The following system settings influence user dialing.

Dial Delay Count: Default = 0 (US/Japan), 4 (ROW) This value sets the number of digits dialed before the system looks for a short code match.

Dial Delay Time: Default = 4 seconds (US/Japan), 1 second (ROW) This value sets the maximum allowed interval between the dialing of each digit. If exceeded, the system looks for a short code match even if the Dial Delay Count has not been reached.

Off-Hook Timer: Length Fixed by locale. When a user goes off-hook, the system starts a 30 second off-hook timer (10 seconds in Italy). If the off-hook timer expires before a short code match occurs, the user is disconnected.

The following rules are used when short code matching is performed for user dialing:

- A short code is used immediately an exact match is found unless followed by a ;.
- If no match is found but partial matches exist, the user can continue dialing.
- If no match or partial matches are found, incompatible is returned.
- The following precedence is used to determine which short codes are used:
- Extension number matches override all short codes.
- User short codes override user rights and system short codes.
- User Rights short code matches override system short codes.
- When multiple exact matches occur,
- The match with the most specified digits rather than wildcards is used.
- If there are still more than one match, the match with the most exact length is used. This means X wildcards will override N when both match.

Related Links

Short Code Overview on page 749

Application Dialing

Numbers speed dialed by system applications such as SoftConsole are treated differently. Since the digits are received en bloc as a single group, they can override some short code matches. The same applies to short codes used within system configuration settings such as Incoming Call Route destinations.

Example:

- Telephone Number: 12345678
- Short Code 1: 1234XX/Dial/Extn/207
- Short Code 2: 12345678/Dial Extn/210

If dialed manually by the user, as soon as they have dialed 123456 a match to short code 1 occurs. They can never dial short code 2.

If dialed using an application, 12345678 is sent as a string and a match to short code 2 occurs.

Partial Dialing

If the application dialing does not trigger an exact match, the user can dial additional digits through their extension. The processes for normal user dialing are applied.

Non-Digit Short Codes

Short codes can be created that use alphabetic characters instead of numbers. While these short codes cannot be dialed from a phone, they can be dialed using application speed dials and settings. However characters that are interpreted as special short code characters will still be interpreted as such.

Related Links

Short Code Overview on page 749

Secondary Dial Tone

Some locales prefer to provide users with secondary dial tone once they have started dialing external calls. This dial tone is heard by the user until they have completed dialing and a trunk is seized at which point call progress tones are provided by the trunk, or camp on/busy tone is provided by the system if the required trunk cannot be seized.

Release 4.0 and Higher

The use of secondary dial tone is provided through the **Secondary Dial Tone** check box option on the ARS form to which the call is routed. When on, this setting instructs the system to play secondary dial tone to the user.

The tone used is set as either **System Tone** (normal dial tone) or **Network Tone** (secondary dial tone). Both tone types are generated by the system in accordance with the system specific locale setting. Note that in some locales normal dial tone and secondary dial tone are the same.

When **Secondary Dial Tone** is selected, the ARS form will return tone until it receives digits with which it can begin short code matching. Those digits can be the result of user dialing or digits passed by the short code which invoked the ARS form. For example with the following system short codes:

In this example, the 9 is stripped from the dialed number and is not part of the telephone number passed to the ARS form. So in this case secondary dial tone is given until the user dials another digit or dialing times out.

- **Code**: 9N
- **Telephone Number**: N
- **Line Group ID**: 50 Main

In this example, the dialed 9 is included in the telephone number passed to the ARS form. This will inhibit the use of secondary dial tone even if secondary dial tone is selected on the ARS form.

- **Code**: 9N
- **Telephone Number**: 9N
- **Line Group ID**: 50 Main

Pre-4.0 IP Office Secondary Dial Tone

Pre-4.0 systems provided dial tone through the use of the short code feature Secondary Dial Tone and the [ ] special characters. For example, on a system where 9 is used as a prefix for external dialing, the system short code 9/./Secondary Dial Tone/0 will trigger secondary dial tone when users dial a number prefixed with 9. This method is not supported by Release 4.0 which provides ARS forms for the control of outgoing calls.

In order to allow further digit matching, the digits dialed are put back through short code matching against any short codes that start with [n] where n is the digit used to trigger the system secondary dial tone short code.

On all systems where secondary dial tone is used, a ; should also be used in dialing short codes that contain N.

For example:

System Short Codes

- 9/SecondaryDialTone/.
- [9]0N;/Dial/0

User Short Code

[9]0N;/Busy/0

The user dials 90114445551234. The 9 is matches the system secondary dial tone short code and unlike other short codes this is applied immediately. The user's dialing is put through short code matching again using the normal order of precedence but matched to possible short codes beginning [9]. In this case the user's [9]0N; short code would take precedence over the system [9]0N; short code.

Related Links

Short Code Overview on page 749

? Short Codes

The ? character can be used in short codes in the following ways:

Default Short Code Matching:

? short codes are used in short code matching in the following way. If no user or system short code match is found, the system will then look for a ? short code match. It will look first for a user ? short code and then, if not found, a system ? short code.

Example: On systems outside North America, the system short code **?/Dial/./0** is added as a default short code. This short code provides a match for any dialing to which there is no other match. Therefore, on systems with this short code, the default is that any unrecognized number will be dialed to Outgoing Line Group 0.

Hot-Line Dialing:

A user short code **?D** can be used to perform a short code action immediately the user extension goes off-hook. This is supported with Dial type short code features. Typically it is used with door, lift and lobby phones to immediately connect the phone to a number such as the operator or reception.

Voicemail Collect Short Codes:

The ? character can appear in the **Telephone Number** field of a short code. This is done with short codes using the VoicemailCollect feature. In this instance the ? character is not interpreted by the system, it is used by the voicemail server.

Related Links

Short Code Overview on page 749

Short Code Matching Examples

The following examples are not meant as practical examples. However they are simple to implement and test on real system without conflicting with its normal operation. They illustrate the interaction between different short codes in resolving which short code is an exact match. They assume that extension numbers are in the 200 to 299 range.

The term 'dials' means dialing the indicated digit or digits without the inter-digit Dial Delay Time expiring.

The term 'pause' means a wait that exceeds the inter-digit Dial Delay Time.

Scenario 1		
Short Code 1 = 60/Dial Extn/203 Dial Delay Count = 0. Dial Delay Time = 4 seconds.		
Test	Dialing	Effect
1	8	No possible match, incompatible returned immediately
2	6	No exact match but there is a potential match, so the system waits. When the Dial Delay Time expires, no exact match is found so incompatible is returned.
3	60	Exact match to Short Code 1. Extension 203 called immediately.
4	61	No possible match, the system returns incompatible.

Scenario 2
Short Code 1 = 60/Dial Extn/203 Short Code 2 = 601/Dial Extn/210

Table continues…

Dial Delay Count = 0. Dial Delay Time = 4 seconds.		
Test	Dialing	Effect
1	8	No possible match, incompatible returned immediately
2	60	Exact match to Short Code 1. Extension 203 called immediately.
3	601	Exact match to Short Code 1 as soon as the 0 is dialed. The user cannot manually dial 601.

Scenario 3		
Short Code 1 = 60/Dial Extn/203 Short Code 2 = 601/Dial Extn/210 Dial Delay Count = 3. Dial Delay Time = 4 seconds.		
Test	Dialing	Effect
1	8	Insufficient digits to trigger matching. The system waits for additional digits or for Dial Delay Time to expire. When Dial Delay Time expires, no possible match is found so incompatible is returned.
2	60	Insufficient digits to trigger matching. The system waits for additional digits or for Dial Delay Time to expire. When Dial Delay Time expires, matching started and exact match to Short Code 1 occurs. .
3	601	Third digit triggers matching. Exact match to Short Code 2. Extension 210 dialed immediately.
4	60#	# is treated as a digit and as the third digit triggers matching. No exact match found. The system returns incompatible.

Scenario 4		
Short Code 1 = 60;/Dial Extn/203 Short Code 2 = 601/Dial Extn/210 Dial Delay Count = 3. Dial Delay Time = 4 seconds.		
Test	Dialing	Effect
1	8	Insufficient digits to trigger matching. The system waits for

Table continues…

		additional digits or for Dial Delay Time to expire. When Dial Delay Time expires, no possible match is found so incompatible is returned.
2	6	Insufficient digits to trigger matching. The system waits for additional digits or for the interdigit Dial Delay Time to expire. If the Dial Delay Time expires, a potential match exists to a short code that uses ; so the system waits for an additional digit until the off-hook timer expires.
3	60	As above but an additional digit now may create a match. If 1 is dialed, it creates an exact match to Short Code 2 and is used immediately. If 0, * or 2 to 9 is dialed, no possible match exists. The system returns incompatible. If the next digit is a #, it is treated as signaling dialing complete rather than being a digit. Short code 1 becomes an exact match and is used immediately.
4	601	Third digit triggers matching. Exact match to Short Code 2. Extension 210 dialed immediately.

Scenario 5		
Short Code 1 = 601/Dial Extn/203 Short Code 2 = 60N/Dial Extn/210 Dial Delay Count = 0. Dial Delay Time = 4 seconds.		
Test	Dialing	Effect
1	6	No exact match but there is a potential match, so the system waits for additional dialing. If the Dial Delay Time expires, no exact match is found so incompatible is returned.
2	60	Potential match to both short codes. The system waits for additional dialing. If the Dial Delay Time expires, Short Code 2

Table continues…

		becomes an exact match with N blank.
3	601	Exact match to Short Code 1. Used immediately
4	602	Exact match to Short Code 2. Used immediately.

Scenario 6		
Short Code 1 = 601/Dial Extn/203 Short Code 2 = 60N/Dial Extn/210 Short Code 3 = 60X/Dial Extn/207 Dial Delay Count = 0. Dial Delay Time = 4 seconds.		
Test	Dialing	Effect
1	6	No exact match but there are potential matches so the system waits for additional dialing. If the Dial Delay Time expires, no exact match has occurred so incompatible is returned.
2	60	Potential match to all short codes. System waits for additional dialing. If the Dial Delay Time expires, Short Code 2 becomes an exact match with N blank. If a digit is dialed, Short Code 3 becomes a more exact match and is used.
3	601	Exact match all short code, however Short Code 1 is treated as being more exact (more matching digits) and is used immediately
4	602	Exact match to short codes 2 and 3, however the Short Code 3 is treated as being more exact (length match) and is used immediately.

Scenario 7		
Short Code 1 = 601/Dial Extn/203 Short Code 2 = 60N/Dial Extn/210 Short Code 3 = 6XX/Dial Extn/207 Dial Delay Count = 0. Dial Delay Time = 4 seconds.		
Test	Dialing	Effect

Table continues…

1	6	No exact match but there are potential matches so the system waits for additional dialing. If the Dial Delay Time expires, no exact match has occurred so incompatible is returned.
2	60	Potential match to all short codes. System waits for additional dialing. If the Dial Delay Time expires, Short Code 2 becomes an exact match with N blank. If a digit is dialed, Short Code 3 becomes an more exact match and is used.
3	601	Exact match all short code, however Short Code 1 is treated as being more exact (more matching digits) and is used immediately
4	602	Exact match to short codes 2 and 3, however the Short Code 2 is treated as being more exact (more matching digits) and is used immediately.
5	612	Exact match to Short Code 3.

Related Links

Short Code Overview on page 749

Default System Short Code List

Most control units are available in A-Law and U-Law models. Typically U-Law models are supplied to North American locales, A-Law models are supplied to the rest of the world. In addition to the using different default companding for digital lines and phone, A-Law and U-Law models support different default short codes. The following table lists the default system short codes present in a system's configuration.

Standard Mode

Short Code	Telephone Number	Feature	A-Law	ULAW
***00**	Blank	Cancel All Forwarding	✓	✓
***01**	Blank	Forward Unconditional On	✓	✓

Table continues…

Short Code	Telephone Number	Feature	A-Law	ULAW
***02**	Blank	Forward Unconditional Off	✓	✓
***03**	Blank	Forward On Busy On	✓	✓
***04**	Blank	Forward On Busy Off	✓	✓
***05**	Blank	Forward On No Answer On	✓	✓
***06**	Blank	Forward On No Answer Off	✓	✓
***07*N#**	N	Forward Number	✓	✓
***08**	Blank	Do Not Disturb On	✓	✓
***09**	Blank	Do Not Disturb Off	✓	✓
***10*N#**	N	Do Not Disturb Exception Add	✓	✓
***11*N#**	N	Do Not Disturb Exception Del	✓	✓
***12*N#**	N	Follow Me Here	✓	✓
***13*N#**	N	Follow Me Here Cancel	✓	✓
***14*N#**	N	Follow Me To	✓	✓
***15**	Blank	Call Waiting On	✓	✓
***16**	Blank	Call Waiting Off	✓	✓
***17**	?U	Voicemail Collect	✓	✓
***18**	Blank	Voicemail On	✓	✓
***19**	Blank	Voicemail Off	✓	✓
***20*N#**	N	Set Hunt Group Night Service	✓	✓
***21*N#**	N	Clear Hunt Group Night Service	✓	✓
***22*N#**	N	Suspend Call	✓	✗
***23*N#**	N	Resume Call	✓	✗
***24*N#**	N	Hold Call	✓	✗
***25*N#**	N	Retrieve Call	✓	✗
***26**		Clear CW	✓	✗
***27*N#**	N	Hold CW	✓	✗
***28*N#**	N	Suspend CW	✓	✗

Table continues…

Short Code	Telephone Number	Feature	A-Law	ULAW
***29**	Blank	Toggle Calls	✓	✓
***30**	Blank	Call Pickup Any	✓	✓
***31**	Blank	Call Pickup Group	✓	✓
***32*N#**	N	Call Pickup Extn	✓	✓
***33*N#**	N	Call Queue	✓	✓
***34N;**	N	Hold Music	✓	✓
***35*N#**	N	Extn Login	✓	✓
***36**	Blank	Extn Logout	✓	✓
***37*N#**	N	Call Park	✓	✓
***38*N#**	N	Unpark Call	✓	✓
***39**	1	Relay On	✓	✓
***40**	1	Relay Off	✓	✓
***41**	1	Relay Pulse	✓	✓
***42**	2	Relay On	✓	✓
***43**	2	Relay Off	✓	✓
***44**	2	Relay Pulse	✓	✓
***45*N#**	N	Acquire Call	✓	✓
***46**	Blank	Acquire Call	✓	✓
***47**	Blank	Conference Add	✓	✓
***48**	Blank	Voicemail Ringback On	✓	✓
***49**	Blank	Voicemail Ringback Off	✓	✓
***50**	Blank	Forward Huntgroup On	✓	✓
***51**	Blank	Forward Huntgroup Off	✓	✓
***52**	Blank	Cancel or Deny	✓	✓
***53*N#**	N	Call Pickup Members	✓	✓
***55**	Blank	Stamp Log	✓	✓
***57*N#**	N	Forward On Busy Number	✓	✓
***70**	Blank	Call Waiting Suspend	✓	✗
***70*N#**	N	Dial Physical Extn by Number	✗	✓

Table continues…

Short Code	Telephone Number	Feature	A-Law	ULAW
***71*N#**	N	Dial Physical Extn by Id	✗	✓
9000	"MAINTENANCE"	Relay On	✓	✓
***91N;**	N".1"	Record Message	✓	✓
***92N;**	N".2"	Record Message	✓	✓
***99;**	"edit_messages"	Voicemail Collect	✓	✓
9N	N	Dial	✗	✓
?	.	Dial	✓	✗

Server Edition

Short Code	Telephone Number	Feature	A-Law	ULAW
***00**	Blank	Cancel All Forwarding	✓	✓
***01**	Blank	Forward Unconditional On	✓	✓
***02**	Blank	Forward Unconditional Off	✓	✓
***03**	Blank	Forward On Busy On	✓	✓
***04**	Blank	Forward On Busy Off	✓	✓
***05**	Blank	Forward On No Answer On	✓	✓
***06**	Blank	Forward On No Answer Off	✓	✓
***07*N#**	N	Forward Number	✓	✓
***08**	Blank	Do Not Disturb On	✓	✓
***09**	Blank	Do Not Disturb Off	✓	✓
***10*N#**	N	Do Not Disturb Exception Add	✓	✓
***11*N#**	N	Do Not Disturb Exception Del	✓	✓
***12*N#**	N	Follow Me Here	✓	✓
***13*N#**	N	Follow Me Here Cancel	✓	✓
***14*N#**	N	Follow Me To	✓	✓
***17**	?U	Voicemail Collect	✓	✓

Table continues…

Short Code	Telephone Number	Feature	A-Law	ULAW
***18**	Blank	Voicemail On	✓	✓
***19**	Blank	Voicemail Off	✓	✓
***20*N#**	N	Set Hunt Group Night Service	✓	✓
***21*N#**	N	Clear Hunt Group Night Service	✓	✓
***29**	Blank	Toggle Calls	✓	✓
***30**	Blank	Call Pickup Any	✓	✓
***31**	Blank	Call Pickup Group	✓	✓
***32*N#**	N	Call Pickup Extn	✓	✓
***33*N#**	N	Call Queue	✓	✓
***34N;**	N	Hold Music	✓	✓
***35*N#**	N	Extn Login	✓	✓
***36**	Blank	Extn Logout	✓	✓
***37*N#**	N	Call Park	✓	✓
***38*N#**	N	Unpark Call	✓	✓
***44**	2	Relay Pulse	✓	✓
***45*N#**	N	Acquire Call	✓	✓
***46**	Blank	Acquire Call	✓	✓
***47**	Blank	Conference Add	✓	✓
***48**	Blank	Voicemail Ringback On	✓	✓
***49**	Blank	Voicemail Ringback Off	✓	✓
***50**	Blank	Forward Huntgroup On	✓	✓
***51**	Blank	Forward Huntgroup Off	✓	✓
***52**	Blank	Cancel or Deny	✓	✓
***53*N#**	N	Call Pickup Members	✓	✓
***55**	Blank	Stamp Log	✓	✓
***57*N#**	N	Forward On Busy Number	✓	✓
***66*N#**	N	Conference Meet Me	✓	✓

Table continues…

Short Code	Telephone Number	Feature	A-Law	ULAW
***70**	Blank	Call Waiting Suspend	✓	✗
***70*N#**	N	Dial Physical Extn by Number	✗	✓
***71*N#**	N	Dial Physical Extn by Id	✗	✓
***99;**	"edit_messages"	Voicemail Collect	✓	✓
9N	N	Dial	✗	✓ [1]
?	.	Dial	✓	✓ [1]

For U-Law systems, a **9N** is a default short code on the Primary Server while a **?** short code is a default on all other servers.

Additional short codes of the form *DSSN, *SDN, *SKN, these are used by the system for internal functions and should not be removed or altered. Short codes *#N and **N may also visible, these are used for ISDN functions in Scandinavian locales.

The default ***34** short code for music on hold has changed to ***34N;**.

Related Links

Short Code Overview on page 749

Chapter 19: Button Programming Overview

This section provides an overview of system actions that can be assigned to programmable buttons on Avaya phones.. For details on each button action, see *Avaya IP Office™ Platform Short Code and Button Action Reference*.

Button assignment can be done through the system configuration using Manager and for some functions using the phone itself. Using Manager, if only button programming changes are required, the configuration changes can be merged back to the system without requiring a reboot.

Appearance Functions The functions **Call Appearance**, **Bridged Appearance**, **Coverage** and **Line Appearance** are collectively known as "appearance functions". For full details of their operation and usage refer to the Appearance Button Operation section. The following restrictions must be observed for the correct operation of phones.

Phone Support Note that not all functions are supported on all phones with programmable buttons. Where possible exceptions, have been indicated. Those buttons will typically play an error tone when used on that phone. Programming of those features however is not restricted as users may hot desk between different types of phones, including some where the feature is supported.

Actions that use status feedback are only supported on buttons that provide that feedback through lamps or icons.

Related Links

Programming Buttons with Manager on page 768
Programming Button via the Menu Key on page 770
Programming Button via an Admin Button on page 773
BST Button Programming on page 774
T3 Self-Administration on page 776
Interactive Button Menus on page 778
Label Templates on page 778

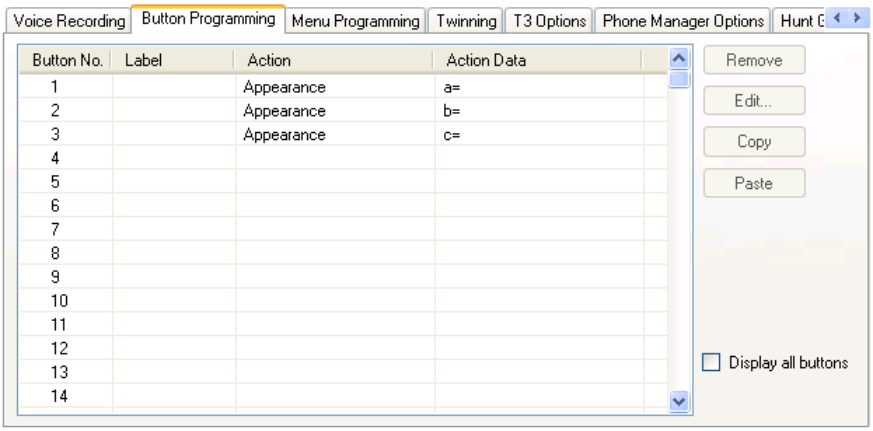
Programming Buttons with Manager

About this task

Procedure

1. Select the  **User** required to display their configuration details.

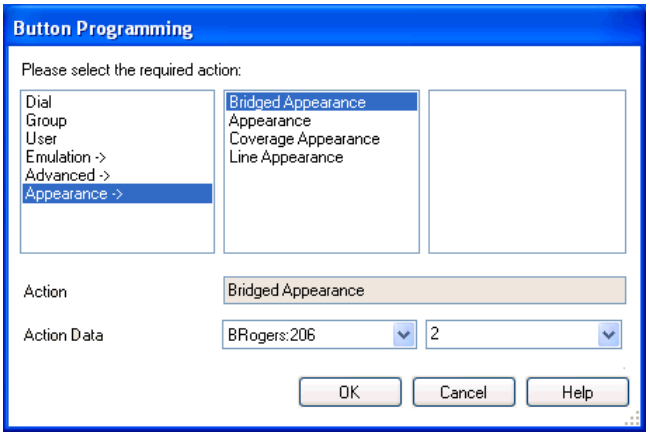
2. Select **Button Programming**.



The number of button displayed is based on the phone associated with the user when the configuration was loaded. This can be overridden by selecting **Display All Buttons**. This may be necessary for users who switch between different phones using hot desking or have an expansion unit attached to their phone.

3. For the required button, either select the button and then click **Edit**or double-click the button.
4. Edit the settings as required.

   Use the **...** button to display the menu for selecting the required button action. Select the action and set the action data, then click **OK**.



5. Click **OK**.

   Repeat for any other buttons.

6. Click **OK**.

Result

An alternate method for the above programming is to right-click on the various fields. To do this start with the **Action** field, then **Action Data** and then **Label** if required.

Related Links

Button Programming Overview on page 768

Programming Button via the Menu Key

On 4412D+, 4424D+, 4612IP, 4624IP, 6408D, 6416D, 6424D phones the **Menu** button can be used to program some functions against other buttons. This programming also includes programmable buttons on any associated add-on units associated with the phone. Buttons already programmed as appearance buttons cannot be altered using these methods.

