Administering Centralized Users for an IP Office™ Platform Enterprise Branch

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

Purpose

This document describes how to administer endpoints as Centralized users in an IP Office Branch solution. Before using this document, make sure you have finished configuring IP Office in the branch environment.

This guide is a supplemental guide that provides the tasks required to add Centralized users to an IP Office enterprise branch. It is intended to be used in addition to *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*, document number 18-603853, which is the base guide that provides the common configuration tasks required to implement all IP Office enterprise branch deployments.

Document changes since last issue

The following changes have been made to this document for Release 9.1:

- Added administration content for E.129 and B.179 series phones.
- Consolidated information about 1100, 1200, E.129, and B.179 series phones in one chapter.
- Added Communication Manager features for ATA users using analog phones.
- Adding identity certificates.

Related resources

Documentation

The following table lists the related documents for the IP Office Branch solution. Download the documents from the Avaya Support website at http://support.avaya.com/.

Document number	Title	Use this document to	Audience
Overview			
15-604258	*Avaya IP Office™ Platform Solution Description*	Understand IP Office platforms, components, and features.	• Sales Engineers
Not numbered	*IP Office Release 9.0 deployed as a Branch Product Offer*	Provides a technical and commercial overview of the IP Office Branch solution.	• Sales Engineers • Reference Architects • Solution Architects
15-601041	*IP Office Product Description*	Understand IP Office systems and requirements.	• Sales Engineers • Reference Architects
Not numbered	*Avaya Aura® System Manager Overview and Specification*	Understand how System Manager works and the performance specifications for the product	• Sales Engineers • Reference Architects
Not numbered	*Avaya Aura® Communication Manager Feature Description and Implementation*	Understand how to use and implement Communication Manager features.	• Sales Engineers • Reference Architects • Solution Architects
Reference Configuration			
15–604253	*Avaya IP Office™ Platform in a Branch Environment Reference Configuration*	Understand the architecture and network engineering requirements for the solution	• Reference Architects • Solution Architects • Sales Engineers
Implementation			
18-603853	*Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*	Deploy an IP Office enterprise branch	• Implementation Engineers • Solution Architects
03-604053	*Deploying IP Office as a Distributed Enterprise Branch in a Communication Server 1000 Environment with Avaya Aura® Session Manager*	Deploy an IP Office enterprise branch with CS 1000	• Implementation Engineers • Solution Architects
15-601042	*Deploying Avaya IP Office™ Platform IP500/IP500 V2*	Install an IP Office system using an IP500 or IP500 V2 control unit.	• Implementation Engineers • Solution Architects
Not numbered	*Implementing Avaya Aura® System Manager*	Implement System Manager and System Platform	• Implementation Engineers • Solution Architects

Document number	Title	Use this document to	Audience
555-245-600	*Avaya Application Solutions: IP Telephony Deployment Guide*	Understand deployment options and provide overview information	• Implementation Engineers • Solution Architects Sales Engineers
15-601067	*Avaya IP Office Implementing Embedded Voicemail*	Implement Embedded Voicemail	• Implementation Engineers
15-601064	*Avaya IP Office Implementing Voicemail Pro*	Implement Voicemail Pro	• Implementation Engineers
Not numbered	*Avaya Port Matrix: IP Office 9.0* (available at https:// support.avaya.com/security under the **Avaya Product Port Matrix Documents** link)	Determine the correct ports to use for the IP Office Branch solution	• Implementation Engineers • Solution Architects
Not numbered	*IP Office: Avaya Radvision Installation Notes*	Deploy Radvision endpoints with IP Office	• Implementation Engineers • Solution Architects
Not numbered	*Avaya Aura® Communication Manager Release 6.2 and Radvision SCOPIA Release 7.7 and 8.0 Interoperability Day 180 Solution Quick Setup*	Deploy Radvision endpoints in the Avaya Aura® infrastructure	• Implementation Engineers • Solution Architects
Administration			
15-604263	*Administering Centralized Users for an IP Office™ Platform Enterprise Branch*	Add Centralized users to an enterprise branch	• Implementation Engineers
15–604268	*Migrating an IP Office or B5800 Branch Gateway to an IP Office Enterprise Branch*	Understand migration procedures for the IP Office Branch solution	• Implementation Engineers • Solution Architects • Administrators
Not numbered	*Administering Avaya Aura® System Manager*	Administer System Manager	• Implementation Engineers • Solution Architects
03-603324	*Administering Avaya Aura® Session Manager*	Administer Session Manager	• Implementation Engineers • Solution Architects
Not numbered	*Avaya IP Office Administering Embedded Voicemail*	Configure Embedded Voicemail	• Implementation Engineers
15-601063	*Avaya IP Office Administering Voicemail Pro*	Configure Voicemail Pro	• Implementation Engineers
Not numbered	*Avaya WebLM Administration Guide*	Administer a WebLM server	• Implementation Engineers

Document number	Title	Use this document to	Audience
Not numbered	*Administering Avaya WebLM (standalone)*	Administer a standalone WebLM server	• Implementation Engineers
White Papers			
Not numbered	*Avaya IP Voice Quality Network Requirements*	Understand Avaya network requirements for good voice quality	• Solution Architects • Reference Architects • Sales Engineers

Training

Obtain the following certifications before deploying or administering the IP Office Branch solution:

- ASPS — Avaya IP Office Deployed as a Branch
- ACSS — Avaya Aura® Session Manager and System Manager
- ACSS — Avaya Small and Medium Enterprise (SME) Communications

To obtain a certification, you must pass an exam. Each certification you obtain is valid for one year.