A Self-Administer button can also be added to allow the phone user to program the functions on their other buttons, see Self-Administer.

T3 phone users can also program buttons using a Menu function, see T3 Self-Administration.

Related Links

Button Programming Overview on page 768

Setting a Button to Dial a Number

About this task

This process sets the selected programmable button to the Dial function in the system configuration.

Procedure

1. With the phone idle and on-hook, press MENU.
2. Press ▶ and select **PROG**.
3. Enter the number required.

   The left-most display button can be used to backspace and the right-most display button can be used to **Clear** the whole number.
4. Press the programmable button against which the number should be set.
5. If the button is already programmed, options to replace (**Repla**), keep (**Keep**) or delete (**Delet**) the buttons existing programming appear.

   Select the option required.
6. The message **BUTTON PROGRAMMED!** indicates that the button is now programmed.

   Select **Cont** and then press Exit.

Setting a Button to a Switch Function

About this task

This process allows users to program there own Group, User, and Park slot monitor buttons. It also allows the programming of Dial and Flash Hook buttons.

Procedure

1. With the phone idle and on-hook, press Menu twice.
2. Press ▶ and select **ProgA**.
3. Press ▶ and select **DSS**.
4. Use the ◀ and ▶ buttons to display the function required. Press the display button below the function to select it.
5. If the function requires a telephone number value set, enter the number.

   The left-most display button can be used to backspace and the right-most display button can be used to **Clear** the whole number.
6. Press the programmable button against which the number should be set.
7. If the button is already programmed, options to replace (**Repla**), keep (**Keep**) or delete (**Delet**) the buttons existing programming appear.

   Select the option required.
8. The message **BUTTON PROGRAMMED!** indicates that the button is now programmed.

   Select **Cont** and then press Exit.

Setting Buttons to Admin Function

About this task

Phones with a **Menu** key can program a range of self-administer functions onto their programmable buttons. These are:

Dir - Directory.

Drop - Drop.

HFAns - Internal Auto-Answer.

Timer - Timer.

AutCB - Automatic Callback.

Prog - Abbreviated Dial Program.

CFrwd - Call Forwarding All.

CPark - Call Park.

SAC - Send All Calls.

TmDay - Time of Day.

Admin - Self-Administer.

Acct - Account Code Entry.

AD - Abbreviated Dial.

Call Park

GrpPg - Group Paging.

CPkUp - Call Pickup.

DPkUp - Directed Call Pickup.

RngOf - Ringer Off.

Spres - AD Suppress.

HdSet - Headset Toggle.

HGNS+ - Set Hunt Group Night Service.

This is the same set of functions that can be programmed by users with a button set to Self-Administer (see Self-Administer).

Procedure

1. With the phone idle and on-hook, press Menu.
2. Press ▶ twice and select **Admin**.
3. Use the ◀ and ▶ keys to display the function required and then select it by pressing the display button below the feature.

   Selecting **Expl?** changes the display from short name mode to long name mode. In this mode the full names of the features are displayed. Select **SHORTMODE** to return to that mode.
4. If the function requires a telephone number value set, enter the number.

   The left-most display button can be used to backspace and the right-most display button can be used to **Clear** the whole number.
5. Press the programmable button against which the number should be set.
6. If the button is already programmed, options to replace (**Repla**), keep (**Keep**) or delete (**Delet**) the buttons existing programming appear.

   Select the option required.
7. The message **BUTTON PROGRAMMED!** indicates that the button is now programmed.

   Select **Cont** and then press Exit.

Programming Button via an Admin Button

The Admin (also called Self-Administer) function can be assigned to a programmable button on a user's phone. That button then allows the user to program functions against other programmable buttons on their phone, except those already set as appearance buttons.

Admin buttons are only supported on **2410**, **2420**, **4406D+**, **4412D+**, **4424D+**, **4606IP**, **4612IP**, **4624IP**, **5410**, **5420**, **6408D**, **6416D** and **6424D**.

On **4412D+, 4424D+, 4612IP, 4624IP, 6408D, 6416D, 6424D** phones:

- **Admin** can be permanently accessed via **Menu**, ▸, ▸, **Admin**.
- **Admin1** can be permanently accessed via **Menu**, **Menu**, ▸, **ProgA**, , ▸, **DSS**.

Related Links

Button Programming Overview on page 768

Using an Admin Button

About this task

Procedure

1. With the phone idle and on-hook, press the button programmed to **Admin** or **Admin1**.

   The list of available functions is shown.

2. Use the ◂ and ▸ buttons to move through the list.

   Selecting **Expl?** changes the display from short name mode to long name mode. In this mode the full names of the features are displayed. Select **SHORTMODE** to return to that mode.

3. Select the function required.

4. If the function requires a telephone number value set, enter the number.

   The left-most display button can be used to backspace and the right-most display button can be used to Clear the whole number.

5. Press the programmable button against which the number should be set.

   On phones with multiple pages of buttons use the ◂ and ▸ button to select the required page before pressing the button to program.

6. If the button is already programmed, options to replace, keep or delete the button's existing programming appear.

   Select the option required.

7. The message **BUTTON PROGRAMMED!** indicates that the button is now programmed.

8. Select **Cont**. and then press `Exit`or lift the handset to go off-hook.

BST Button Programming

About this task

The process below can be used to assign functions to programmable buttons on T-Series and M-Series phones. Existing button can be overwritten except buttons set to appearance functions.

Procedure

1. Press `Feature *3`.

   If a security code is requested, enter your phone login code and press #.

2. Use one of the processes below.

   Press * to switch between processes (or **More** if displayed). On T7000 phones, only the first process is supported.

3. Select Button and then Function

   a. Press the button to program.

   b. Enter the feature code of the function required (the only * function supported is *7 for contrast).

   c. If the button has an existing function it is displayed and the option to replace the button or return to function selection.

4. Select Function and then Button.

   Enter the number for the feature required or use the volume buttons to move through the list of functions.

   01. Speed dial
   02. Ring Again
   03. Conference
   04. Call Forward All
   05. Last Number Redial
   06. Page Group
   07. Voicemail
   08. Automatic Intercom
   09. Priority Call
   10. Transfer
   11. Call Park
   12. Group Pickup
   13. Direct Pickup
   14. Timer

15. Do Not Disturb On
16. Contrast
17. Group Listen On
18. Time of Day
17. Call Log
18. Self-Administer
19. Account Code
20. Forward on Busy
21. Forward on No Answer
22. Pickup
23. Directory
24. Flash Hook
25. Internal Auto Answer
26. Set Hunt Group Night Service
27. Twinning
28. Ringer Off

    a. Press `Hold`to select a currently displayed function.

    b. Press the button to which the function should be assigned.

    c. If the button has an existing function it is displayed and the option to replace the button or return to function selection.

5. When **Default Buttons** is displayed, press `Hold`(or the **Prog** softkey if displayed).

   The phone buttons are defaulted to those appropriate to the phone type. Note that only buttons that have a default function on the phone type are defaulted. It does not affect the functions assigned to any buttons that do not have default functions.

   Default Buttons

   For T-Series and M-Series phones, default button functions are assigned to buttons when a phone is first connected to the extension port. The functions assigned depend on the particular phone model.

   The default functions for the phone model are also assigned when **Feature *3** is used to default the phone's buttons. Buttons without a default function are not overwritten when the buttons are defaulted.

Related Links

Button Programming Overview on page 768

T3 Self-Administration

Release 4.2+ supports functions for T3 phone users to be able to program their own buttons. This is similar to the existing Self-Administer button supported on other phones but is configured and accessed via different methods.

The user accesses button programming through **Menu | Settings | Button programming**. This function is not available by default, instead it must be configured as available for the user using the method detailed below.

Once enabled, the user is able to configure the following functions on buttons:

Function	Description
empty	Returns the button to it normal default function.
Account Code	Allows the user to enter an account code before or during a call. The account code can be preset or entered after the button press. See the Account Code Entry function.
Callback	Set a callback from the currently dialed extension number. See the Automatic Callback function.
Call list	Displays a list of calls received. See the Call List function.
Call Tracing	Activate malicious call tracing. See the MCID Activate function and Malicious Call Tracing (MCID).
Dial	Dial a preset number or partial number that can be completed after the button press. See the Dial function.
Dial Intercom	Make a page call to the selected target if it supports handsfree answer. See Dial Intercom.
Directory	Display the system directory. See the Directory function.
Do not disturb	Toggle the phone between do not distrub on and off. See the Send All Calls function.
Follow me here	Activate/cancel follow me here. See the Follow Me Here function.
Forward unconditional	Activate/cancel forward all calls. See the Forward Unconditional On function.
Group Paging	Page a group of phones. See the Group Paging function.
Group Membership	Enable/disable the user membership of a group or all groups. See the Hunt Group Enable function.
Group State	Change a hunt group's out of service status. See the Set Hunt Group Out of Service function.

Table continues…

Headset	Switch between handset and headset modes. See the Headset Toggle function.
Internal Auto-Answer	Auto connect internal calls after a single tone. See the Internal Auto-answer function.
Login	Access the menu for phone log in. See the Extn Login function.
Logout	Log out from the phone. See the Extn Logout function.
Night Service	Change a hunt group's night service status. See the Set Hunt Group Night Service function.
Paging	Page an extension or group. See the Dial Paging function.
Pickup	Answer a call alerting on the system. See the Call Pickup function.
Pickup Member	Answer a call alerting the hunt group of which the user is a member. See the Call Pickup Members function.
Twinning	Switch mobile twinning on/off and set the twinning destination. Also used to pull a call answered at the twinned number back to the users primary extension. See the Twinning function.
User	Monitor the status of a user. Also used to call them or to pickup calls alerting them. See the User function.
Visual Voice	Create a visual voice access button. See Visual Voice.
Voicemail	Equivalent to the Voicemail Collect function.
Voicemail on/off	Switch the use of the user's mailbox to answer unanswered calls calls on/off. See the Voicemail On function.

The user will need to be made aware of which physical buttons can be programmed as this varies between the different T3 phones. See T3 Compact, T3 Classic and T3 Comfort.

Configuring a T3 User for Button Programming

1. Using Manager, receive the configuration from the system.
2. Select the T3 user and then select **Menu Programming**.
3. Set the action for one of the menus to **Self-Administer**.
4. Send the configuration back to the system.
5. The user will now be able to access button programming from their phone via **Menu | Settings | Button programming**.

Related Links

Button Programming Overview on page 768

Interactive Button Menus

For display phones where the a button has been configured without a specific number, the menu for number entry. The menu includes a Dir option for selecting a number from the directories held by the system.

Functions that use the interactive menu are:

Feature	Directory lists...		Feature	Directory lists...
Automatic Intercom	Users		Follow Me Here Cancel	Users
Acquire Call/Call Steal	Users		Follow Me Here	Users
Call Forwarding All	Users		Follow Me To	Users
Call Intrude	Users		Forward Number	Users/Groups
Call Park To Other Extension	Users		Forward Busy Number	Users/Groups
Dial Inclusion	Users		Group Paging	Users/Groups
Dial Intercom	Users		Leave Word Calling	Users/Groups
Directed Call Pickup	Users/Groups		Priority Calling	Users/Groups

User and Group buttons can be used to indicate the required user or hunt group only if those buttons are on an associated button module. **User** and **Group** buttons on the users extension are not accessible while the interactive button menu is being displayed.

For functions supported across a multi-site network, the directory will include remote users and advertised hunt groups.

For M-Series and T-Series phone, the volume buttons are used to scroll through the list of matching names. If this is done during a call or while a call is alerting, this will also adjust the call or ring volume.

Related Links

Button Programming Overview on page 768

Label Templates

The attached zip file below contains Word document templates for the paper programmable key labels on various phones supported by the system. Two templates are provided, one for A4 size paper, the other for US Letter sized paper.

DSS Key Label Template File (Microsoft Word .dot Files)

For ETR, M-Series, T-Series, 1400 and 1600 phones, a number of tools and perforated printable labels are available. For further details visit http://support.avaya.com and search for information on DESI. Alternatively visit http://www.desi.com.

Manager is able to pass user button information to a DESI application on the same PC. This allows printing of labels using the label text set within the system configuration. Currently only ETR, M-Series, T-Series, 1400 and 1600 phonesphones are supported by DESI.

Related Links

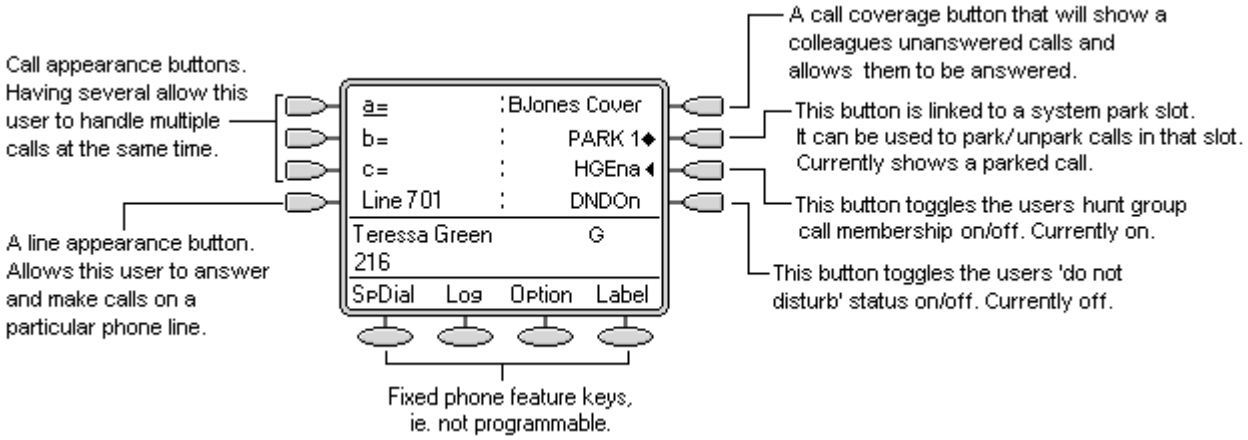
Button Programming Overview on page 768

Chapter 20: Appeance Button Operation

Many Avaya phones supported on system have a programmable keys or buttons (the terms 'key' and 'button' mean the same thing in this context). Various actions can be assigned to each of these keys, allowing the phone user to access that action.

Many of the phones also have indicator lamps next to the programmable buttons. These lamps are used to indicate the status of the button, for example 'on' or 'off'. On other phones the programmable buttons use an adjacent area of the phones display to show status icons and text labels for the buttons.

Example The example below shows the display and programmable buttons on an Avaya 5421 phone where a number of programmable features have been assigned to the user.



This type of phone displays text labels for the programmed features. On other phones a paper label may have to be updated to indicate the programmed feature.

The system supports the following 'appearance' actions - Call Appearance, Bridged Appearance, Line Appearance and Call Coverage Appearance. These actions can be assigned to the programmable buttons on a user's phone. Those 'appearance' buttons can then be used to answer, share, switch between and in some case make calls. This type of call handling is often called 'key and lamp mode'.

This document covers the programming and operation of phones using the appearance functions. Details of the other actions that can be assigned to programmable keys are covered in Button Programming.

Note:

For all the examples within this documentation, it is assumed that **Auto Hold** is on and **Answer Pre-Select** is off unless otherwise stated.

The text shown on phone displays are typical and may vary between phone types, locales and system software releases.

Related Links

Appearance Button Features on page 781
Call Appearance Buttons on page 782
Bridged Appearance Buttons on page 787
Call Coverage Buttons on page 792
Line Appearance Buttons on page 796
Selected Button Indication on page 802
Idle Line Preference on page 803
Ringing Line Preference on page 806
Answer Pre-Select on page 808
Auto Hold on page 809
Ring Delay on page 810
Delayed Ring Preference on page 812
Collapsing Appearances on page 813
Joining Calls on page 814
Multiple Alerting Appearance Buttons on page 817
Twinning on page 817
Busy on Held on page 818
Reserving a Call Appearance Button on page 818
Logging Off and Hot Desking on page 819
Applications on page 819
Programming Appearance Buttons on page 820

Appearance Button Features

Appearance functions are only supported on Avaya phones which have programmable buttons and also support multiple calls. Appearance functions are also only supported on those buttons that have suitable adjacent indicator lamps or a display area. Appearance buttons are not supported across a multi-site network.

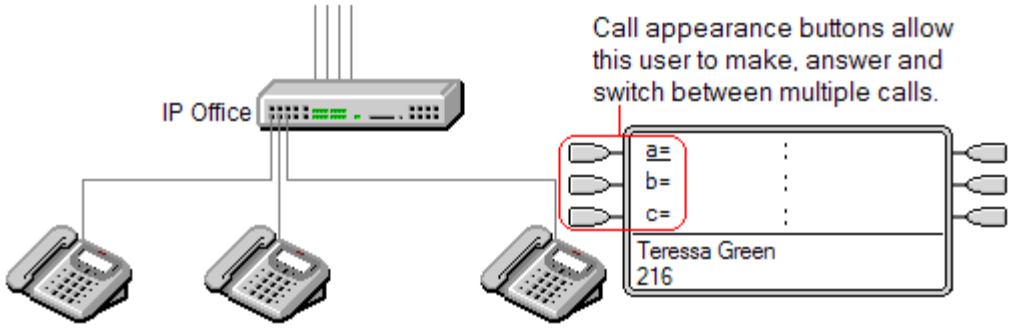
Related Links

Appeance Button Operation on page 780

Call Appearance Buttons

Call appearance buttons are used to display alerts for incoming calls directed to a user's extension number or to a hunt group of which they are a member. Call appearance buttons are also used to make outgoing calls.

By having several call appearance buttons, a user is able to be alerted about several calls, select which call to answer, switch between calls and take other actions.



When all the user's call appearance buttons are in use or alerting, any further calls to their extension number receive busy treatment. Instead of busy tone, the user's forward on busy is used if enabled or otherwise voicemail if available.

Call appearance buttons are the primary feature of key and lamp operation. None of the other appearance button features can be used until a user has some call appearance button programmed[1].

There are also addition requirements to programming call appearance buttons:

Call appearance buttons must be the first button programmed for the user.

Programming a single call appearance button for a user is not supported. The normal default is 3 call appearances per user except on phones where only two physical buttons are available.

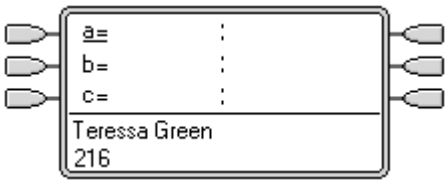
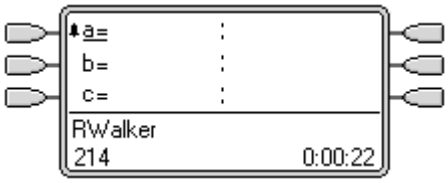
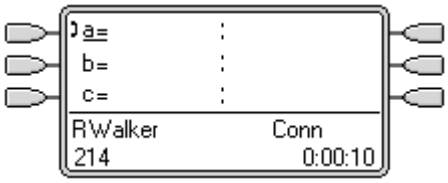
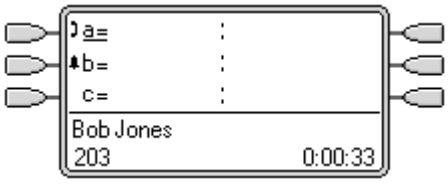
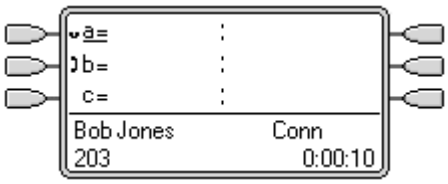
[1] For Release 4.2+, T3 phones support the use of Line Appearance buttons. These can be programmed against buttons on T3 phones without requiring call appearance buttons. See T3 Phone Line Appearances.

Related Links

Appeance Button Operation on page 780
Call Appearance Example 1 on page 782
Call Appearance Example 2 on page 783
How are Call Appearance Buttons Treated? on page 784
Call Appearance Button Indication on page 785

Call Appearance Example 1

In this example, the user has multiple call appearance buttons.

	**Phone Idle** The phone is currently idle.
	**First Call Alerts** A call arrives. It alerts against the first available call appearance button. Pressing that button will answer the call.
	**Call Answered** The call is now connected.
	**Second Call Alerts** A second call arrives whilst the first is still connected. It alerts against the next available call appearance button. As the user has a call in progress, the alert gives just a single ring and briefly display details of the caller.
	**Pressing the Second Call Appearance** Pressing the second call appearance button will hold the first call and answer the second.

Related Links

Call Appearance Buttons on page 782

Call Appearance Example 2

In this example, the user will use their call appearances to make two calls and start a conference between those calls.

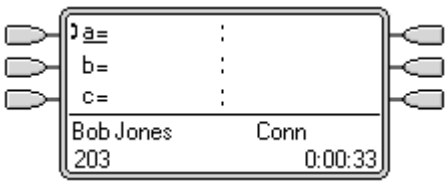
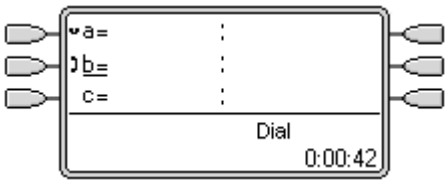
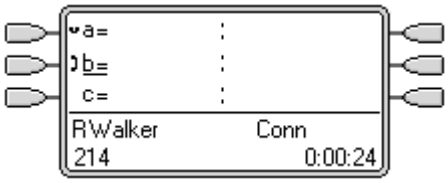
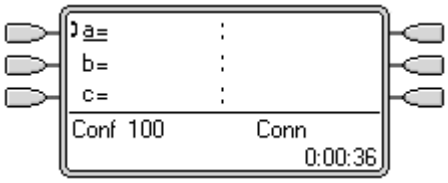
	**Initial Call** The user has a call in progress, shown on their first call appearance button. It is decided to conference another user into the call.

Table continues…

	**Make Conference Enquiry** Pressing the **CONFERENCE** button on the users phone automatically places the current call on hold and takes the phone off hook on the next available call appearance.
	**Enquiry in Progress** The other extension has been dialed and invited to join a conference call. The user presses the **CONFERENCE** button on their phone again.
	**Conference Starts** The conference call has started. The separate call appearances have collapsed to a single appearance that represents the conference.

Related Links

Call Appearance Buttons on page 782

How are Call Appearance Buttons Treated?

For incoming calls

Call Waiting settings are ignored except for hunt group call waiting where the call waiting tone is replaced by an alert on a call appearance button if available.

Follow Me, **Forward Unconditional** and **Forward Hunt Group Calls** are used when set.

If **Do Not Disturb** is set, only calls from numbers in the user's Do Not Disturb Exception list will alert if a call appearance is available.

Busy status

For calls direct to the user's extension number The user is busy when all their available call appearances are in use. Instead of busy tone, the user's forward on busy is used if enabled or otherwise voicemail if available.

For calls to a hunt group of which the user is a member The user is busy to further hunt group calls when they have any appearance button in use on their phone. The only exception is calls to a collective hunt group with call waiting.

In both cases above, even when busy, the user may still receive alerts on other appearance buttons.

For outgoing calls

Outgoing calls are treated exactly the same as calls made by non-appearance button users.

External Calls made on a call appearance, which route out on a line for which the user also has a line appearance, will remain on the call appearance. The line appearance will indicate 'in use elsewhere'.

For call appearance buttons matched by a bridged appearance button

If the bridged appearance is used to make or answer calls, the state of the call appearance will match that of the bridged appearance.

If the call is put on hold by the bridged appearance user, the call appearance will show 'on hold elsewhere'.

Other

Held/Parked Call Timeout If the user has parked a call, the parked call timer only starts running when the user is idle rather than on another call.

Incoming calls routed directly to the user as the incoming call routes destination on a line for which the user also has a line appearance, will only alert on the line appearance. These calls do not follow any forwarding set but can be covered.

Related Links

Call Appearance Buttons on page 782

Call Appearance Button Indication

On phones with a text display area next to the button, by default **a=**, **b=** and so on is displayed. This can be replaced by another label if required.

When the user is not connected to a call, the button indicated as selected is the button that will be used if the user goes off hook without pressing an appearance button. When a user is connected to a call, that call is the selected button.

The following table shows how the different states of call appearance buttons (alerting, held, etc) are indicated. This is a general table, not all phone button types are covered. The ring that accompanies the visual indication can be delayed or switched off. See Ring Delay.

Icon Button	Dual LED Button	Call Appearance Button State
CA1	 Red off, Green off.	**Idle** The call appearance is not in use and is not currently selected.
CA1	 Red on, Green off.	**Idle + Selected** The call appearance is not in use but is the current selected button that will be used if the user goes off hook.
CA1 Flashing icon.	 Red off,	**Alerting** The matching call appearance is alerting for an

Table continues…

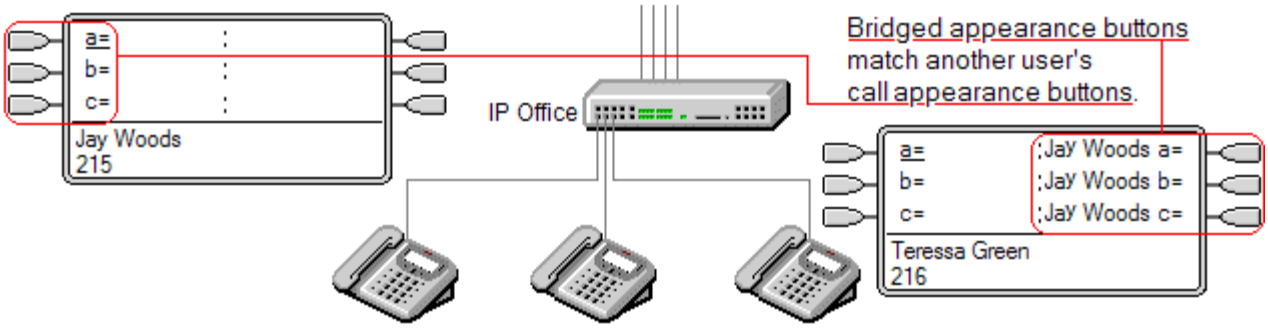
	Green steady flash.	incoming call. This is accompanied by ringing. If the user is already on a call, only a single ring is given.
CA1 Flashing icon.	 Red on, Green steady flash.	**Alerting + Selected** As above but Ringing Line Preference has made this the user's current selected button.
CA1	 Red on, Green on.	**In Use Here** The user has a call connected on the call appearance or is dialing.
CA1	 Red off, Green on.	**In Use Elsewhere** The call appearance button is in use on a bridged appearance.
CA1	 Red off, Green fast flash.	**On Hold Here** The call has been put on hold by this user.
CA1	 Red fast flash, Green fast flash	**On Hold Pending Transfer** Applies to 1400, 1600, 9500 and 9600 Series phones in Release 8.1 and higher.
CA1	 Red off, Green intermittent flash.	**On Hold Elsewhere** A call on a bridged appearance button matched to the call appearance has been put on hold. Calls on a call appearance that are put on hold by another user will continue to show connected lamp status, though the phone display will indicate a held call.
CA1 Icon flashes off.	 Red off, Green broken flash.	**Inaccessible** The button pressed is not accessible. The call is still dialing, ringing or cannot be bridged into.

Related Links

Call Appearance Buttons on page 782

Bridged Appearance Buttons

A bridged appearance button shows the state of one of another user's call appearance buttons. It can be used to answer or join calls on that user's call appearance button. It can also be used to make a call that the call appearance user can then join or retrieve from hold.



When the user's call appearance button alerts, any associated bridged appearance buttons on other user's phones also alert. The bridged appearance buttons can be used to answer the call on the call appearance button user's behalf.

When the call appearance button user answers or makes a call, any associated bridged appearance buttons on other users' phones show the status of the call, ie. active, on hold, etc. The bridged appearance button can be used to retrieve the call if on hold or to join the call if active (subject to intrusion permissions).

Note Bridged appearance buttons are different from the action of bridging into a call (joining a call). See Joining Other Calls (Bridging).

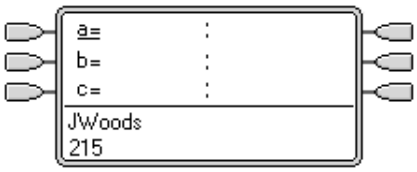
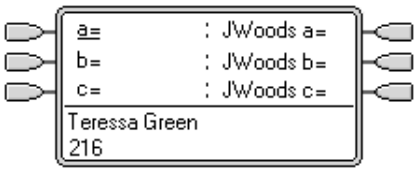
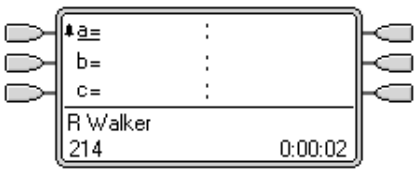
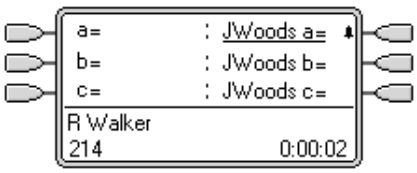
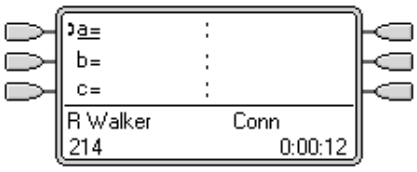
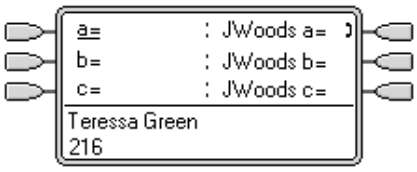
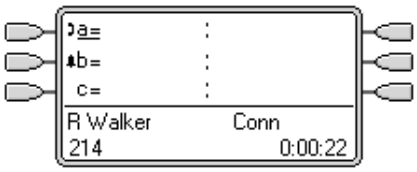
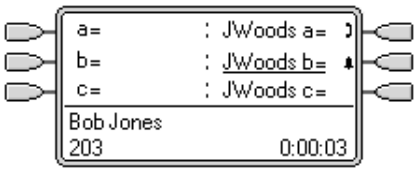
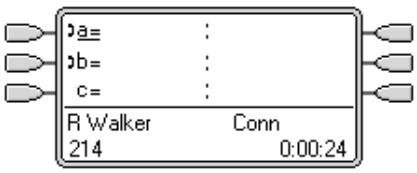
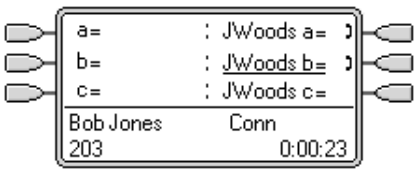
Bridged appearance buttons are not supported between users on different systems in a multi-site network.

Related Links

Appeance Button Operation on page 780
Bridged Appearance Example 1 on page 787
Bridged Appearance Example 2 on page 788
Bridged Appearance Example 3 on page 789
How are Bridged Appearances Treated? on page 790
Bridged Appearance Button Indication on page 791

Bridged Appearance Example 1

In this example, one user is able to see the status of the other user's call appearances, and when necessary answer calls for the other user. Both users have **Ringing Line Preference** and **Auto Hold** on.

Call Appearance User	Bridged Appearance User	
		**Both Phone Idle** Our user has bridged appearance buttons that match a colleague's call appearances buttons.
		**First Call** The colleague has a call alerting on their first call appearance button. It also alerts on our user's first bridged appearance button.
		**Call Answered** The colleague has answered the call. The bridged appearance indicates 'in use elsewhere'.
		**Second Call** Another call alerts at the colleagues phone and again is mirrored on our user's second bridged call appearance button.
		**Call Answered** Our user has gone off hook and answered the incoming call alerting on the bridged call appearance.

Related Links

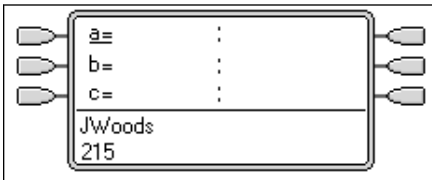
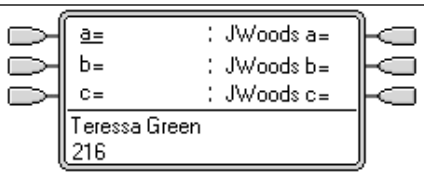
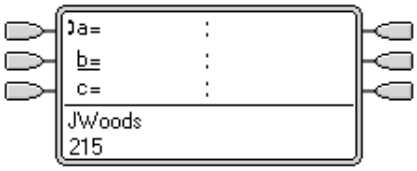
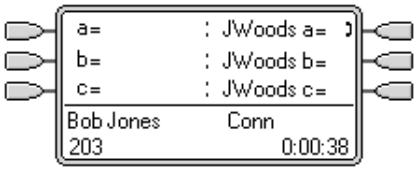
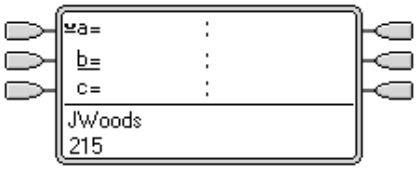
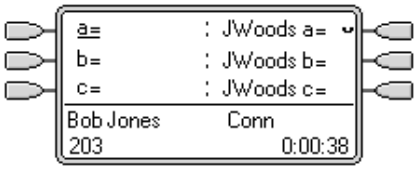
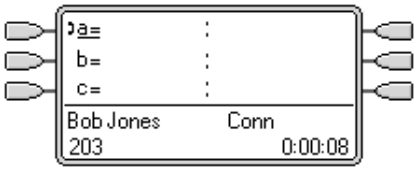
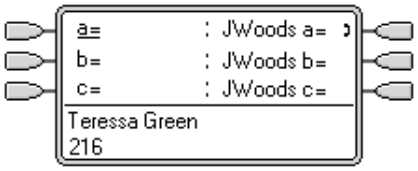
Bridged Appearance Buttons on page 787

Bridged Appearance Example 2

In this example, the bridged appearance user makes a call on behalf of the call appearance user. Once the call is connected, they put it on hold. The call appearance user is able to take the call off hold using their call appearance button. Both users have **Ringing Line Preference** and **Auto Hold** on.

Call Appearance User	Bridge Appearance User	
		Both Phones Idle Our user has bridged appearance buttons that match a colleague's call appearances buttons.

Table continues…

		
		**Bridged User Makes Call** Our user has pressed a bridged appearance and made a call on it. The matching call appearance shows 'in use elsewhere'.
		**Call Put on Hold** Having made the call, the bridged user puts it on hold. The matching call appearance indicates 'on hold elsewhere'.
		**Call Taken Off Hold** By pressing the call appearance, the first user has answered the held call. The bridged appearance user returns to idle.

Related Links

Bridged Appearance Buttons on page 787

Bridged Appearance Example 3

In this example, a call is passed from the call appearance user to the bridged appearance user. Both users have **Ringing Line Preference** and **Auto Hold** on.

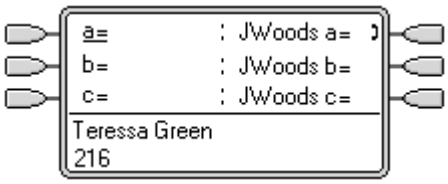
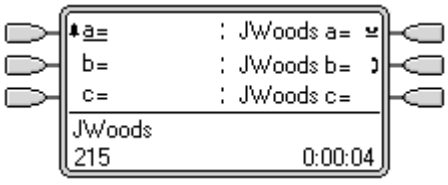
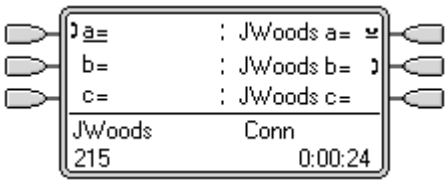
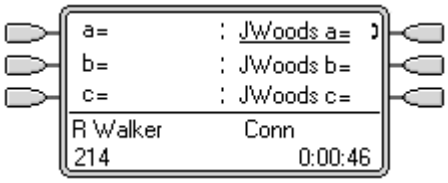
Bridged Appearance User	**Call on Colleague's Phone** The call appearance user has answered a call on one of their call appearances. The bridged appearance user's matching bridged appearance shows 'in use elsewhere'.
	
	**Call Held by Colleague** The call appearance user has put the call on hold and called the bridged appearance user. The first bridged call appearance shows a call 'on hold elsewhere' whilst the second matches the call between users.

Table continues…

	**Enquiry Call Between Colleagues** By going off hook, the bridged appearance user has answered the call from the call appearance user. They are asked to pickup the call on the colleagues first call appearance.
	**Call Taken Off Hold** Pressing the first bridged appearance button takes that call off hold and connects it to the bridged appearance user. In this example, **Auto Hold** is not set for the system, so pressing the bridged appearance button disconnected the call from the colleague. If **Auto Hold** had been set, the colleague's call would have been put on hold until they hung up.

Related Links

Bridged Appearance Buttons on page 787

How are Bridged Appearances Treated?

Bridged appearance buttons operate in parallel with their matching call appearance button.

Whose user settings control the call ? Until answered on a bridged appearance button, calls alerting on a bridged appearance button follow the settings of the user or hunt group to which the call was originally directed.

If the call appearance is in use, any matching bridged appearance will indicate the same.

If a bridged appearance is in use, the call appearance it matches will indicate the same.

The bridge appearance will only alert if the call appearance is alerting. For example, direct intercom and paging call to the call appearance will show on the bridged appearance but will not give any audible alert.

If the bridged appearance user put the call on hold, the call appearance will indicate 'on hold elsewhere'.

Bridged appearances to a user who has logged out, or has logged into a non-multi line phone, will not operate.

If the bridged appearance user has 'do not disturb' (DND) enabled, the bridge appearance button icon or lamps will still operate but alerting and ringing line preference selection are not applied unless the caller is in their DND exception list.

Bridged appearance buttons are not supported between users on different systems in a multi-site network.

Related Links

Bridged Appearance Buttons on page 787

Bridged Appearance Button Indication

On phones with a text display area next to the button, the name of the bridged user and the label from the bridged user's call appearance key are displayed.

The following table shows how the different states of bridged appearance buttons (alerting, held, etc) are indicated. This is a general table, not all phone button types are covered. The ring that accompanies the visual indication can be delayed or switched off. See Ring Delay.

Icon Button	Dual LED Button	Bridge Appearance Button State
JWoods CA1	 Red off, Green off.	**Idle** The bridged appearance is not in use.
JWoods CA1 Flashing icon.	 Red off, Green steady flash.	**Alerting** The matching call appearance is alerting for an incoming call. This is accompanied by ringing. If the user is already on a call, only a single ring is given.
JWoods CA1 Flashing icon.	 Red on, Green steady flash.	**Alerting + Selected** As above but Ringing Line Preference has made this the user's current selected button.
JWoods CA1	 Red off, Green on.	**In Use Elsewhere** The matching call appearance button is in use.
JWoods CA1	 Red on, Green on.	**In Use Here** The user has made a call or answered a call on the bridged appearance, or bridged into it.
JWoods CA1	 Red off, Green fast flash.	**On Hold Here** The call has been put on hold by this user.
JWoods CA1	 Red off, Green intermittent flash.	**On Hold Elsewhere** The call on that call appearance has been put on hold by another user.
JWoods CA1 Icon flashes off.		**Inaccessible** The button pressed is not usable. The call is still

Table continues…

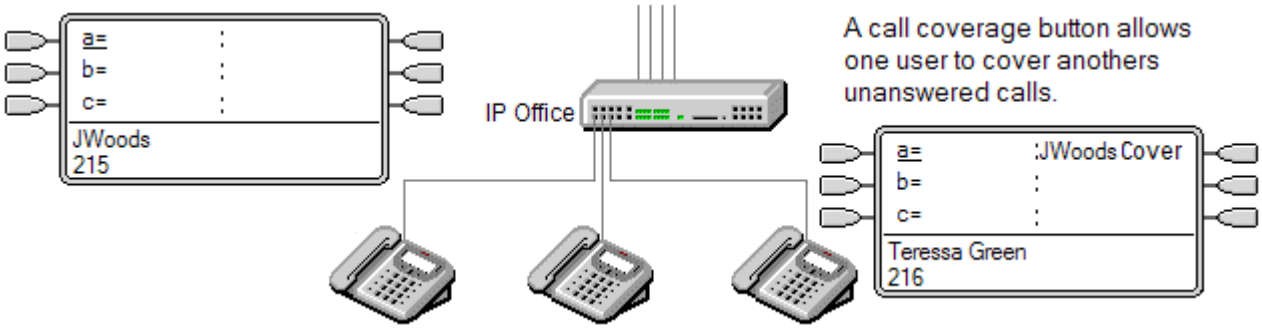
	Red off, Green broken flash.	dialing, ringing or cannot be bridged into.

Related Links

Bridged Appearance Buttons on page 787

Call Coverage Buttons

Call coverage allows a user to be alerted when another user has an unanswered call.



The user being covered does not necessarily have to be a key and lamp user or have any programmed appearance buttons. Their Individual Coverage Time setting (default 10 seconds) sets how long calls will alert at their extension before also alerting on call coverage buttons set to that user.

The user doing the covering must have appearance buttons including a call coverage appearance button programmed to the covered users name.

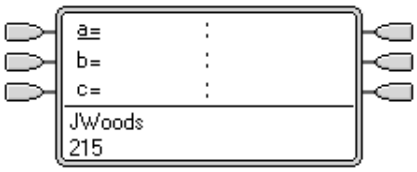
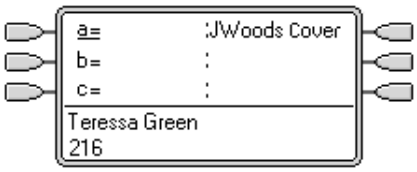
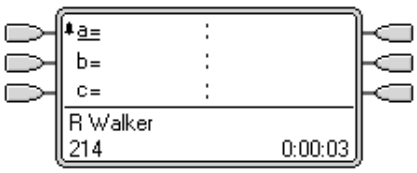
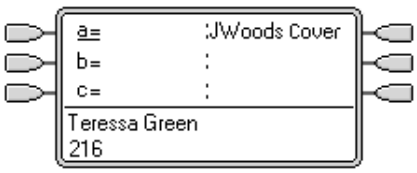
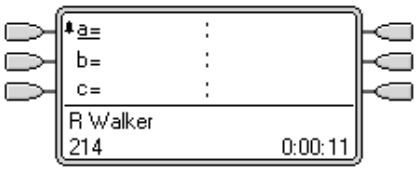
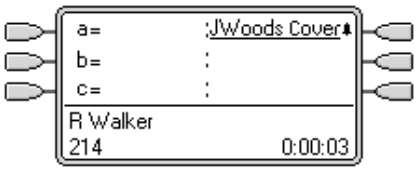
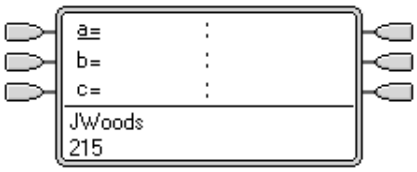
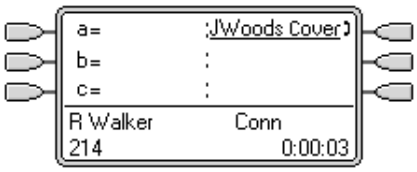
Call coverage appearance buttons are not supported between users on different systems in a multi-site network.

Related Links

Appeance Button Operation on page 780
Call Coverage Example 1 on page 792
Call Coverage Example 2 on page 793
How is Call Coverage Treated? on page 794
Call Coverage Button Indication on page 795

Call Coverage Example 1

In this example, the covering user is able to answer their colleagues call when it rings unanswered. Both users have **Ringing Line Preference** and **Auto Hold** on.

Covered User	Covering User	
		**Both Phones Idle** Our user has a call coverage button to cover their colleague.
		**Call to Covered User** A call arrives for the covered user.
		**Call Alerts to Coverage** After ringing for the covered user's Individual Coverage Time, the call also begins alerting on the call coverage button .
		**Covering User Answers** By going off hook or pressing the alerting button, the covering user has answered the call.

Related Links

Call Coverage Buttons on page 792

Call Coverage Example 2

In this example, the covered user has calls on all their available call appearances. Both users have **Ringing Line Preference** and **Auto Hold** on.

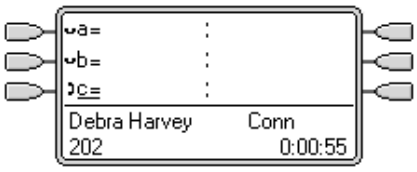
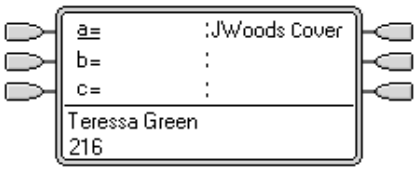
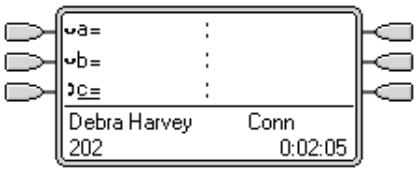
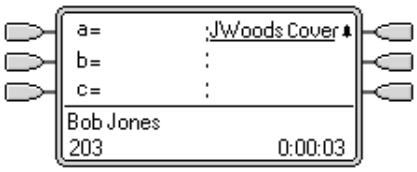
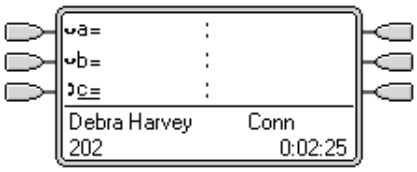
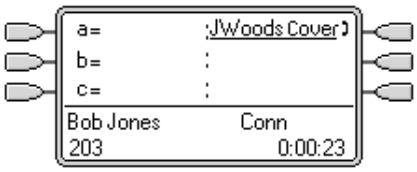
Covered User	Covering User	
		**Calls in Progress** The covered user already has a number of calls in progress on all their call appearance keys.
		**Call Alerts to Coverage** The covered user is treated as busy, so their next call goes immediately to call coverage.

Table continues…

		**Covering User Answers** The covering user has answered the call.

Related Links

Call Coverage Buttons on page 792

How is Call Coverage Treated?

Whose user settings control the call ?

Until answered, calls alerting on a call coverage button follow the settings of the user to which the call was originally directed.

Once answered, the call follows the user settings of the user who answered it.

Coverage is applied to :

- Internal calls dialed to the covered user's extension number.
- External calls routed to the covered user by a incoming call route.
- Calls forwarded internally by the covered user or on follow me from the covered user.

Coverage is not applied to :

- Hunt group calls to a hunt group of which the covered user is a member.
- Calls forwarded to the covered user using forward or follow me functions.
- Calls alerting on the covered user's bridged appearance and call coverage buttons.
- Coverage is only applied to calls alerting on a line appearance if the call was also routed to that user by an incoming call route.
- Page and intercom calls.
- Parked, transferred and held calls ringing back to the user.
- Automatic callback calls set by the covered user.
- Voicemail ringback calls.
- Call coverage appearance buttons are not supported between users on different systems in a multi-site network.

Coverage is applied :

- If the covered user's phone is available, call coverage is applied only after the covered user's Individual Coverage Time has expired.
- If the covered user's phone is busy, call coverage is applied immediately.
- If the covered user is using follow me or forward all to an internal number to divert their calls, call coverage is still applied.

- If the covered user has 'do not disturb' on, call coverage is applied immediately except for calls from numbers in the covered user's do not disturb exceptions list.

Other items :

If the call is not answered after the covered user's **No Answer Time** it will go to the covered user's voicemail if available or follow their forward on no answer settings.

If the covered user has several alerting calls, the call answered by the call coverage button is the covered user's longest ringing call.

Calls will not alert at a covering user who has 'do not disturb' enabled, except when the calling number is in the covering user's do not disturb exception list.

Related Links

Call Coverage Buttons on page 792

Call Coverage Button Indication

On phones with a text display area next to the button, the name of the covered user is displayed followed by the word **Cover**.

When the user is not connected to a call, the button indicated as selected is the button that will be used if the user goes off hook without pressing an appearance button. When a user is connected to a call, that call is the selected button.

The following table shows how the different states of call coverage appearance buttons (alerting, held, etc) are indicated. This is a general table, not all phone button types are covered. The ring that accompanies the visual indication can be delayed or switched off. See Ring Delay.

Icon Button	Dual LED Button	Call Coverage Button State
JWoods Cover	 Red off, Green off.	**Idle** The button is not in use.
JWoods Cover Flashing icon.	 Red off, Green steady flash.	**Alerting** The call coverage is alerting for an unanswered call at the covered user's phone. This is accompanied by ringing. If the user is already on a call, only a single ring is given.
JWoods Cover Flashing icon.	 Red on, Green steady flash.	**Alerting + Selected** As above but Ringing Line Preference has made this the user's current selected button.

Table continues…

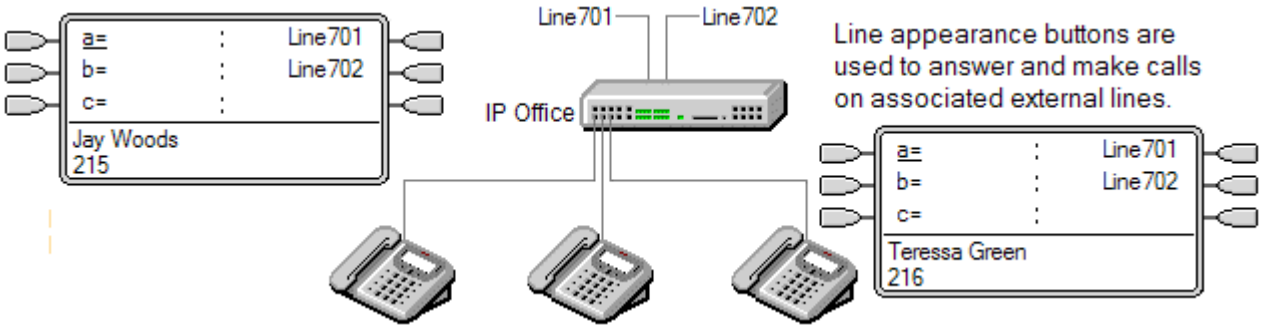
JWoods Cover	 Red on, Green on.	**In Use Here** The user has answered the call requiring coverage.
JWoods Cover	 Red off, Green fast flash.	**On Hold Here** The covered call has been put on hold by the call coverage button user.

Related Links

Call Coverage Buttons on page 792

Line Appearance Buttons

Line appearance buttons allow specific individual line to be used when making calls or answered when they have an incoming call. It also allows users to bridge into calls on a particular line.



Incoming call routing is still used to determine the destination of all incoming calls. Line appearance buttons allow a call on a specific line to alert the button user as well as the intended call destination. When these are one and the same, the call will only alert on the line appearance but can still receive call coverage.

When alerting on suitable phones, details of the caller and the call destination are shown during the initial alert.

Individual line appearance ID numbers to be assigned to selected lines on a system. Line appearance buttons are only supported for analog, E1 PRI, T1, T1 PRI, and BRI PSTN trunks; they are not supported for other trunks including E1R2, QSIG and IP trunks.

Line appearance buttons are not supported for lines on remote systems in a multi-site network.

Using Line Appearances for Outgoing Calls In order to use a line appearance to make outgoing calls, changes to the normal external dialing short codes are required. For full details see Outgoing Line Programming.

Private Lines Special behaviour is applied to calls where the user has both a line appearance for the line involved and is also the Incoming Call Route destination of that call. Such calls will alert only

on the Line Appearance button and not on any other buttons. These calls will also not follow any forwarding.

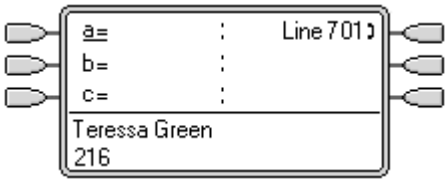
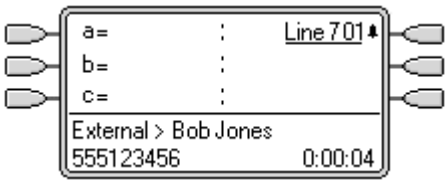
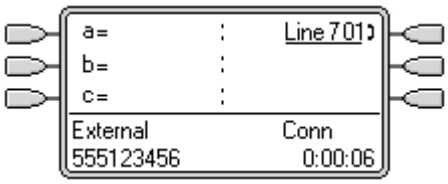
T3 Phone Line Appearances Line appearances are supported on T3 and T3 IP phones, see T3 Phone Line Appearances.

Related Links

Appeance Button Operation on page 780
Line Appearance Example 1 on page 797
Line Appearance Example 2 on page 798
How are Line Appearances Treated? on page 798
Line Appearance Button Indication on page 800
T3 Phone Line Appearances on page 801

Line Appearance Example 1

In this example, the user is able to answer a call alerting on a particular line.

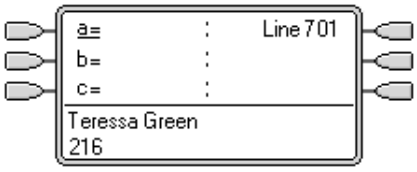
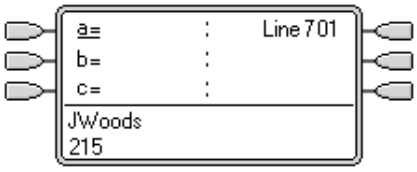
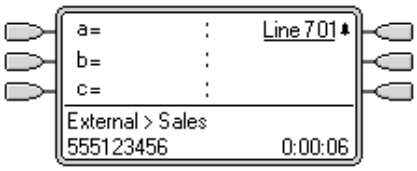
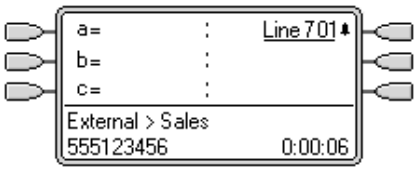
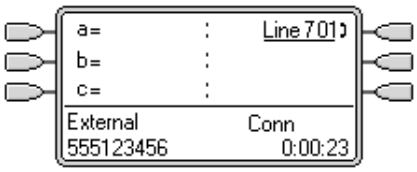
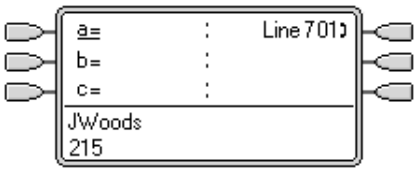
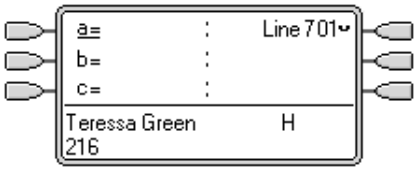
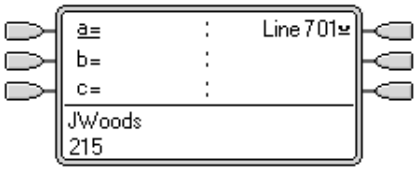
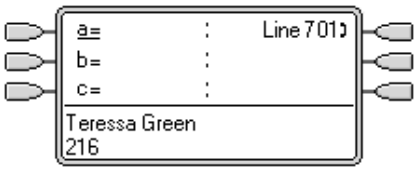
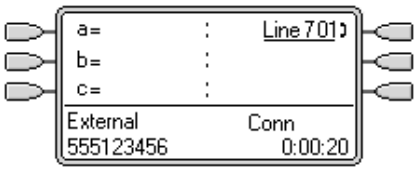
	**Line Goes Active** A call is active on the line with line ID number 601. This is indicated as 'in use elsewhere'. For an incoming call, the line will show active but will not alert until call routing has been determined. On analog ICLID lines, alerting is delayed until the ICLID that might be used to do the call routing has been received.
	**Line Appearance Alerting** The routing of the call has been complete and it is ringing against its destination. On our user's phone the line appearance also alerts and ringing line preference has made it the current selected button.
	**Answer Call** By going off hook or pressing the line appearance, our user has answered the call on that line.

Related Links

Line Appearance Buttons on page 796

Line Appearance Example 2

In this example, two users exchange a call using line appearance buttons set to the same line. Note that this requires that the user who first answers the call to have **Cannot be Intruded** off. Both users have **Ringing Line Preference** and **Auto Hold** on.

		**Idle** The two users has line appearances for the same line.
		**Call Alerts** A call arrives. Either user can answer it by pressing the alerting line appearance
		**Call Answered** The first user has answer the call.
		**Line Held** The first user has put the call on hold.
		**Line Retrieved** The second user has retrieved the held call by pressing the line appearance.

Related Links

Line Appearance Buttons on page 796

How are Line Appearances Treated?

Incoming Calls

Until answered using a line appearance button, incoming calls alerting on a line appearance, follow the settings of the incoming call route's destination group or user. They do not follow the settings of any line appearance user.

If an incoming calls destination is voicemail, or once the incoming call has passed from its destination to voicemail, it cannot be answered or bridged into using a line appearance button.

If the line appearance user is also the incoming call route destination for the call, the call will alert on their line appearance only. In this case:

- It will alert on the line appearance even if all call appearances are in use.
- The call will not follow any of the user's forwarding settings .
- The call will receive call coverage from other user's with call coverage buttons set to the line appearance user.
- The ring delay used is that of the first free call appearance.

For analog lines set to ICLID, any line appearances show active while the system waits for ICLID information. During this time the line has not been routed and cannot be answered using a line appearance button.

Calls alerting on a line appearance can also alert on a call coverage appearance on the same phone. If Ringing Line Preference is set, the current selected button will change from the line appearance to the call coverage appearance.

If the line appearance user has do not disturb (DND) enabled, the line appearance button icon or lamps will still operate but alerting and ringing line preference selection are not applied unless the caller is in their DND exception list.

Outgoing Calls

In order to be used for making outgoing calls, some additional system programming may be required. See Outgoing Line Programming.

Calls made on a call appearance, which are routed out on a line for which the user also has a line appearance, will remain on the call appearance. The line appearance will indicate 'in use elsewhere'.

Additional Notes

Calls alerting on a line appearance do not receive call coverage or go to a users voicemail unless the user was the call's original incoming call route destination.

If a call indicated by a line appearance is parked, it cannot be joined or unparked by using another line appearance.

Where a line appearance button is used to answer a call for which automatic call recording is invoked, the recording will go to the automatic recording mailbox setting of the original call destination.

Line appearance buttons are not supported for lines on remote systems in a multi-site network.

Related Links

Line Appearance Buttons on page 796

Line Appearance Button Indication

On phones with a text display area next to the button, the label **Line** and the line number are displayed.

When the user is not connected to a call, the button indicated as selected is the button that will be used if the user goes off hook without pressing an appearance button. When a user is connected to a call, that call is the selected button.

The following table shows how the different states of line appearance buttons (alerting, held, etc) are indicated. This is a general table, not all phone button types are covered. The ring that accompanies the visual indication can be delayed or switched off. See Ring Delay.

Icon Button	Dual LED Button	Line Appearance Button State
Line 601	 All off.	**Idle** The associated line is not in use.
Line 601		**Idle + Selected** The associated line is not in use but the button is the user currently selected button.
Line 601 Flashing icon.	 Red off, Green steady flash.	**Alerting** The line is ringing at its incoming call route destination. This is accompanied by ringing. If the user is already on a call, only a single ring is given.
Line 601 Flashing icon.	 Red on, Green steady flash.	**Alerting + Selected** As above but Ringing Line Preference has made this the user's current selected button.
Line 601	 Red off, Green on.	**In Use Elsewhere** The line is in use.
Line 601	 Red on, Green on.	**In Use Here** The user has answered the line, made a call on it or bridged into the call on the line.
Line 601	 Red off, Green fast flash.	**On Hold Here** The call on the line has been put on hold by this user.
Line 601	 Red off, Green intermittent flash.	**On Hold Elsewhere** The call on the line has been put on hold by another appearance button user.
Line 601 Icon flashes off.	 Red off, Green broken flash.	**Inaccessible** The button pressed is not accessible. The call is still dialing, ringing, routing or cannot be bridged into.

Related Links

Line Appearance Buttons on page 796

T3 Phone Line Appearances

Release 4.2+: Line appearances are supported on T3 and T3 IP phones. As these phones do not support call appearance, bridge appearance or call coverage appearance buttons the user can be programmed with just line appearance buttons.

Soft Key	LED Key	Line Appearance Button State
L601	Off	**Idle** The associated line is not in use.
✓ **601**	Off	**Idle + Selected** The associated line is not in use but the button is the user currently selected button.
L601 alternating with bell symbol.	Fast flashing	**Alerting** The line is ringing at it incoming call route destination. This is accompanied by ringing. If the user is already on a call, only a single ring is given.
L601 alternating with bell symbol.	Fast flashing	**Alerting + Selected** As above but Ringing Line Preference has made this the user's current selected button.
L601	On	**In Use Elsewhere** The line is in use.
✓ **601**	On	**In Use Here** The user has answered the line, made a call on it or bridged into the call on the line.
L601 Slow flash	Slow flash	**On Hold Here** The call on the line has been put on hold by this user.
L601 Slow flash	Slow flash	**On Hold Elsewhere** The call on the line has been put on hold by another appearance button user.
-601	Off	**Inaccessible** The button pressed is not accessible. The call is still dialing, ringing, routing or cannot be bridged into. A single tone is also given.

Notes

Hot Desking The following applies to appearance button programmed for a user on a system with T3 phones.

- **From a T3 Phone** If a T3 user with programmed line appearances but no programmed call appearances hot desks onto a phone type that requires call appearances, the phone will not operate correctly. This configuration is not supported by Avaya.
- **To a T3 Phone** If appearance buttons other than line appearance are programmed for a user, when that user in on a T3 phone those other appearance buttons will be treated as blank. Depending on the button and type of T3 phone the button may assume its default T3 phone function. See T3 Compact, T3 Classic and T3 Comfort.

Call Waiting Line appearances will ignore the T3 phones user selected call waiting setting. So with a call connected and call waiting off, calls can still alert on line appearances.

Multiple Calls T3 phones are limited to a maximum of 6 associated calls at any time, including calls connected, on hold and alerting.

Delayed Ringing The only Ring Delay options supported are Immediate or No Ring. Any other delayed

Preference Idle line preference is always used, however T3 phones will never default to using a line appearance for an outbound call.

Joining/Bridging Joining a call active on a line appearance is supported. This is subject to the intrusion settings of the users involved. The call then becomes a conference call.

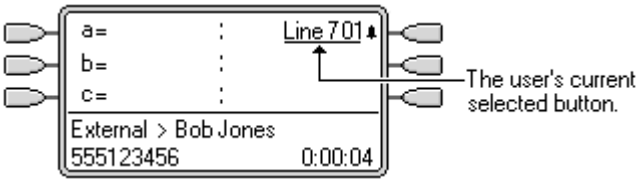
Related Links

Line Appearance Buttons on page 796

Selected Button Indication

During appearance button usage, one of the user's appearance buttons may be indicated as the user's current selected button. This is the appearance button already in use, or if idle, the appearance button that will be used if the user goes off hook by lifting the handset.

On phones with a display area next to each button, the current selected button is indicated by either an _ underscore of the button label, a * star or a shaded background.



On phones with twin LED lamps, the current selected button is indicated by the red lamp being on

.

On Transtalk 9040 phones, the current selected button is indicated by a ◂ icon.

The system sets which appearance button is the current selected button using the following methods:

- Idle Line Preference This feature can be set on or off for each individual user, the default is on. When on, it sets the current selected button as the first available idle call/line appearance button. See Idle Line Preference.
- Ringing Line Preference This feature can be set on or off for each individual user, the default is on. When on, it sets the current selected button as the button which has been alerting at the users phone for the longest. Ringing Line Preference overrides Idle Line Preference. See Ringing Line Preference.
- Delayed Ring Preference: This setting is used in conjunction with ringing line preference and appearance buttons set to delayed or no ring. It sets whether ringing line preference should observe or ignore the delayed ring applied to the user's appearance buttons when determining which button should have current selected button status.
- **User Selection** The phone user can override both **Idle Line Preference** and **Ringing Line Preference** by pressing the appearance button they want to use or answer. That button will then remain the current selected button whilst active.

  If the user currently has a call connected, pressing another appearance button will either hold or disconnect that call. The action is determined by the system's Auto Hold setting.

Answer Pre-Select: Normally when a user has multiple alerting calls, only the details of the call on current selected button are shown. Pressing any of the alerting buttons will answer the call on that button, going off-hook will answer the current selected button. Enabling the user telephony setting **Answer Pre-Select** allows the user to press any alerting button to make it the current selected button and displaying its call details without answering that call. To answer a call when the user has **Answer Pre-Select** enabled, the user must press the alerting button to display the call details and then either press the button again or go off-hook.

Related Links

Appeance Button Operation on page 780

Idle Line Preference

Idle Line Preference determines the user's currently selected button as the first available idle call/line appearance button. Selected button indication is applied to that button and if the user goes off-hook, for example by lifting their handset, an outgoing call is started on that button.

Idle Line Preference is overridden by **Ringing Line Preference** if also on for the user.

By default **Idle Line Preference** is on for all users.

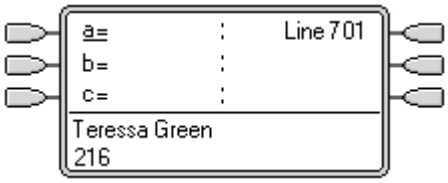
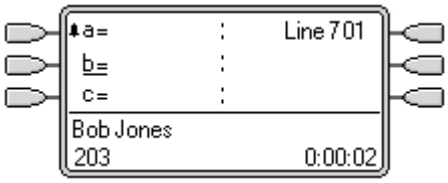
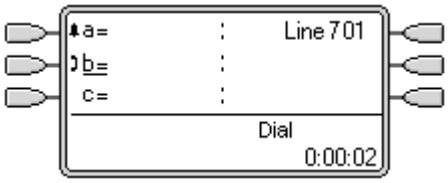
For appearance button users with **Idle Line Preference** off, going off-hook (lifting the handset or pressing **SPEAKER**, **HEADSET**, etc) will have no effect until an appearance button is pressed.

If all the available call/line appearance buttons are in use, no current selected button choice is made by **Idle Line Preference**. In this case, going off hook will have no effect.

?Why Would I Use Just Idle Line Preference In environments that are focused on making outgoing calls, for example telemarketing, incoming calls are infrequent and user's go off-hook expecting to make a call. Using **Idle Line Preference** without **Ringing Line Preference** ensures that the user doesn't inadvertently answer a call when expecting to make a call.

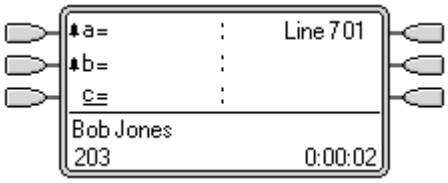
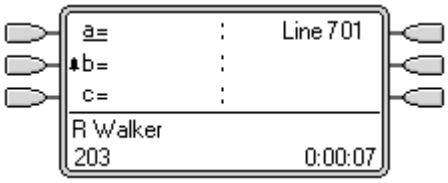
Idle Line Preference Example 1

In this example, only **Idle Line Preference** has been programmed for the user. **Ringing Line Preference** has not been programmed.

	**Phone Idle** The phone is idle. The current selected button determined by Idle Line Preference is the first available idle call appearance button. This is shown by the _ underscore of the button text.
	**First Call to User** A call for the user arrives. It alerts on the first available call appearance button. Idle Line Preference has changed the current selected button to the next available idle call appearance.
	1. **User Goes Off Hook** With the call still alerting, if the user goes off hook, it will be interpreted as making a call using the currently selected button, not as answering the alerting button. 2. To answer the alerting call, the user should press the alerting button.

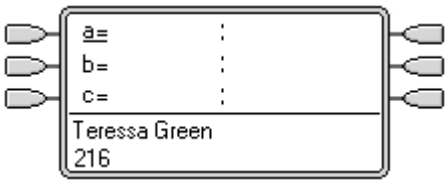
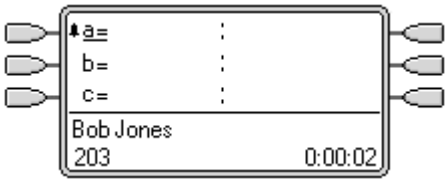
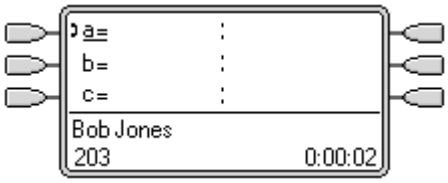
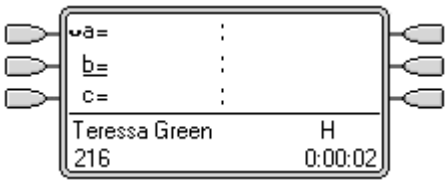
Idle Line Preference Example 2

In this example, only **Idle Line Preference** has been programmed for the user. **Ringing Line Preference** has not been not programmed.

	**Two Calls Alerting** The users has two incoming calls alerting. Idle Line Preference has set the currently selected button to their third call appearance.
	**First Caller Abandons** If the first incoming caller disconnects, the currently selected button changes to the first call appearance as this is now the first available idle call appearance button.

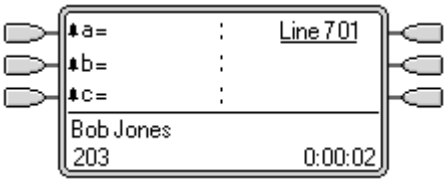
Idle Line Preference Example 3

In this example, both **Idle Line Preference** and **Ringing Line Preference** are set for the user.

	**Phone Idle** The phone is idle and **Idle Line Preference** has assigned current selected button to the first call appearance.
	**Call Alerting** A call has arrived and **Ringing Line Preference** keeps the current selected button at the first call appearance.
	**Call Answered** With the call answered it retains current selected button status.
	**Call Held** When the call is put on hold, **Idle Line Preference** assigns current selected button status to the next available call appearance button.

Idle Line Preference Example 4

In this example, only **Idle Line Preference** has been programmed for the user. **Ringing Line Preference** has not been programmed.



All Call Appearances Alerting In this case, all the users call appearance buttons are alerting incoming calls. Idle Line Preference has changed the currently selected button to the first available line appearance.

Related Links

Appeance Button Operation on page 780

Ringing Line Preference

Ringing Line Preference determines the user's currently selected button as the button which has been alerting the longest. Selected button indication is applied to that button and if the user goes off-hook, for example by lifting their handset, the alerting call on that button is answered.

Ringing Line Preference includes calls alerting on call appearance, line appearance, bridged appearance and call coverage buttons.

Ringing Line Preference overrides **Idle Line Preference**.

By default **Ringing Line Preference** is on for all users.

Ringing Line Preference Order When a user's longest waiting call alerts on several of the user's appearance buttons and Ringing Line Preference is set for the user, the order used for current selected button assignment is;

Call appearance.

Bridged appearance.

Call coverage.

Line appearance.

Example: A user has a call to a covered user alerting initially on a line appearance button. Ringing Line Preference assigns current selected button status to the line appearance. When the same call also begins to alert on the call coverage appearance button, current selected button status switches to the call coverage appearance button.

Ring Delay and Ringing Line Preference Appearance buttons can be set to **Delayed Ring** or **No Ring**. These buttons still alert visually but do not give an audible ring or tone. Ringing line preference is still applied to alerting buttons even if set to **Delayed Ring** or **No Ring**.

Delayed Ring Preference For users with **Ringing Line Preference** selected, their **Delayed Ring Preference** setting sets whether ringing line preference is used or ignores buttons that are visually alerting but have **Delayed Ring** or **No Ring** set. The default is off, ie. ignore ring delay.

Ringing Line Preference Example 1

In this example, both **Ring Line Preference** and **Idle Line Preference** have been set for the user. They also have **Ringing Line Preference** on and **Auto Hold** is on. **Answer Pre-Select** is off.

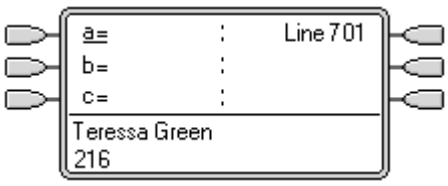
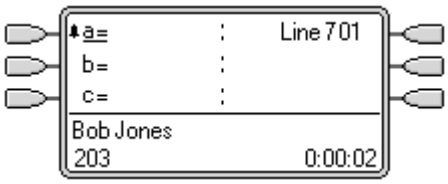
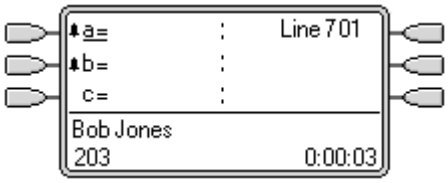
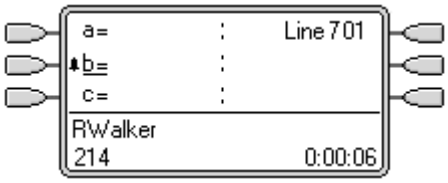
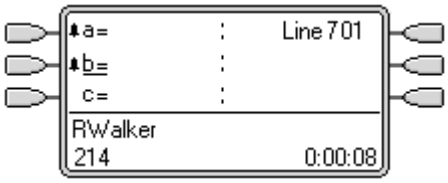
	**Phone Idle** The phone is idle. The current selected button has been determined by Idle Line Preference as the first available idle call appearance button. This is shown by the _ underscore next to that button.

Table continues…

	**First Call Alerting** A call for the user arrives. It alerts on the first available call appearance button. Ringing Line Preference uses this as the currently selected button as it is the only alerting call.
	**Second Call Alerting** Another call for the user arrives. It alerts on the next available call appearance button. As the first call has been alerting longer, under Ringing Line Preference it retains the currently select button status.
	**The First Call Abandons** The first caller disconnects. Ringing Line Preference changes the currently selected button status to the second call appearance button.
	**Another Call Arrives** Another call arrives. It alerts as the first free call appearance button. However the call at the second call appearance has been alerting longer and so under Ringing Line Preference retain the currently selected button status.

Ringing Line Preference Example 2

In this example, the user has both Ring Line Preference and Idle Line Preference programmed. They also have **Ringing Line Preference** on and **Auto Hold** is on. **Answer Pre-Select** is off.

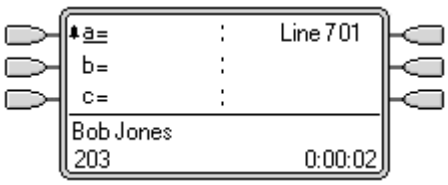
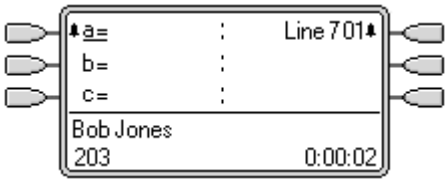
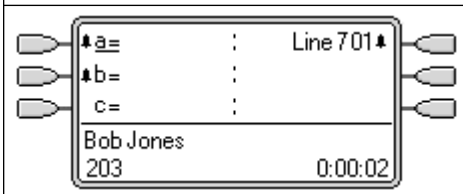
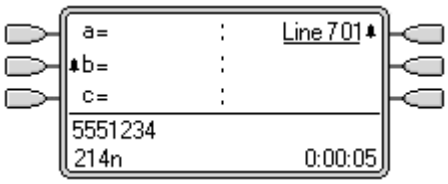
	**First Call to User** A call for the user arrives. It alerts on the first available call appearance button. Ringing Line Preference uses this as the currently selected button as it is the only alerting call.
	**Call on Line 601** The user's Line Appearance is alerting due to an incoming call on the associated line. Details of the call and its destination are shown. Ringing Line Preference keeps the currently selected button status on the call appearance button as this has been alerting longest.
	**Second Call to User** A second call to the user arrives and alerts on the second call appearance button. Ringing Line Preference keeps the currently selected button status on the call appearance button as this has been alerting longest.

Table continues…

	**The First Caller Abandons** The first call to the user disconnects. Ringing Line Preference passes the currently selected button status to the Line Appearance button as this has been alerting longest.

Related Links

Appeance Button Operation on page 780

Answer Pre-Select

On some phones, only the details of the call alerting or connected on the current selected button are shown. The details of calls alerting on other buttons are not shown or only shown briefly when they are first presented and are then replaced again by the details of the call on the current selected button.

By default, pressing any of the other alerting buttons will answer the call on that button. Answer pre-select allows a user to press alerting buttons other than the current selected button without actually answering them. Instead the button pressed becomes the current selected button and its call details are displayed.

Note that using answer pre-select with a currently connected call will still either hold or end that call in accordance with the system's Auto Hold setting.

Answer Pre-Select Example 1

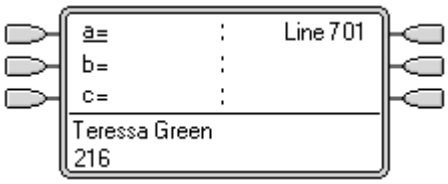
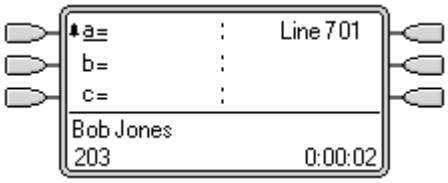
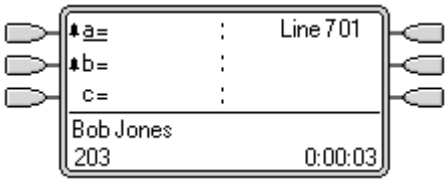
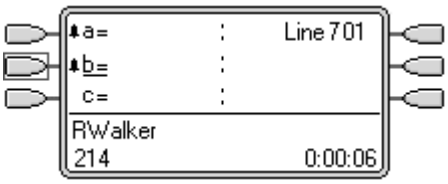
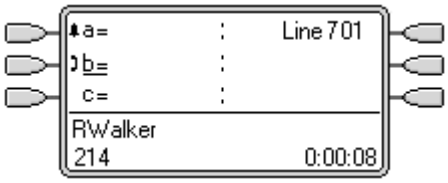
	**Phone Idle** The phone is idle. The current selected button has been determined by Idle Line Preference as the first available idle call appearance button. This is shown by the _ underscore next to that button.
	**First Call Alerting** A call for the user arrives. It alerts on the first available call appearance button. Ringing Line Preference uses this as the currently selected button as it is the only alerting call.
	**Second Call Alerting** Another call for the user arrives. It alerts on the next available call appearance button. As the first call has been alerting longer, under Ringing Line Preference it retains the currently select button status.

Table continues…

	**The User Presses the Second Call Appearance** Pressing the second call appearance overrides ringing line preference and assigns current selected button status to the button without actually answering the call. The details of the caller are displayed.
	**The User Answers the Call** The user can press the button again to answer the call or just go off-hook to answer as it is now the currently selected button.

Related Links

Appeance Button Operation on page 780

Auto Hold

Auto Hold is a system wide feature that affects all appearance button users. This feature determines what happens when a user, who is already on a call, presses another appearance button. The options are:

- If **Auto Hold** is **off**, the current call is disconnected.
- If **Auto Hold** is **on**, the current call is placed on hold.

On Release 4.0 and higher systems **Auto Hold** is **on** by default. On previous levels of system software the default for US was **off**.

Auto Hold Example 1

In this example, the user has two calls currently shown on call appearance buttons. **Answer Pre-Select** is off.

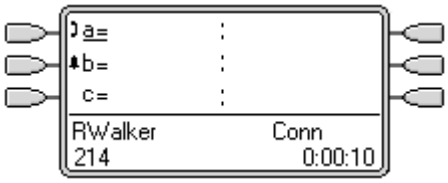
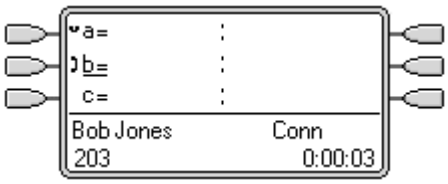
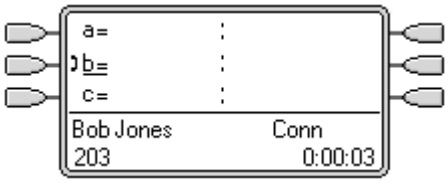
	1. This user has three call appearance buttons. They have answer one call and are still connected to it, shown by the icon. A second call is now alerting on their second call appearance button, shown by the icon. 2. What happens when the user presses the second call appearance key is determined by the system's **Auto Hold** setting:

Table continues…

	**Auto Hold On** When the second call appearance key is pressed, that call is answered and the first call is put on hold, shown by the ↵ icon. The user can switch between calls using the call appearance buttons and make/receive other calls if they have additional call appearance buttons
	**Auto Hold Off** When the second call appearance key is pressed, that call is answered and the first call is disconnected.

Related Links

Appeance Button Operation on page 780

Ring Delay

Ring delay can be applied to appearance buttons. This option can be used with all types of appearance buttons and can be selected separately for each appearance button a user has. Using ring delay does not affect the buttons visual alerting through the display and display icons or button lamps.

Ring delay is typically used with line appearance buttons for lines which a user wants to monitor but does not normally answer. However ring delay can be applied to any type of appearance button.

The selectable ring delay options for an appearance button are listed below. The option is selected as part of the normal button programming process.

Immediate Provide audible alerting as per normal system operation.

Delayed Ring Only provide audible alerting after the system ring delay or, if set, the individual user's ring delay.

No Ring Do not provide any audible alerting.

There are two possible sources for the delay used when delayed ringing is selected for a button.

System | Telephony | Telephony | Ring Delay: Default = 5 seconds, Range 1 to 98 seconds. This is the setting used for all users unless a specific value is set for an individual user.

User | Telephony | Multi-line Options | Ring Delay: Default = Blank (Use system setting), Range 1 to 98 seconds. This setting can be used to override the system setting. It allows a different ring delay to be set for each user.

Notes

Calls That Ignore Ring Delay Ring delay is not applied to hold recall calls, park recall calls, transfer return calls, voicemail ringback calls and automatic callback calls. For phones using Internal

Twinning, ring delay settings are not applied to calls alerting at a secondary twinned extension (except appearance buttons set to **No Ring** which are not twinned).

Auto Connect Calls Ring delay is applied to these calls before auto-connection. This does not apply to page calls.

Multiple Alerting Buttons Where a call is presented on more than one button on a user's phone, see Multiple Alerting Buttons, the shortest delay will be applied for all the alerting buttons. For example, if one of the alerting buttons is set to **Immediate**, that will override any alerting button set to **Delayed Ring**. Similarly if one of the alerting buttons is set to **No Ring**, it will be overridden if the other alerting button is set to **Immediate** or **Delayed Ring**.

Line Appearance Buttons Calls routed to a user that could potentially be presented on both a call appearance button and a line appearance button are only presented on the line appearance button. In this scenario, the ring delay settings used is that of the first free call appearance button.

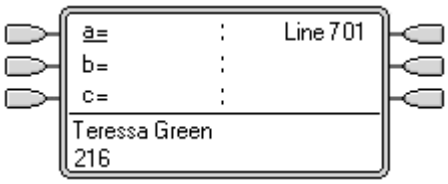
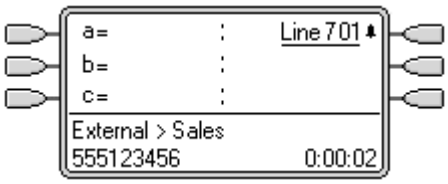
Delay on Analog Lines Analog lines set to Loop Start ICLID already delay ringing whilst the system waits for the full ICLID in order to resolve incoming call routing. In this scenario the ring delay operates in parallel to the routing delay.

Ring Delay and Ringing Line Preference Appearance buttons can be set to **Delayed Ring** or **No Ring**. However ringing line preference is still applied to alerting buttons even if set to **Delayed Ring** or **No Ring**.

The user's **Delayed Ring Preference** setting is used to determine whether ringing line preference is used with or ignores buttons that are alerting but have **Delayed Ring** or **No Ring** set.

Ring Delay Example 1

In this example, the user has a line appearance button set but configured to no ring.

	**Phone Idle** The phone is idle. The current selected button has been determined by Idle Line Preference as the first available call appearance button. This is shown by the _ underscore next to that button.
	**Incoming Call Alerting on the Line** An incoming call arrives on the line and begin to alert somewhere on the system. The user's line appearance button shows this visually but doesn't ring audibly. Ringing line preference would makes the line appearance the user's currently selected button and therefore they would answer the line if they went off-hook.

Related Links

Appeance Button Operation on page 780

Delayed Ring Preference

When a call is alerting at an idle phone, by default Ringing Line Preference sets the call as the currently selected button and if the user then goes off-hook they will answer that call.

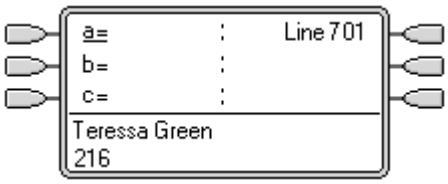
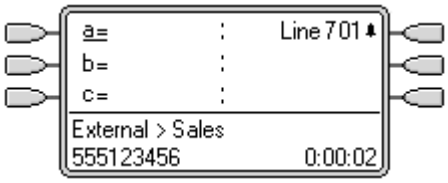
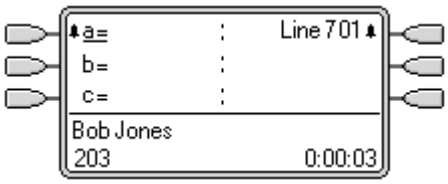
In most situations this is acceptable as the user hears ringing which informs them that there is a call waiting to be answered. If the user wants to make a call instead, they can press another call appearance button to go off-hook on that other button.

When ring delay is being used there can potentially be a problem if the user lifts the handset to make a call without looking at the display. If they do this while the a call is alerting silently on a button with ring delay, the user will actually answer the waiting call rather than get dial tone to make a call.

Once the call alerting on a button has currently selected call status, it retains that status even if a prior call on a button with ring delay applied comes out of its ring delay period.

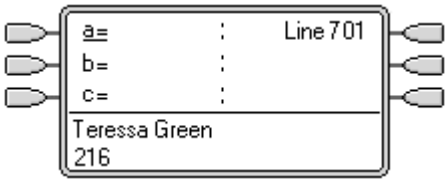
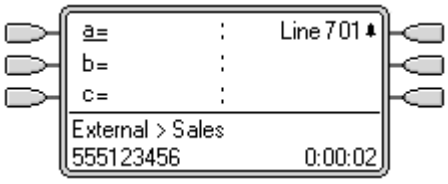
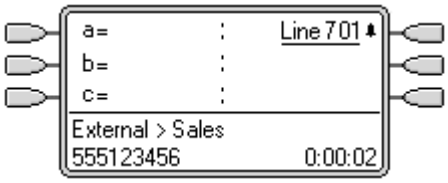
Delayed Ring Preference Example 1

In this example the user has a line appearance button for a line they monitor. This line appearance button has been set to no ring as the user occasionally need to use that line but does not normally answer calls on that line.

	**Phone Idle** The phone is idle. The current selected button has been determined by Idle Line Preference as the first available call appearance button. This is shown by the _ underscore next to that button.
	**Incoming Call Alerting on the Line** An incoming call arrives on the line and begin to alert somewhere on the system. The user's line appearance button shows this visually but doesn't ring audibly. Normally ringing line preference would make the line appearance the user's currently selected button and therefore they would answer the line if they went off-hook expecting to make a call. However, because **Delayed Ring Preference** is on for the user, ringing line preference is not applied and idle line preference makes their current selected button the first call appearance. If the user were to go off-hook they would be making a call on that call appearance.
	**Call Alerting for the User** A call for the user arrives. It alerts on the first available call appearance button. Ringing line preference is applied and makes that the users currently selected button. If the user goes off-hook now that will answer the call on the call appearance and not the line appearance.

Delayed Ring Preference Example 2

This is similar to the previous example except that the user and the line has been configured for a 15 second ring delay. This informs the users that the line has not been answered for some reason and allows them to answer it by just going off-hook.

	**Phone Idle** The phone is idle. The current selected button has been determined by Idle Line Preference as the first available call appearance button. This is shown by the _ underscore next to that button.
	**Incoming Call Alerting on the Line** An incoming call arrives on the line and begin to alert somewhere on the system. The user's line appearance button shows this visually but doesn't ring audibly. Because **Delayed Ring Preference** is on for the user, ringing line preference is not applied and idle line preference makes their current selected button the first call appearance. If the user were to go off-hook they would be making a call on that call appearance.
	**Call Continues Alerting** When the ring delay for the line appearance expires, if no other call has taken ringing line preference it becomes the current selected call and will be answered if the user goes off-hook.

Related Links

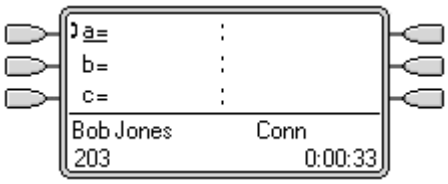
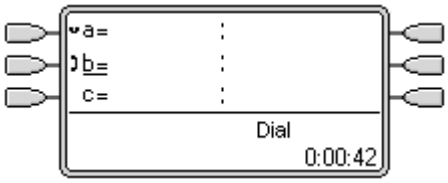
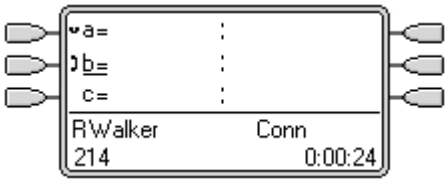
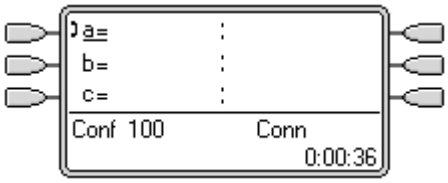
Appeance Button Operation on page 780

Collapsing Appearances

This topic covers what happens when a user with several calls on different appearance buttons, creates a conference between those calls. In this scenario, the call indication will collapse to a single appearance button and other appearance buttons will return to idle. The exception is any line appearance buttons involved which will show 'in use elsewhere'.

Collapsing Appearances Example 1

In this example, the user will setup a simple conference. **Ringing Line Preference** and **Idle Line Preference** are set for the user. **Auto Hold** for the system is on. **Answer Pre-Select** is off.

	**Initial Call** The user has a call in progress, shown on their first call appearance button. It is decided to conference another user into the call.
	**Make Conference Enquiry** Pressing the **CONFERENCE** button on the users phone automatically places the current call on hold and takes the phone off hook on the next available call appearance.
	**Enquiry in Progress** The other extension has answered and is invited to join a conference call. The user presses the **CONFERENCE** button on their phone again.
	**Conference Starts/Call Appearances Collapse** The conference call has started. The call appearances have collapsed to a single appearance.

Related Links

Appeance Button Operation on page 780

Joining Calls

Appearance buttons can be used to "join" existing calls and create a conference call. A user can join calls that are shown on their phone as 'in use elsewhere'.

This feature is often referred to as 'bridging into a call'. However this causes confusion with Bridged appearance buttons and so the term should be avoided.

The ability to join calls is controlled by the following feature which can be set for each user:

- **Cannot be Intruded**: Default = On If this option is set on for the user who has been in the call the longest, no other user can join the call. If that user leaves the call, the status is taken from the next internal user who has been in the call the longest. The exceptions are:
  - Voicemail calls are treated as **Cannot be Intruded** at all times.
  - When an external call is routed off switch by a user who then leaves the call, the **Cannot be Intruded** status used is that of the user who forwarded the call off switch.

- Any call that does not involve an internal user at any stage is treated as **Cannot be Intruded** on. For example:
  - When an external call is routed off switch automatically using a short code in the incoming call route.
  - multi-site network calls from other systems that are routed off-switch.
  - VoIP calls from a device not registered on the system.

- The **Can Intrude** setting is not used for joining calls using appearance buttons.

The following also apply:

Inaccessible In addition to the use of the **Cannot be Intruded** setting above, a call is inaccessible if:

- The call is still being dialed, ringing or routed.
- It is a ringback call, for example a call timing out from hold or park.
- If all the internal parties, if two or more, involved in the call have placed it on hold.
- **Conferencing Resources** The ability to bridge depends on the available conferencing resource of the system. Those resources are limited and will vary with the number of existing parties in bridged calls and conferences. The possible amount of conferencing resource depends on the system type and whether Conferencing Center is also installed.
- **Conference Tone** When a call is joined, all parties in the call hear the system conferencing tones. By default this is a single tone when a party joins the call and a double-tone when a party leaves the call. This is a system setting.
- **Holding a Bridged Call** If a user puts a call they joined on hold, it is their connection to the joined call (conference) that is put on hold. The other parties within the call remain connected and can continue talking. This will be reflected by the button status indicators. The user who pressed hold will show 'on hold here' on the button they used to join the call. All other appearance users will still show 'in use here'.
- **Maximum Two Analog Trunks** Only a maximum of two analog trunks can be included in a conference call.
- **Parked Calls** A Line Appearance button may indicate that a call is in progress on that line. Such calls to be unparked using a line appearance.

Joining Example 1: Joining with a Bridged Appearance

In this example, the user joins a call using a bridged appearance button. **Answer Pre-Select** is off.

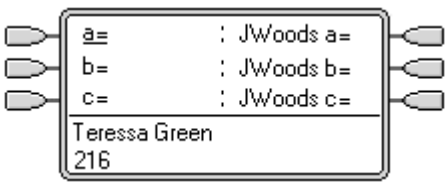
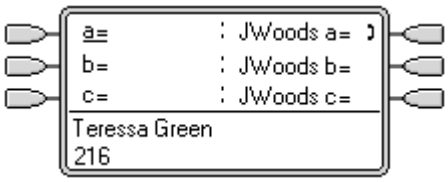
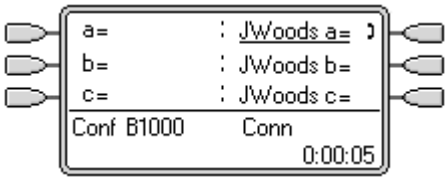
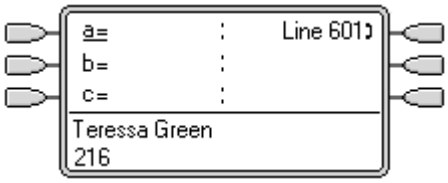
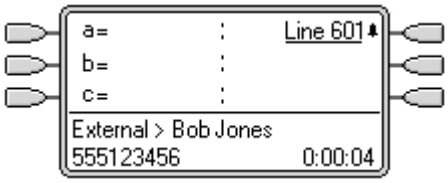
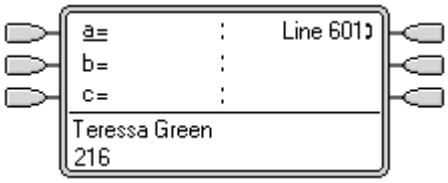
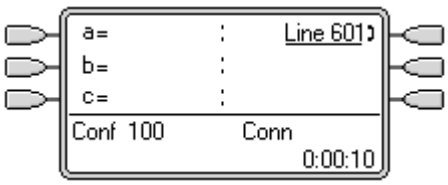
	**User with Bridged Appearance Buttons** The user has bridged appearance buttons that match their colleagues call appearance buttons.

Table continues…

	**Call on Bridged Appearance** The colleague has a call in progress on their first call appearance. This is matched on the first bridged appearance button.
	**User Joins the Call** Pressing the bridged appearance button will take our user off hook and join them into their colleagues call, creating a conference call.

Joining Example 2: Joining with a Line Appearance

In this example, the user joins a call by pressing a line appearance button. **Answer Pre-Select** is off.

	**Line Goes Active** A call is active on the line with line ID number 601. If this is an incoming call, it will show active but will not alert until its call routing has been determined. On ICLID analog lines, alerting is delayed until the ICLID that might be used to do that routing has been received.
	**Line Appearance Alerting** The call routing is completed and the call is now ringing against its target. The line appearance also begins alerting and Ringing Line Preference has made it the current selected button.
	**Call Answered** Alerting on the line appearance has stopped but the line is still active. This indicates that the call has probably been answered. As our user's phone is idle, Idle Line Preference has returned the current select button to the first available call appearance button.
	**User Joins the Call** Our extension user has been asked by their colleague to join the call just answered on line 601. By pressing the line appearance button they have joined the call on that line and created a conference call.

Related Links

Appeance Button Operation on page 780

Multiple Alerting Appearance Buttons

In some scenarios, it is may be potentially possible for the same call to alert on several appearance buttons. In this case the following apply:

- **Line appearance buttons override call and bridged appearance buttons** In cases where a call on a line goes directly to the user as the incoming call route's destination, the call will only alert on the line appearance. In this scenario the ring delay settings used is that of the first free call appearance button.
- **A call can alert both call appearance, line appearance and bridged appearance buttons** The most common example of this will be hunt group calls where the hunt group members also have bridged call appearances to each other. In this case the button used to answer the call will remain active whilst the other button will return to idle.
- **Calls on a line/bridged appearance buttons can also alert on call coverage button** In this case alerting on the call coverage button may be delayed until the covered user's **Individual Coverage Time** has expired.
- **Ringing Line Preference Order** When a call alerts on several of the user's appearance buttons and **Ringing Line Preference** is set for the user, the order used for current selected button assignment is:

  1. Call appearance.
  2. Bridged appearance.
  3. Call coverage.
  4. Line appearance.

Example A user has a call to a covered user alerting initially on a line appearance button. **Ringing Line Preference** will assign current selected button status to the line appearance. When the same call also begins to alert on the call coverage appearance button, current selected button status switches to the call coverage appearance button.

Ring Delay Where ring delays are being used, the shortest delay will be applied for all the alerting buttons. For example, if one of the alerting buttons is set to **Immediate**, that will override any alerting button set to **Delayed Ring**. Similarly if one of the alerting buttons is set to **No Ring**, it will be overridden if the other alerting button is set to **Immediate** or **Delayed Ring**.

Related Links

Appeance Button Operation on page 780

Twinning

Twinning is a mechanism that allows an user to have their calls alert at two phones. The user's normal phone is referred to as the primary, the twinned phone as the secondary.

By default only calls alerting on the primary phone's call appearance buttons are twinned. For internal twinning, the system supports options to allow calls alerting on other types of appearance

buttons to also alert at the secondary phone. These options are set through the **User | Twinning** section of the system configuration and are **Twin Bridge Appearances**, **Twin Coverage Appearances** and **Twin Line Appearances**. In all cases they are subject to the secondary having the ability to indicate additional alerting calls.

Call alerting at the secondary phone ignoring any Ring Delay settings of the appearance button being used at the primary phone. The only exception is buttons set to No Ring, in which case calls are not twinned.

Related Links

Appeance Button Operation on page 780

Busy on Held

For a user who has **Busy on Held** selected, when they have a call on hold, the system treats them as busy to any further calls. This feature is intended primarily for analog phone extension users. Within Manager, selecting **Busy on Held** for a user who also has call appearance keys will cause a prompt offering to remove the **Busy on Held** selection.

Related Links

Appeance Button Operation on page 780

Reserving a Call Appearance Button

Functions such as transferring calls using a **Transfer** key require the user to have at least one available call appearance button in order to complete the outgoing call part of the process. However, by default all call appearance button are available to receive incoming calls at all times. Through the system configuration it is possible to reserve the user's last call appearance button for making outgoing calls only.

1400, 1600, 9500 and 9600 Series telephone users can put a call on hold pending transfer if they already have held calls even if they have no free call appearance button available. See Context Sensitive Transfer.

Reserving a Call Appearance

The method for doing this depends on the system software level.

Pre-4.0 IP Office: On the **User | Source Numbers** tab, enter the line **RESERVE_LAST_CA=** .

Release 4.0+: On the **User | Telephony | Multi-line Options** tab, select the option **Reserve Last CA**.

Related Links

Appeance Button Operation on page 780

Logging Off and Hot Desking

Users can be setup to log in and log out at different phones, this is called 'hot desking'. All the users settings, including their extension number, are transferred to the phone at which the user is logged in. This includes their key and lamp settings and appearance buttons.

This type of activity has the following effect on appearance buttons:

If logged out, or logged in at a phone that doesn't support appearance button functions:

- Bridged appearances set to the user will be inactive.
- Call coverage set to the user will still operate.

If logged in at a phone with fewer buttons than programmed for the user:

- Those buttons which are inaccessible on the logged in phone will be inactive.
- Any bridged appearances to those button from other users will be inactive.

Remote Hot Desking

Release 4.0+ supports, through the addition of license keys, users hot desking between systems within a multi-site network. However, the use of appearance buttons (call coverage, bridged appearance and line appearance) within a multi-site network is not supported. Therefore when a user logs in to a remote system, any such button that they have will no longer operate. Similarly any button that other users have with the remote user as the target will not operate.

Related Links

Appeance Button Operation on page 780

Applications

A number of system applications can be used to make, answer and monitor calls. These applications treat calls handled using key and lamp operation follows:

SoftConsole These applications are able to display multiple calls to or from a user and allow those calls to be handled through their graphical interface.

- All calls alerting on call appearance buttons are displayed.
- Calls on line, call coverage and bridged appearance buttons are not displayed until connected using the appropriate appearance button
- Connected and calls held here on all appearance button types are displayed.

Related Links

Appeance Button Operation on page 780

Programming Appearance Buttons

About this task

This section covers the programming of appearance buttons for users into existing system configurations.

Appearance Functions The functions **Call Appearance**, **Bridged Appearance**, **Coverage** and **Line Appearance** are collectively known as "appearance functions". For full details of their operation and usage refer to the Appearance Button Operation section. The following restrictions must be observed for the correct operation of phones.

Appearance functions programmed to buttons without suitable status lamps or icons are treated as disabled. These buttons are enabled when the user logs in on a phone with suitable buttons in those positions.

Line appearance buttons require line ID numbers to have been assigned, see Programming Line Appearance Numbers. The use of line appearances to lines where incoming calls are routed using DID (DDI) is not recommended.

How many buttons are allowed? The recommended limits are as follows:

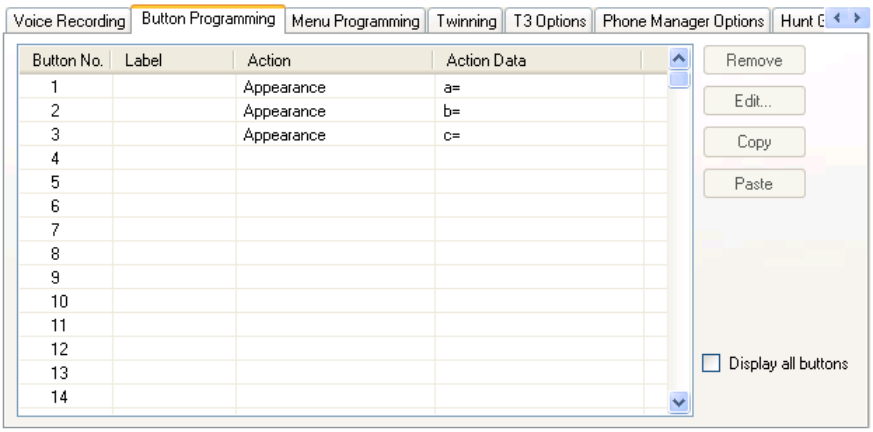
- A maximum of 10 bridged appearances to the same call appearance.
- A maximum of 10 line appearances to the same line.
- A maximum of 10 call coverages of the same covered user.

Programming Appearance Buttons Using Manager

If only button programming changes are required, the configuration changes can be merged back to the system without requiring a reboot.

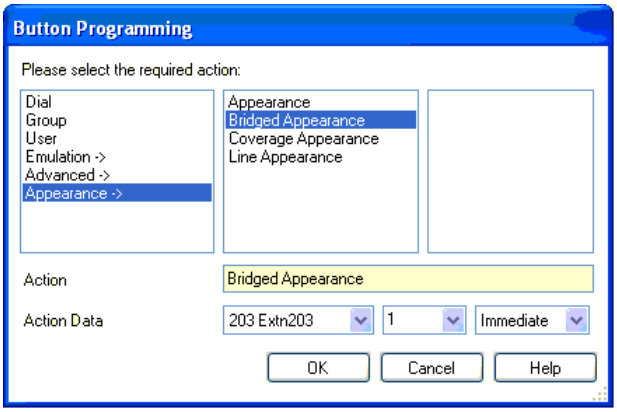
Procedure

1. Start Manager and load the current configuration from the system.
2. Locate and select the user for whom appearance buttons are required.
3. Select **Button Programming**.



The number of buttons displayed is based on the phone associated with the user when the configuration was loaded from the system. This can be overridden by selecting **Display all buttons**.

4. For the required button, click the button number and then click **Edit**.
5. Click the **...** button.



6. From the list of options that appears, click **Appearance**.
7. Select the type of appearance button required.
8. Use the **Action Data** drop-down fields to select the required settings.

   Click **OK**.
9. Repeat for any additional call appearance buttons required.

   Click **OK**.
10. Repeat for any other users requiring appearance buttons.

Related Links

Appeance Button Operation on page 780
Appearance Function System Settings on page 821
Appearance Function User Settings on page 822
Programming Line Appearance ID Numbers on page 823
Outgoing Line Programming on page 825

Appearance Function System Settings

System settings are applied to all users and calls. The system settings that affect appearance operation are found on the System | Telephony tabs and are:

- Auto Hold
- Conferencing Tone
- Ring Delay
- Visually Differentiate External Call

Related Links

Programming Appearance Buttons on page 820

Appearance Function User Settings

User settings are applied separately to each individual user. In addition to button programming, the following user settings are applicable to appearance button operation:

Cannot be Intruded: Default = On. This feature controls whether other users can use their appearance buttons to join the users call. It applies when the user is the longest present internal party already within the call.

- **Individual Coverage Time (secs):** Default = 10 seconds, Range 1 to 99999 seconds. This function sets how long the phone will ring at your extension before also alerting at any call coverage users. This time setting should not be equal to or greater than the **No Answer Time** applicable for the user.
- **Ring Delay**: Default = Blank (Use system setting). Range = 0 (use system setting) to 98 seconds. This setting is used when any of the user's programmed appearance buttons is set to Delayed ringing. Calls received on that button will initially only alert visually. Audible alerting will only occur after the ring delay has expired.
- **Coverage Ring**: Default = Ring. This field selects the type of ringing that should be used for calls alerting on any the user's call coverage and bridged appearance buttons. **Ring** selects normal ringing. **Abbreviated Ring** selects a single non-repeated ring. **No Ring** disables audible ringing. Note that each button's own ring settings (**Immediate**, **Delayed Ring** or **No Ring**) are still applied.

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

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

Attention Ring Setting	Coverage Ring Setting		
	Ring	**Abbreviated**	**Off**
Ring	Ring	Abbreviated	Off
Abbreviated	Abbreviated	Abbreviated	Off

- **Attention Ring**: Default = Abbreviated Ring. This field selects the type of ringing that should be used for calls alerting on appearance buttons when the user already has a connected call on one of their appearance buttons. **Ring** selects normal ringing. **Abbreviated Ring** selects a single ring. Note that each button's own ring settings (**Immediate**, **Delayed Ring** or **No Ring**) are still applied.
- **Ringing Line Preference**: Default = On. For users with multiple appearance buttons. When the user is free and has several calls alerting, ringing line preference assigns currently selected button status to the appearance button of the longest waiting call. Ringing line preference overrides idle line preference.

- **Idle Line Preference**: Default = On. For users with multiple appearance buttons. When the user is free and has no alerting calls, idle line preference assigns the currently selected button status to the first available appearance button.
- **Delayed Ring Preference**: Default = Off. This setting is used in conjunction with appearance buttons set to delayed or no ring. It sets whether ringing line preference should use or ignore the delayed ring settings applied to the user's appearance buttons.

When on, ringing line preference is only applied to alerting buttons on which the ring delay has expired.

When off, ringing line preference can be applied to an alerting button even if it has delayed ring applied.

- **Answer Pre-Select**: Default = Off. Normally when a user has multiple alerting calls, only the details and functions for the call on currently selected button are shown. Pressing any of the alerting buttons will answer the call on that button, going off-hook will answer the currently selected button. Enabling **Answer Pre-Select** allows the user to press any alerting button to make it the current selected button and displaying its call details without answering that call until the user either presses that button again or goes off-hook. Note that when both **Answer Pre-Select** and **Ringing Line Preference** are enabled, once current selected status is assigned to a button through ringing line preference it is not automatically moved to any other button.
- **Reserve Last CA**: Default = Off. Used for users with multiple call appearance buttons. When selected, this option stops the user's last call appearance button from being used to receive incoming calls. This ensures that the user always has a call appearance button available to make an outgoing call and to initiate actions such as transfers and conferences.

1400, 1600, 9500 and 9600 Series telephone users can put a call on hold pending transfer if they already have held calls even if they have no free call appearance button available. See Context Sensitive Transfer.

Abbreviated Ring: This option has been replaced by the **Attention Ring** setting above.

Related Links

Programming Appearance Buttons on page 820

Programming Line Appearance ID Numbers

Line appearances are supported for analog, E1 PRI, T1, T1 PRI, and BRI PSTN trunks. They are not supported for E1R2, QSIG and IP trunks.

Note that setting and changing line settings including line appearance ID numbers requires the system to be rebooted.

Related Links

Programming Appearance Buttons on page 820

Automatic Renumbering

About this task

Procedure

1. Select **Tools | Line Renumber**.
2. Select the starting number required for line numbering and click **OK**.
3. All lines that support **Line Appearance ID** will be numbered in sequence.

Manual Renumbering

About this task

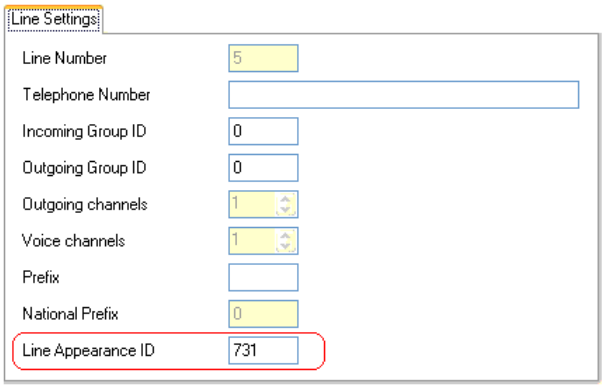
Procedure

1. Start Manager and load the current configuration from the system.
2. Select **Line**.
3. Select the line required.

   The tab through which line appearance ID numbers are set will vary depending on the type of line. A couple of examples are shown below.

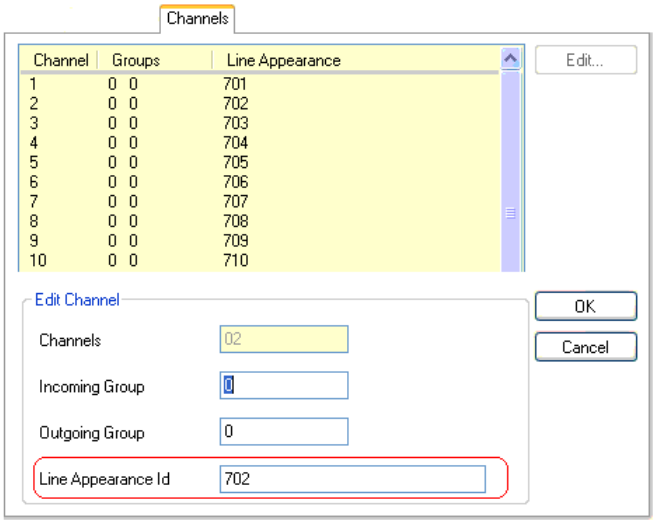
   a. Analog Line

   ts br?>On the **Line Settings** tab select **Line Appearance ID** and enter the ID required.



   b. Basic/Primary Rate Trunks

   ts br?>On the Channels tab select the individual channel and click Edit. Select **Line Appearance ID** and enter the required ID, then click **OK**. Repeat for all the channels required.



4. Click **OK**and repeat for any other lines.

Outgoing Line Programming

Assigning line ID numbers to lines and associating line appearance buttons to those lines is sufficient for answering incoming calls on those lines. However, to use line appearance buttons for outgoing calls may require further programming.

Short Codes and Outgoing Line Appearance Calls Once a line has been seized using a line appearance button, short code matching is still applied to the number dialed. That can include user, system and ARS or LCR short codes.

The short codes matching must resolve to an off-switch number suitable to be passed direct to the line.

The final short code applied must specify a 'dial' feature. This allows call barring of specific matching numbers to be applied using short codes set to features such as 'Busy'.

Related Links

Programming Appearance Buttons on page 820

Chapter 21: Overview of Data Routing

The system is a network router. In this role it can connect users on its LAN to remote services by using WAN links and telephone trunk connections. It can also allow users to dial-in and then act as if they were using a PC on the LAN.

As well as being a network router, the system is a telephone system. These dual roles allow it to support a range of functions that involve traffic between the network and telephony interfaces. These functions use internal data channels. The number of internal data channels that can be connected from the system's LAN interface to its telephony interface at any time is restricted.

An internal data channel is a connection between the system's telephony and LAN interfaces. For example a Voicemail connection, an internet connection or a RAS user.

Calls using a VCM channel do not use a data channel.

The number of data channels in use does not necessarily match the number of users:

- Several LAN network users, browsing the internet using the same service to an ISP would be a single data channel.
- Several dial-in network users would each have a separate data channel.

The maximum number of data channels that can be simultaneously in use for voicemail is restricted. These channels also require entry of an appropriate license.

The restriction depends on the type of control unit being used.

System Control Unit	Internal Data Channels	Maximum Data Channels for Voicemail
Small Office Edition	18	10
IP403	18	10
IP406 V1	24	20
IP406 V2	40	20
IP412	100	30
IP500 V2	48[1]	40

1. Reduced to 44 when an IP500 V2 4-Port Expansion card is installed.

Related Links

Network Address Translation (NAT) on page 827
Dynamic Host Configuration Protocol (DHCP) on page 827
Simple ISDN Internet Connection on page 828

ISDN Link Between IP Offices on page 828
Using a Dedicated T1/PRI ISP Link on page 829
Remote Access on page 832
Creating a VoIP Link via the WAN Port Using PPP on page 835

Network Address Translation (NAT)

NAT allows the addresses used within your LAN to be replaced by a different address when connecting to an external service.

Typically a service provider will allocate you a single IP address to be used when connecting to their service. NAT allows all your user's traffic to appears to be coming from that single address without having to change any of your user's real addresses. This is useful as internally most networks use addresses that have been reserved for public use within networks but are not valid for routing across the internet (since the same addresses may be being used on other networks). Also as stated it allows multiple users to use the same service simultaneously.

The use of NAT is automatically enabled if the system Service being used includes an IP address that is not in the same domain as the its LAN1 IP address.

An exception to the above applies for systems with two LAN's, LAN1 and LAN2. For these units, on each LAN, **Enable NAT** can be selected and then applied to traffic between the two LAN's.

Related Links

Overview of Data Routing on page 826

Dynamic Host Configuration Protocol (DHCP)

The system can act as a simple DHCP server. When switched on with a defaulted configuration, the Control Unit request IP address information from a DHCP server. If it gets no response it assumes the role of DHCP server for the LAN.

In DHCP Server mode, by default the Control Unit issues itself the address 192.168.42.1. It allocates 200 addresses for DHCP clients, 192.168.42.1 to 19.168.42.200. This leaves 192.168.42.201 to 192.168.42.254 available for any computers that need to be allocated a fixed or static IP address. 192.168.42.255 is not used as this is a broadcast address for the LAN.

Related Links

Overview of Data Routing on page 826

Simple ISDN Internet Connection

In this example, we want all non-local data traffic to be routed to the Internet. The Internet Service Provider (ISP) has provided the account details required. Using the system's Network Address Translation (NAT), a single account can be used for all users.

Select  **Service** and add a normal service. Change the following settings and click **OK**.

Name: Internet

Account Name: As provided by the ISP.

Password: As provided by the ISP.

Telephone Number: As provided by the ISP.

Check **Request DNS**.

Select  **IP Route** and add a new route. Change the following settings and click **OK**.

1. Leave the **IP Address** and **IP Mask** blank. This will then match any data traffic that isn't matched by any other IP Route record.
2. Select the service created above as the **Destination**.

Alternate In the example above, a default IP Route was created which then routed all traffic to the required Service. An alternate method to do this with system is to select Default Route within the Service settings.

Related Links

Overview of Data Routing on page 826

ISDN Link Between IP Offices

To create a data link between two sites via ISDN configure the Control Unit as per the following example:

At Site A on IP address 192.168.43.1

1. **Create a Normal Service:** The Service name can be any text and is used to identify this particular Service. The Account Name and password are presented to the remote end, therefore must match the User name and password configured at Site B. The Telephone Number is the number of the remote end.
2. **Create an IP Route**: In the IP Address field enter the network address of the remote end, not the IP address of the Control Unit. Under Destination select the Service created above.
3. **Create a User**: Under the Dial In tab tick Dial In On. This User account is used to authenticate the connection from the Site B. Note that as the Service and User have the same names, these two configuration forms are automatically linked and become an Intranet

Service. The User password is displayed at the bottom of the Service tab as the Incoming Password.

4. **Setup RAS**: Check the default RAS settings "Dial In" are available, otherwise create a new one. If the RAS settings are given the same name as the Service and User they are automatically linked and become a WAN Service. Ensure that the Encrypted Password option is not checked when using a WAN Service.
5. **Setup an Incoming Call Route**: Check the default Incoming Call Route is available, otherwise create a new one. If the Incoming Number is left blank, the Incoming Call Route accepts data calls on any number. Under Destination select the RAS service created above. The Bearer Capability should be AnyData.

At Site B on IP address 192.168.45.1

Repeat the above process but altering the details to create an route from Site B to Site A.

Related Links

Overview of Data Routing on page 826

Using a Dedicated T1/PRI ISP Link

This section shows an example of a dedicated WAN PPP link to an Internet Service Provider (ISP) over a set of T1 or T1 PRI line channels. The ISP must support this mode of connection and will need to provide details of the required settings. If multiple channels are to be used, then the ISP must support Multilink PPP.

Related Links

Overview of Data Routing on page 826

Tasks for Using a Dedicated T1/PRI ISP Link

About this task

Procedure

1. Create a New WAN Service
2. Create the Virtual WAN Port
3. Create an IP Route
4. T1 PRI Trunk

Create a New WAN Service

About this task

A service is used to define connection settings such as name, password, bandwidth, etc.

Procedure

1. Select  **Service** to display the existing services.
2. Click on and select **WAN Service**.
3. Select the **Service** tab.
4. In the **Name** field enter an appropriate name, such as **"Internet"**.

   Note that the system will also automatically create User record and a RAS record with the same name.
5. Enter the **Account Name**, **Password** and **Telephone Number** details provided by the ISP.
6. For the **Firewall Profile** select the firewall created previously.
7. Click the **Bandwidth** tab.
   a. Set the **Maximum No. of Channels** to the maximum number of channels that the service should use.

      In this example, 12 channels were used.
   b. Leave all the other records at their default values.
   c. If the ISP has allocated IP address details these are entered through the IP tab.

      If the IP Address and IP Mask define a different domain from the system LAN, then NAT is automatically applied.
8. Click the **IP** tab.
   a. In the **IP Address** field enter the IP address specified by the ISP.
   b. In the **IP Mask** field enter the IP Mask specified by the ISP.
   c. The settings shown are typical.

      The actual settings must match those required by the ISP. For example, if Cisco routers are being used then IPHC needs to be ticked.
9. Click the **PPP** tab.

   Ensure that the following options are selected. Leave all other options at their default settings.
   - **Multilink**.
   - **Compression Mode**: Disable.
   - **Callback Mode**: Disable.
   - **Access Mode**: Digital64
10. Click **OK**.

Create the Virtual WAN Port

About this task

In this stage, a WAN port is defined that actually uses T1 or T1 ISDN trunk channels.

Procedure

1. Select  **WAN Port** to display existing ports.
2. Click on  and select **WAN Port**.
3. In the Name field, enter either **LINEx.y** where:
   - **LINE** must be in uppercase.
   - **x** is the line number. For a trunk card in Slot A, this will be 1. For a trunk card in Slot B, this will be 5.
   - **y** is the lowest numbered channel number to be used by the WAN link minus 1. For example, if the lowest channel to be used is channel 1 then y = 1 - 1 = 0.
4. In the **Speed** field, enter the total combined speed of the maximum number of channels sets in the Service.

   In this example, 12 channels x 64000 bits = 76800.
5. Set the **Mode** to **SyncPPP**.
6. In the **RAS Name** field, select the name used for the Service.
7. Click **OK**.

Create an IP Route

About this task

By creating an IP route with blank IP address details, it becomes the default route for outgoing IP traffic.

Procedure

1. Select  **IP Route** to display existing routes.
2. Click on  and select **IP Route**.
3. Leave the **IP Address** and **IP Mask** fields blank.
4. In the **Destination** field, select the WAN service.
5. Leave the **Metric** at default value of **1**.
6. Click **OK**.

7. **Configure the Line Channels** This stage of the process differs according to the type of trunk being used.
8. **T1 Trunk** Use the following for a T1 trunk.
9. Click **Line** to display the existing lines.
10. Double-click on the line previously entered in the WAN Port settings.
11. Check that the **Channel Allocation** order matches that required by the ISP.

    Cisco routers typically use 1|24.
12. Select the channels to be used in the WAN PPP link and change their Channel Type to “Clear Channel 64k”.
13. Click **OK**.
14. Click **OK**again.
15. Send the configuration to the system and reboot.

T1 PRI Trunk

About this task

Use the following for a T1 PRI trunk.

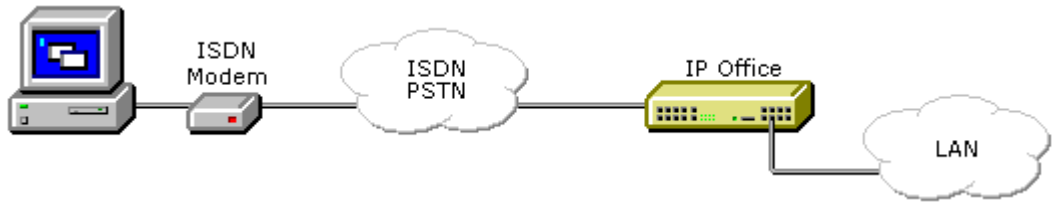
Procedure

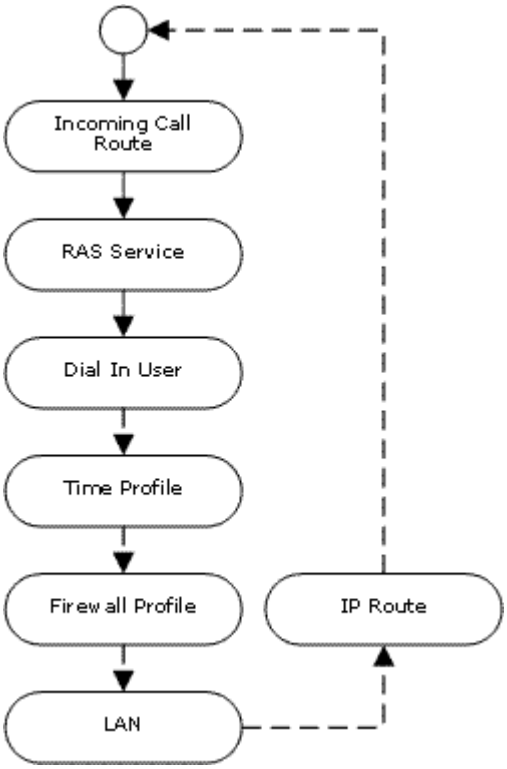
1. Click on **Line** to display the list of existing lines.
2. Double-click on the line previously entered in the WAN Port settings.
3. Check that the **Channel Allocation** order matches that required by the ISP.

    Cisco routers typically use 1|23.
4. Select the channels to be used in the WAN PPP link and change their Admin to “Out of Service”.
5. Click **OK**.
6. Click **OK**again.
7. Send the configuration to the system and reboot.

Remote Access

The system support remote access for incoming data calls on trunks.





To do remote access, an incoming call is passed through the following elements of the system configuration.

Incoming Call Route A Incoming Call Route is used to match incoming remote access calls and pass them to a RAS service as the destination.

RAS Service The RAS service defines settings relating to the data traffic methods usable with the call.

User The user defines the name and password required for the RAS service. The user must have Dial In On enabled.

An **R** setting on the user's Source Numbers tab can be used to define the ICLID from which RAS calls are accepted.

Time Profile The user settings can specify a time profile. The time profile then controls when remote access is allowed.

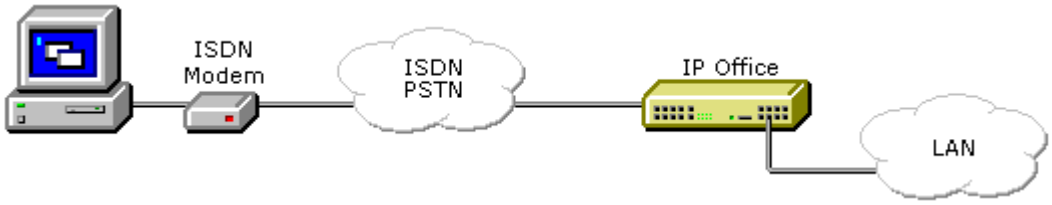
Firewall Profile The user settings can specify a firewall profile. The firewall profile then controls what traffic is allowed through the remote access connection.

Static NAT The system supports the use of Static NAT records in firewall profiles. These are used to translate external IP addresses to internal IP addresses.

System | LAN The system can provide DHCP support for remote access connections when it is set to Server or Dial in modes. Alternatively the remote access client can use a static IP address on the system's subnet.

IP Route If the remote access client uses a IP address that is from a different subnet from the system, then a IP route record is required for returning data. The RAS service is set as the destination.

ISDN Remote Access Example



Create a User The required details are:

- **In the User tab**: Enter a Name and Password. The system is case sensitive. Remember to take care with passwords as this is a remote access link into your network.
- **In the Dial In tab**: Ensure that Dial In On is ticked. The Firewall Profile and Time Profile are optional.

Create a RAS Record

In the RAS tab: Enter the same name as the user that you created earlier. Again, remember this is case sensitive.

Create an Incoming Call Route

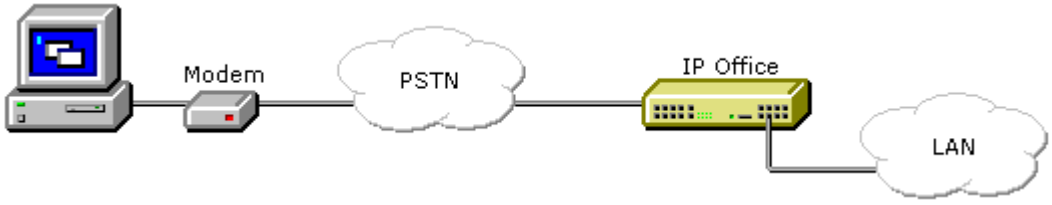
- Set the **Bearer Capability** to **Any Data**.
- In the **Destination** drop-down list, select the RAS record created above.
- The values that you enter for any of the other fields will depend on whether the remote user will be calling in on a particular line, number or from a set ICLID.

1. **Is a Return IP Route Needed ?** Go to Step 5.
2. **Create a IP Route (Optional)** If the remote user has an IP address that is not in the same domain as the system, then an IP Route is needed for return data. This is not

necessary if the remote user's dial-up connection method is set to 'Obtain an IP Address Automatically' and the system's **DHCP mode** is set to **Server** or **Dial In**.

- Enter the **IP Address** and **IP Mask** of the remote system.
- In the **Destination** drop-down list select the RAS record created above.

Analog Remote Access Example



Configuration for a connection from an analog modem call is very similar to the ISDN example. However the system must be able to answer modem calls. This can be done in the following ways:

Analog Trunk Modem Mode On systems with an analog trunk card in the control unit, the first analog trunk can be set to answer V.32 modem calls. This is done by checking the Modem Enabled option on the analog line settings or using the default short code *9000* to toggle this service on or off.

IP500 ATM4 Uni Trunk Card Modem Support It is not required to switch the card's modem port on/off. The trunk card's V32 modem function can be accessed simply by routing a modem call to the RAS service's extension number. The modem call does not have to use the first analog trunk, instead the port remains available for voice calls.

When using an analog modem, the **Bearer Capability** of the incoming call route used should be **Any Voice**.

Related Links

Overview of Data Routing on page 826

Creating a VoIP Link via the WAN Port Using PPP

A VoIP link across a leased line requires the Control Unit at both ends to have a Voice Compression Module installed. These provide for a fixed number of channels to use VoIP at any time. They are used to compress voice down to either 6k3 (G.723) or 8k (G.729) and provide echo cancellation.

Both ends must using the same version of software and configured to use the same speed and compression.

For example, consider this VoIP link:

- Site A on IP address 192.168.42.1
- Site B on IP address 192.168.45.1

Perform the following steps, once for Site A and once for Site B.

1. **Create a Normal Service**: The Account Name and password is presented to the remote end, therefore must match the User name and password configured at Site B. The Encrypted Password option can only be used if the remote end also supports CHAP.
2. **Create a User**: Under the Dial In tab tick Dial In On. This User account is used to authenticate the connection from the Site B. As the Service and User have the same name these two configuration forms are automatically linked and become an Intranet Service. The User password is displayed at the bottom of the Service tab as the Incoming Password.
3. **Name**: SiteB
4. **Dial In | Dial In On**: Enabled.
5. **Create a RAS service**: If CHAP is to be used on this link, then the Encrypted Password option must be checked in the Service and in the RAS service. The name of the RAS service must match the name of the Service at Site B. If the RAS service is given the same name as the Service and User, they are automatically linked and become a WAN Service. Ensure that the Encrypted Password option is not checked when using a WAN Service.
6. **Edit the WANPort**: Note - do not create a new WANPort, this is automatically detected. If a WANPort is not displayed, connect the WAN cable, reboot the Control Unit and receive the configuration. The WANPort configuration form should now be added.

   RAS Name: SiteA
7. **Create an IP Route**: The IP Address is the network address of the remote end. Under Destination select the Service created above.
8. **Create a new Line:** The Line Number and Line Group ID must be unique, in other words, not used by any other line. The Gateway IP Address is the IP Address of the Control Unit at the remote end. The Compression Mode used is dependent on the Voice Compression Card the Control Unit is running and the speed of the link.
9. **Create a Short Code:** To route all calls where the number dialed starts with 8 via Line Group ID 1, therefore via the VPN Line created above.
10. **Short Code**: 8N
11. **Telephone Number**: N
12. **Line Group ID**: 1
13. **Feature**: Dial

Related Links

Overview of Data Routing on page 826

Chapter 22: Appendix: SMDR

The control unit is able to send SMDR (Station Message Detail Reporting) records to a specified IP address and port.

Typically an SMDR record is output for each call between two parties (internal and or external) that is handled by the system. In some scenarios, for examples transfers, where a call involves multiple parties then multiple SMDR records may be output for each part of the call.

Each SMDR record contains call information in a comma-separated format (CSV) format, that is variable-width fields with each field separated by commas.

The recommended limit for authorization codes is 1000 entries

The IP500 V2 control units can store any buffered SMDR records during any controlled system power downs or reboots.

Note:

Outbound Contact Express

The Outbound Contact Express solution does not generate SMDR records.

Enabling SMDR

1. Receive the configuration from the system.
2. Select **System** and then select the **CDR/SMDR** tab.
3. Use the **Output** drop down box to select **SMDR only**.
4. In the **SMDR** settings, enter the required **IP Address** and **TCP Port**.

Overview of SMDR Records

An SMDR record is generated for each call between two devices on the system. Devices include extensions, trunk lines (or channels on a trunk), voicemail channels, conference channels and system tones.

Calls which are not presented to another device do not generate an SMDR record. For example internal users dialing short code that simply changes a configuration setting.

The SMDR record is generated when the call ends, therefore the order of the SMDR records output does not match the call start times.

Each record contains a call ID which is increased by 1 for each subsequent call.

When a call moves from one device to another, an SMDR record is output for the first part of the call and an additional SMDR record will be generated for the subsequent part of the call.

Each of these records will have the same Call ID.

Each record for a call indicates in the Continuation field if there will be further records for the same call.

Call Times

Each SMDR record can include values for ringing time, connected time, held time and parked time. The total duration of an SMDR record is the sum of those values.

The time when a call is not in any one of the states above, for example when one party to the call has disconnected, is not measured and included in SMDR records.

Where announcements are being used, the connected time for a call begins either when the call is answered or the first announcement begins.

All times are rounded up to the nearest second.

Each SMDR record has a Call Start time taken from the system clock time. For calls being transferred or subject to call splitting, each of the multiple SMDR records will have the same Call Start time as the original call.

Related Links

SMDR Fields on page 838

SMDR Examples on page 842

SMDR Fields

The SMDR output contains the following fields. Note that time values are rounded up to the nearest second.

1. **Call Start**

   Call start time in the format YYYY/MM/DD HH:MM:SS. For all transferred call segment this is the time the call was initiated, so each segment of the call has the same call start time.

2. **Connected Time**

   Duration of the connected part of the call in HH:MM:SS format. This does not include ringing, held and parked time. A lost or failed call will have a duration of 00:00:00. The total duration of a record is calculated as Connected Time + Ring Time + Hold Time + Park Time.

3. **Ring Time**

   Duration of the ring part of the call in seconds.

   - For inbound calls this represents the interval between the call arriving at the switch and it being answered, not the time it rang at an individual extension.
   - For outbound calls, this indicates the interval between the call being initiated and being answered at the remote end if supported by the trunk type. Analog trunks are not able to detect remote answer and therefore cannot provide a ring duration for outbound calls.

4. **Caller**

The callers' number. If the call was originated at an extension, this will be that extension number. If the call originated externally, this will be the CLI of the caller if available, otherwise blank.

5. **Direction**

   Direction of the call – **I** for Inbound, **O** for outbound. Internal calls are represented as **O** for outbound. This field can be used in conjunction with **Is_Internal** below to determine if the call is internal, external outbound or external inbound.

6. **Called Number**

   This is the number called by the system. For a call that is transferred this field shows the original called number, not the number of the party who transferred the call.

   - **Internal calls**: The extension, group or short code called.
   - **Inbound calls**: The target extension number for the call.
   - **Outbound calls**: The dialed digits.
   - **Voice Mail**: Calls to a user's own voicemail mailbox.

7. **Dialled Number**

   For internal calls and outbound calls, this is identical to the **Called Number** above. For inbound calls, this is the DDI of the incoming caller.

8. **Account**

   The last account code attached to the call.

   Note:

   System account codes may contain alphanumeric characters.

9. **Is Internal**

   0 or **1**, denoting whether both parties on the call are internal or external (**1** being an internal call). Calls to destinations on other switches in a network are indicated as internal.

Direction	Is Internal	Call Type
I	**0**	Incoming external call.
O	**1**	Internal call.
O	**0**	Outgoing external call.

10. **Call ID**

    This is a number starting from 1,000,000 and incremented by 1 for each unique call. If the call has generates several SMDR records, each record will have the same Call ID. Note that the Call ID used is restarted from 1,000,000 if the system is restarted.

11. **Continuation**

    1 if there is a further record for this call id, **0** otherwise.

12. **Party1Device**

The device 1 number. This is usually the call initiator though in some scenarios such as conferences this may vary. If an extension/hunt group is involved in the call its details will have priority over a trunk. That includes remote network destinations.

Type	Party Device	Party Name
Internal Number	**E**<extension number>	<name>
Voicemail	**V**<9500 + channel number>	**VM Channel** <channel number>
Conference	**V**<1><conference number> +<channel number>	**CO Channel** <conference number.channel number>
Line	**T**<9000+line number>	**Line** <line number>.<channel if applicable>
Other	**V**<8000+device number>	**U**<device class> <device number>**.**<device channel>
Unknown/Tone	**V8000**	**U1 0.0**

13. **Party1Name**

    The name of the device – for an extension or agent, this is the user name.

14. **Party2Device**

    The other party for the SMDR record of this call segment. See **Party1Device** above.

    For barred calls, this field is populated with “Barred”.

15. **Party2Name**

    The other party for the SMDR record of this call segment. See **Party1Name** above.

    For barred calls, this field is populated with “Barred”.

16. **Hold Time**

    The amount of time in seconds the call has been held during this call segment.

17. **Park Time**

    The amount of time in seconds the call has been parked during this call segment.

18. **AuthValid**

    This field is used for authorization codes. This field shows **1** for valid authorization or **0** for invalid authorization.

19. **AuthCode**

    For security, this field shows **n/a** regardless of whether an authorization code was used.

20. **User Charged**

    This and the following fields are used for ISDN Advice of Charge (AoC). The user to which the call charge has been assigned. This is not necessarily the user involved in the call.

21. **Call Charge**

    The total call charge calculated using the line cost per unit and user markup.

22. **Currency**

    The currency. This is a system wide setting set in the system configuration.

23. **Amount at Last User Change**

    The current AoC amount at user change.

24. **Call Units**

    The total call units.

25. **Units at Last User Change**

    The current AoC units at user change.

26. **Cost per Unit**

    This value is set in the system configuration against each line on which Advice of Charge signalling is set. The values are 1/10,000th of a currency unit. For example if the call cost per unit is £1.07, a value of 10700 should be set on the line.

27. **Mark Up**

    Indicates the mark up value set in the system configuration for the user to which the call is being charged. The field is in units of 1/100th, for example an entry of 100 is a markup facto of 1 .

28. **External Targeting Cause**

    This field indicates who or what caused the external call and a reason code. For example **U FU** indicates that the external call was caused by the Forward Unconditional setting of a User.

Targeted by		**Reason Code**	
HG	Hunt Group.	**fb**	Forward on Busy.
U	User.	**fu**	Forward unconditional.
LINE	Line.	**fnr**	Forward on No Response.
AA	Auto Attendant.	**fdnd**	Forward on DND.
ICR	Incoming Call Route.	**CfP**	Conference proposal (consultation) call.
RAS	Remote Access Service.	**Cfd**	Conferenced.
?	Other.	**MT**	Mobile Twinning.
		TW	Teleworker.
		XfP	Transfer proposal (consultation) call.
		Xfd	Transferred call.

29. **External Targeter Id**

The associated name of the targeter indicated in the External Targeting Cause field. For hunt groups and users this will be their name in the system configuration. For an Incoming Call Route this will be the Tag if set, otherwise **ICR**.

30. **External Targeted Number**

    This field is used for forwarded, Incoming Call Route targeted and mobile twin calls to an external line. It shows the external number called by the system as a result of the off switch targeting where as other called fields give the original number dialled.

Related Links

Appendix: SMDR on page 837

SMDR Examples

The following are examples of system SMDR records for common call scenarios.

Lost incoming Call

In this record, the Call duration is zero and the Continuation field is 0, indicating that the call was never connected. The Ring Time shows that it rang for 9 seconds before ending.

```
2014/06/28 09:28:41,00:00:00,9,8004206,I,4324,4324,,0,1000014155,0,E4324,Joe
Bloggs,T9161,LINE 5.1,0,0,,,,,,,,,,,,
```

Call Answered by Voicemail

In this example, 215 has made a call to 211. However the Party2Device and Party2Name show that the call was answered by voicemail.

```
2014/10/20 06:43:58,00:00:10,21,215,O,211,211,,I,28,0,E215,Extn215,V9051,VM Channel
1,0,0,,,,,,,,,,,,
```

Call Transferred to Voicemail

In this example, the Continuation field in the first record tells us that it wasn't the end of the call. The matching Call ID identifies the second record as part of the same call. The change in Party 1 details between the two records show that the call was transferred to voicemail.

```
2014/06/28 09:30:57,00:00:13,7,01707392200,I,299999,299999,,0,1000014160,1,E4750,John
Smith,T9002,LINE 1.2,11,0,,,,,,,,,,,, 2014/06/28 09:30:57,00:00:21,0,01707392200,I,
299999,299999,,0,1000014160,0,V9502,VM Channel 2,T9002,LINE 1.2,0,0,,,,,,,,,,,,
```

External Call

The Is Internal field being 0 shows this to be a external call. The Direction field as I shows that it was an incoming call. The Ring Time was 7 seconds and the total Connected Time was 5 seconds.

```
2014/08/01 15:14:19,00:00:05,7,01707299900,I,
403,390664,,0,1000013,0,E403,Extn403,T9001,Line 1.2,0,0,,,,,,,,,,,,
```

Internal Call

The Is Internal field being 1 shows this to be a internal call. The Ring Time was 4 seconds and the total Connected Time was 44 seconds.

```
2014/06/26 10:27:44,00:00:44,4,4688,O,4207,4207,,1,1000013898,0,E4688,Joe
Bloggs,E4207,John Smith,0,0,,,,,,,,,,,,
```

Outgoing Call

The combination of the Direction field being outbound and the Is Internal field be 0 show that this was a outgoing external call. The line (and in this case channel) used are indicated by the Party2 Name and being a digital channel the Ring Time before the call was answered is also shown.

```
2014/06/28 08:55:02,00:08:51,9,4797,O,08000123456,08000123456,,0,1000014129,0,E4797,Joe
Bloggs,T9001,LINE 1.1,0,0,,,,,,,,,,,,
```

Voicemail Call

The two records below show calls to voicemail. The first shows the Dialed Number as*17, the default short code for voicemail access. The second shows the Dialed Number as VoiceMail, indicating some other method such as the Message key on a phone was used to initiate the call.

```
2014/06/28 09:06:03,00:00:19,0,4966,O,*17,*17[1],,1,1000014131,0,E4966,John
Smith,V9501,VM Channel 1,0,0,,,,,,,,,,,, 2014/06/28
09:06:03,00:00:19,0,4966,O,VoiceMail,VoiceMail,,1,1000014134,0,E4966,John Smith,V9501,VM
Channel 1,0,0,,,,,,,,,,,,
```

Parked Call

In this example the first record has a Park Time showing that the call was parked. The Continuation field indicates that the call did not end this way and there are further records. The second record has the same Call ID and shows a change in the Party2Name [4], indicating that party unparked the call. Note also that both records share the same call start time.

```
2014/10/20 07:18:31,00:00:12,3,215,O,
210,210,,1,38,1,E215,Extn215,E210,Extn210,0,7,,,,,,,,,,,, 2014/10/20
07:18:31,00:00:10,0,215,O,210,210,,1,38,0,E215,Extn215,E211,Extn211,0,0,,,,,,,,,,,,
```

Incoming call with Account Code

In this example, at some stage as the call was made or during the call, an Account Code has been entered.

```
2014/06/28 11:29:12,00:00:02,2,5002,I,1924,1924,Support,
0,1000014169,0,E1924,Extn1924,T9620,LINE 8.20,0,0,,,,,,,,,,,,
```

Conference Using Conference Add Short Code

In this example 2101 has made a call and put put it on hold (record 2), then made another call and put it on hold (record 1) and then dialled the default short code *47 to conference all their held calls (record 3). The records for the first two calls have the Continuation field set as 1 indicating that the calls continued in further records.

Record 3 shows 2101 making a new call in which they dial *47, which places them and their held calls into a conference. This is shown by the Party Device and Party Name details as being a conference (100) and the conference channel used for each.

For both the Continuation fields show that the calls do not end but rather have subsequent records.

```
2014/07/09 17:55,00:00:03,3,2101,O,8262623#,8262623#,,
0,1000024,1,E2101,Extn2101,T9002,Line 2.1,8,0,,,,,,,,,,,,
```

```
2014/07/09 17:54,00:00:29,7,2101,O,
2121,2121,,1,1000023,1,E2101,Extn2101,E2121,Extn2121,23,0,,,,,,,,,,,,
```

```
2014/07/09 17:55,00:00:46,0,2101,O,*47,*47,,1,1000026,0,E2101,Extn2101,V11001,CO Channel
100.1,0,0,,,,,,,,,,,,
```

```
2014/07/09 17:54,00:00:49,0,,O,
71234567890,71234567890,,1,1000023,0,E2121,Extn2121,V11003,CO Channel
100.3,0,0,,,,,,,,,,,,
```

```
2014/07/09 17:55,00:00:49,0,,O,8262623#,8262623#,,0,1000024,0,V11002,CO Channel
100.2,T9002,Line 2.1,0,0,,,,,,,,,,,,
```

Conference Using Conference Button

In this example, an extension user answers a call and then brings in another user by using the Conference button on their phone. Again we see records for the initial call, the conference proposal call and then for the 3 parties in the conference that is created.

```
2014/07/09 15:05:41,00:00:04,3,203,O,
201,201,,1,1000009,1,E203,Extn203,E201,Extn201,0,0,,,,,,,,,,,,
```

```
2014/07/09 15:05:26,00:00:09,3,207,O,
203,203,,1,1000008,1,E207,Extn207,E203,Extn203,10,0,,,,,,,,,,,,
```

```
2014/07/09 15:05:41,00:00:08,0,,O,,,,1,1000009,0,E201,Extn201,V11001,CO Channel
100.1,0,0,,,,,,,,,,,,
```

```
2014/07/09 15:05:50,00:00:10,0,203,O,201,201,,1,1000010,0,E203,Extn203,V11002,CO Channel
100.2,0,0,,,,,,,,,,,,
```

```
2014/07/09 15:05:26,00:00:10,0,207,O,203,203,,1,1000008,0,E207,Extn207,V11003,CO Channel
100.3,0,0,,,,,,,,,,,,
```

Adding a Party to a Conference

This example is a variant on that above. Having started a conference, extension 203 adds another party.

```
2014/07/09 15:08:31,00:00:03,3,203,O,
201,201,,1,1000014,1,E203,Extn203,E201,Extn201,0,0,,,,,,,,,,,,
```

```
2014/07/09 15:08:02,00:00:22,6,207,O,
203,203,,1,1000013,1,E207,Extn207,E203,Extn203,9,0,,,,,,,,,,,,
```

```
2014/07/09 15:08:45,00:00:02,4,203,O,403,403,,0,1000016,1,E203,Extn203,E403,Libby Franks,
0,0,,,,,,,,,,,,
```

```
2014/07/09 15:08:02,00:00:24,0,207,O,203,203,,1,1000013,0,E207,Extn207,V11003,CO Channel
100.3,0,0,,,,,,,,,,,,
```

```
2014/07/09 15:08:39,00:00:17,0,203,O,201,201,,1,1000015,0,E203,Extn203,V11002,CO Channel
100.2,8,0,,,,,,,,,,,,
```

```
2014/07/09 15:08:31,00:00:26,0,,O,,,,1,1000014,0,E201,Extn201,V11001,CO Channel
100.1,0,0,,,,,,,,,,,,
```

```
2014/07/09 15:08:45,00:00:12,0,,O,403,403,,0,1000016,0,E403,Libby Franks,V11004,CO
Channel 100.4,0,0,,,,,,,,,,,,
```

Transfer

In this example 2126 has called 2102. The record (1) for this has the Continuation set a 1 indicating that it has further records. In the following record (3) with the same Call ID it can be seen that the Party 2 Device and Party 2 Name fields have changed, indicating that the call is now connected to a different device, in this example 2121. We can infer the blind transfer from the intermediate record (2) which shows a call of zero Connected Time between the original call destination 2102 and the final destination 2121.

```
2014/07/09 17:51,00:00:38,18,2126,O,
2102,2102,,1,1000019,1,E2126,Extn2126,E2102,Extn2102,19,0,,,,,,,,,,,,
```

```
2014/07/09 17:52,00:00:00,7,2102,O,
2121,2121,,1,1000020,0,E2102,Extn2102,E2121,Extn2121,0,0,,,,,,,,,,,,
```

```
2014/07/09 17:51,00:00:39,16,2126,O,
2102,2102,,1,1000019,0,E2126,Extn2126,E2121,Extn2121,0,0,,,,,,,,,,,,
```

In this second example extension 402 answers an external call and then transfers it to extension 403. Again the two legs of the external call have the same time/date stamp and same call ID.

```
2014/08/01 15:23:37,00:00:04,7,01707299900,I,
4001,390664,,0,1000019,1,E402,Extn402,T9001,Line 1.1,6,0,,,,,,,,,,,,
```

```
2014/08/01 15:23:46,00:00:00,3,402,O,
403,403,,1,1000020,0,E402,Extn402,E403,Extn403,0,0,,,,,,,,,,,,
```

```
2014/08/01 15:23:37,00:00:04,4,01707299900,I,
4001,390664,,0,1000019,0,E403,Extn403,T9001,Line 1.1,0,0,,,,,,,,,,,,
```

Busy/Number Unavailable Tone

In this example 2122 calls 2123 who is set to DND without voicemail. This results in 2122 receiving busy tone.

The records shows a call with a Connected Time of 0. The Call Number field shows 2123 as the call target but the Party 2 Device and Party 2 Name fields show that the connection is to a virtual device.

```
2014/07/09 17:59,00:00:00,0,2122,O,2123,2123,,1,1000033,0,E2122,Extn2122,V8000,U1
0.0,0,0,,,,,,,,,,,,
```

Call Pickup

The first record shows a call from 2122 to 2124 with a Connected Time of zero but a Ring Time of 8. The Continuation field indicates that the call has further records.

The second record has the same Call ID but the Party 2 Device and Party 2 Name details show that the call has been answered by 2121.

```
2014/07/09 18:00,00:00:00,8,2122,O,
2124,2124,,1,1000038,1,E2122,Extn2122,E2124,Extn2124,0,0,,,,,,,,,,,,
```

```
2014/07/09 18:00,00:00:38,1,2122,O,
2124,2124,,1,1000038,0,E2122,Extn2122,E2121,Extn2121,0,0,,,,,,,,,,,,
```

Internal Twinning

The records for scenarios such as internal call forwarding or follow me indicate the rerouting in a single record by having Caller and Called Number details that differ from the final Party 1 and Party 2 details. Internal twinning differs is showing a call answered at the twin exactly the same as having been answered at the primary.

203 is internally twinned to 201. Call from 207 to 203 but answer at 201.

```
2014/07/09 16:25:26,00:00:03,7,207,O,
203,203,,1,1000037,0,E207,Extn207,E203,Extn203,0,0,,,,,,,,,,,,
```

Park and Unpark

Parking and unparking of a call at the same extension is simply shown by the Park Time field of the eventual SMDR record. Similarly calls held and unheld at the same extension are shown by the Held Time field of the eventual SMDR record for the call. The records below however show a call parked at one extension and then unparked at another.

The records show a call from 207 to 203. 203 then parks the call shown by the Park Time. The call is unparked by 201, hence the first record is indicated as continued in its Continuation field. The matching Call ID indicates the subsequent record for the call.

```
2014/07/09 16:39:11,00:00:00,2,207,O,
203,203,,1,1000052,1,E207,Extn207,E203,Extn203,0,4,,,,,,,,,,,,
```

```
2014/07/09 16:39:11,00:00:02,0,207,O,
203,203,,1,1000052,0,E207,Extn207,E201,Extn201,0,0,,,,,,,,,,,,
```

Distributed Hunt Group Call

An incoming call to site A is targeted to a distributed hunt group member on site B. They transfer the call back to a hunt group member on site A.

```
2014/08/01 15:32:52,00:00:10,19,01707299900,I,
4002,390664,,0,1000024,1,E209,Luther-209,T9001,Line 1.2,0,0,,,,,,,,,,,,
```

```
2014/08/01 15:33:19,00:00:00,2,209,I,
403,403,,0,1000025,0,E209,Luther-209,E403,Extn403,0,0,,,,,,,,,,,,
```

```
2014/08/01 15:32:52,00:00:03,3,01707299900,I,
4002,390664,,0,1000024,0,E403,Extn403,T9001,Line 1.2,0,0,,,,,,,,,,,,
```

Voicemail Supervised Transfer

A call is routed to a voicemail module that performs a supervised transfer.

```
2014/08/01 16:36:04,00:00:09,0,01707299900,I,xfer,390664,,0,1000061,1,T9001,Line
1.1,V9508,VM Channel 8,0,0,,,,,,,,,,,,
```

```
2014/08/01 16:36:07,00:00:03,4,,I,402,402,,0,1000062,0,E402,Extn402,V8000,U12
0.8,0,0,,,,,,,,,,,,
```

```
2014/08/01 16:36:04,00:00:09,0,01707299900,I,
402,390664,,0,1000061,0,E402,Extn402,T9001,Line 1.1,0,0,,,,,,,,,,,,
```

Outgoing External Call

The External Targeting Cause indicates that the external call was caused by a user. The lack of specific reason implies that it was most likely dialed. The External Targeter ID is the user name in this example

```
… 16:23:06,00:00:04,5,203,O,9416,9416,,0,1000035,0,E203,Extn203,T9005,Line
5.1,0,0,,,Extn203,,,,,,,,U,Extn203,,
```

Rerouted External Call

In this example an incoming external call has been rerouted back off switch, shown by the Party 1 fields and the Party 2 fields being external line details. The External Targeter Cause shows that rerouting of the incoming call was done by an incoming call route (ICR). The External Targeter ID in

this case is the Tag set on the incoming call route. The External Targeted Number is the actual external number call.

```
… 08:14:27,00:00:03,5,392200,I,9416,200,,0,1000073,0,T9005,Line 5.1,T9005,Line
5.2,0,0,,,,0000.00,,0000.00,0,0,618,0.01,ICR,Main ICR,416,
```

External Forward Unconditional

In this example, user 203 has a forward unconditional number set for calls. This is indicated by the External Targeting Cause showing user and forward unconditional. The External Targeter ID shows the source of the call being forwarded, in this example user 207. The External Targeted Number shows the actual external number called by the system.

```
… 16:22:41,00:00:02,5,207,O,203,203,,0,1000034,0,E207,Extn207,T9005,Line
5.1,0,0,,,Extn203,0000.00,,0000.00,0,0,618,1.00,U fu,Extn207,9416,
```

Transferred Manually

In this example the internal user transfers a call to an external number. The External Targeting Cause in the first record indicates that this external call is the result of a user (U) transfer proposal (XfP) call. The Continuation field indicates that another record with the same Call ID will be output.

The additional records are output after the transferred call is completed. The first relates to the initial call prior. The second is the transferred call with the External Targeting Cause now indicating user (U) transferred (Xfd).

```
… 16:33:19,00:00:05,3,203,O,9416,9416,,0,1000044,1,E203,Extn203,T9005,Line
5.1,0,0,,,,,,,,,,U XfP,Extn207,,
```

```
… 16:33:09,00:00:02,2,207,O,
203,203,,1,1000043,0,E207,Extn207,E203,Extn203,11,0,,,,,,,,,,,,
```

```
… 16:33:19,00:00:04,0,207,O,9416,9416,,0,1000044,0,E207,Extn207,T9005,Line
5.1,0,0,,,Extn207,,,,,,,,U Xfd,Extn203,,
```

Mobile Twinned Call Answered Internally

For this example user 203 has mobile twining enabled to the external number 9416 as twin. Their mobile dial delay is set to 2 seconds. The call is answered at the user's internal extension.

In this scenario the record for the external call part of twinning is output immediately the call is answered internally. The Call Start for this record differs dues to the user's **Mobile Dial Delay** setting. The External Targeting Cause indicates the external call was the result of user (U) mobile twinning (MT) settings. If the call had been answered before the mobile dial delay expired, no external call and therefore no record would be produced. When the call is completed the second record is output.

```
… 16:17:59,00:00:00,7,,O,9416,9416,,0,1000028,0,E203,Extn203,T9005,Line
5.1,0,0,,,,,,,,,,U MT,Extn203,9416,
```

```
… 16:17:58,00:00:07,9,207,O,
203,203,,1,1000027,0,E207,Extn207,E203,Extn203,0,0,,,,,,,,,,,,
```

Mobile Twinned Call Answered at the Mobile Twin

This is the same scenario as the example above except that the call is answered at the external mobile twinning destination. Unlike the previous example the external call record has a non-zero Call Time showing that the call was also answered externally.

```
… 16:17:04,00:00:06,9,,O,9416,9416,,0,1000026,0,E203,Extn203,T9005,Line
5.1,0,0,,,,,,,,,,U MT,Extn203,9416
```

```
… 16:17:02,00:00:06,11,207,O,
203,203,,1,1000025,0,E207,Extn207,E203,Extn203,0,0,,,,,,,,,,,,
```

Mobile Twinned Call Picked Up Using the Twinning Button

This is the same scenario as the example above, however after answering the call on the external twinned device, the user has picked it up internally by using a twinning button. The first two records are for the answered external call and are output when that call is picked up by the internal extension. The third record is output when the call is ended internally.

```
… 16:19:18,00:00:05,11,207,O,
203,203,,1,1000029,1,E207,Extn207,E203,Extn203,0,0,,,,,,,,,,,,
```

```
… 16:19:20,00:00:05,9,,O,9416,9416,,0,1000030,0,E203,Extn203,T9005,Line
5.1,0,0,,,,,,,,,,U MT,Extn203,9416
```

```
… 16:19:18,00:00:05,0,207,O,
203,203,,1,1000029,0,E207,Extn207,E203,Extn203,0,0,,,,,,,,,,,,
```

External Conference Party

This is similar to internal conferencing (see examples above) but the conference setup and progress records include External Targeting Cause codes for user (U) conference proposal (CfP) and user (U) conferenced (Cfd).

```
… 16:48:58,00:00:02,2,203,O,9416,9416,,0,1000066,1,E203,Extn203,T9005,Line
5.1,0,0,,,,,,,,,,U CfP,Extn203,,
```

```
… 16:48:37,00:00:04,3,203,O,
207,207,,1,1000064,1,E203,Extn203,E207,Extn207,7,0,,,,,,,,,,,,
```

```
… 16:49:04,00:00:08,0,203,O,9416,9416,,1,1000067,0,E203,Extn203,V11002,CO Channel
100.2,0,0,,,,,,,,,,,,
```

```
… 16:48:37,00:00:13,0,,O,,,,1,1000064,0,E207,Extn207,V11003,CO Channel
100.3,0,0,,,,,,,,,,,,
```

```
… 16:48:58,00:00:13,0,,O,9416,9416,,0,1000066,0,V11001,CO Channel 100.1,T9005,Line
5.1,0,0,,,Extn203,,,,,,,,U Cfd,Extn203,
```

Call Routed by Incoming Call Route

Call from external number 403 rerouted by incoming call route (ICR) for incoming line group 701 back out to 404.

```
2014/08/01 11:45:36,00:00:01,2,403,I,9404,,,0,1000007,0,T9001,Line 1.0,T9010,Line
10.0,0,0,0,n/a,,,,,,,,,ICR,ICR701,404
```

Two Outgoing External Calls Transferred Together

This scenario shows an outgoing call which is then transferred to another outgoing call.

```
2009/02/19 11:13:26,00:00:06,0,203,O,9403,9403,,0,1000012,1,E203,Extn203,T9001,Line
1.0,8,0,0,n/a,,,,,,,,,U,Extn203,,
```

```
2009/02/19 11:13:36,00:00:02,0,203,O,8404,8404,,0,1000013,0,E203,Extn203,T9002,Line
2.0,0,0,0,n/a,,,,,,,,,U XfP,Extn203,,
```

```
2009/02/19 11:13:26,00:00:11,0,8404,I,404,,,0,1000012,0,T9002,Line 2.0,T9001,Line
1.0,0,0,0,n/a,,,,,,,,,LINE Xfd,0.1038.0 13 Alog Trunk:2,,
```

Authorization code

In this example, an authorization code was used and the 0 indicates that it is invalid:

```
2014/02/20 11:04:59,00:00:00,0,319,O,,,,0,1000009,0,E319,Alice,V8000,U1 0.0,0,0,0,n/
a,,,,,,,,,U,Alice,
```

In this example, the authorization code is valid.

```
2014/02/20 11:04:59,00:00:00,0,319,O,,,,0,1000009,0,E319,Alice,V8000,U1 0.0,0,0,1,n/
a,,,,,,,,,U,Alice,
```

Related Links

Appendix: SMDR on page 837

Chapter 23: Single Server Support

The following scenarios are supported for combining system server applications onto a single Windows server PC.

In all cases, the individual requirements of each application as if installed on a separate server are still applicable. Also, depending on the application combination, additional restrictions and requirements may be applied as detailed below.

	Voicemail Pro	Customer Call Reporter	one-X Portal for IP Office	Minimum IP Office	Minimum PC Specification
1.	**16 Ports**	**150 Agents**	**–**	Release 5.0	As per each application.
2.	**8 Ports (4 TTS)**	**–**	**50 Simultaneous users**.	Release 6.0	2GHz Dual Core, 4GB RAM, Windows 2008 Server (32 or 64-bit).
3.	**16 ports (8 TTS)**	**50 Agents**	**150 Simultaneous users**.	Release 6.0	2GHz Quad Core, 6GB RAM, Windows 2008 64-bit. CCR run in Windows 2003 on a virtual server.

Voicemail Pro includes UMS, VB Scripting and 3rd party database operation. It also includes the installation of ContactStore if required.

Both ContactStore and one-X Portal for IP Office use Tomcat servers as part of the application. For scenarios with both installed, the redirect port setting of the ContactStore's Tomcat server should be configured to a port other than 8080.

The supported virtual servers are:

- **VMWare Server.**
- **Microsoft Virtual Server 2005 R2.**
- **Microsoft Server Hyper-V**.

When used in a virtual server configuration, Customer Call Reporter and one-X Portal each require a 2GB RAM virtual machine. Voicemail Pro and ContactStore each require a 1GB RAM virtual machine.

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W