The following table lists the main IP Office Branch courses you must obtain. For a complete list of courses available for each certification assessment, visit the Avaya Learning web site at http://www.avaya-learning.com/.

Table 1: Courses for IP Office as a Branch Deployment

Course code	Course title
Knowledge Transfers (KTs)	
8U00010O	Knowledge Transfer: Avaya IP Office Deployed as a Branch Pre-GA KT
Knowledge Access License 5U00130E	
5U00130E_TH	Knowledge Access: IP Office Deployed as a Branch Theory
5U00130E_ATM	Knowledge Access: IP Office Deployed as a Branch Ask the Mentor
5U00130E_Lab	Knowledge Access: IP Office Deployed as a Branch Practise Lab Workshop

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:

  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.

  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:

  - Enter a key word or key words in the Search Channel to search for a specific product or topic.

  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

  * **Note:**

     Videos are not available for all products.

Web sites

Information to support IP Office can be found on a number of web sites.

- Avaya (http://www.avaya.com)

  The official web site for Avaya. The front page also provides access to individual Avaya web sites for different countries.

- Avaya Enterprise Portal (http://partner.avaya.com)

  This is the official web site for all Avaya Business Partners. The site requires registration for a user name and password. Once accessed, the site portal can be individually customized for what products and information types you wish to see and to be notified about by email.

- Avaya Support (http://support.avaya.com)

  Contains documentation and other support materials for Avaya products.

- Avaya IP Office Knowledge Base (http://marketingtools.avaya.com.knowledgebase)

  Provides access to an on-line regularly updated version of the IP Office Knowledge Base.

- Avaya University (http://www.avaya-learning.com)

  This site provides access to the full range of Avaya training courses. That includes both on-line courses, course assessments and access to details of classroom based courses. The site requires users to register in order to provide the user with access to details of their training record.

- Avaya Community (http://www.aucommunity.com)

  This is the official discussion forum for Avaya product users. However it does not include any separate area for discussion of IP Office issues.

- Other non-Avaya Web sites — There are several third-party web forums that discuss IP Office. These can be a useful source of information about how IP Office is used. Some of these

forums require you to be a member and to register. These are not official Avaya forums and their content is not monitored or sanctioned by Avaya.

- Tek-Tips (http://www.tek-tips.com)
- IP Office Info (http://ipofficeinfo.com)
- Yahoo Groups (http://groups.yahoo.com/group/ipoffice)
- PBX Tech (http://www.pbxtech.info/forumdisplay.php?f=8)

Support

Go to 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.

Chapter 2: Overview of IP Office as an enterprise branch

IP Office supports the deployment of IP Office as an enterprise branch to provide a communications solution that is adaptable to meet the growing needs of an enterprise branch network while providing investment protection of the installed hardware platform and phones. An IP Office enterprise branch deployment can be implemented on an IP Office Standard Mode (Essential or Preferred) system. The IP Office system can be installed as an independent, standalone branch, or be connected to the Avaya Aura® network and migrated to a Distributed, Centralized, or Mixed enterprise branch to provide specific features and applications to meet the needs of individual employees in each branch location. For more information about the branch evolution phases, see *Avaya IP Office™ Platform Solution Description*, document number 15-604258.

In addition to centralized SIP endpoints, IP Office can concurrently support other IP and TDM endpoints for a community of Centralized users and IP Office users in the same branch. Ideal for enterprises wanting applications deployed in customer data centers or in the branch itself, an IP Office branch can effectively deliver a range of communication tools without complex infrastructure and administration.

This guide is a supplemental guide that provides the tasks required to add Centralized users to an IP Office enterprise branch. It is intended to be used in addition to *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*, document number 18-603853, which is the base guide that provides the common configuration tasks required to implement all IP Office enterprise branch deployments.

Related Links

Branch deployment options

An IP Office system can be deployed as a Distributed, Centralized, or Mixed enterprise branch. A new IP Office system can be installed with one of these branch deployment options or a standalone IP Office system that is already installed can be migrated to one of these deployment options.

- **Distributed enterprise branch deployment option** — With this option, all users in a branch are IP Office users. IP Office users get their telephony features and services from the local IP Office system. IP Office users were referred to as distributed users, local users, or native users.

  IP Office users with non-IP phones are connected to the IP Office system while IP Office users with IP endpoints can be administered with IP Office as their controller. Access to and from the rest of the Avaya Aura® network is via the IP Office system's SM Line, which connects to Avaya Aura® Session Manager across the enterprise WAN. This connection allows for VoIP connectivity to other sites in the enterprise, to centralized trunking, and to centralized applications such as conferencing and Avaya Aura® Messaging.

- **Centralized enterprise branch deployment option** — With this option, all users in a branch are Centralized users. A Centralized user is a user whose call processing is controlled by Avaya Aura® Communication Manager Feature Server or Evolution Server in the enterprise core. During normal operation, the Centralized user gets their telephony features and services from the Communication Manager Feature Server or Evolution Server. Through the core Session Manager, the Centralized user can also access local PSTN trunks and services, such as local paging, local auto-attendant, and local Meet-me conferencing, on the IP Office system in the branch. If WAN connectivity to Session Manager is lost, the Centralized user gets basic services from the local IP Office system. When connection to Session Manager is available again, failback occurs either automatically or by manual administrative action where call processing for the Centralized user is returned to being controlled by Avaya Aura®.

  A Centralized user must be configured on Session Manager, on Communication Manager, and on the IP Office system. On the IP Office system, the Centralized user must have either a SIP extension or an analog extension. There are two types of centralized users:

  - Centralized SIP user — a user configured as a Centralized user whose associated extension is a SIP extension.
  - ATA user — a user configured as a Centralized user whose associated extension is an analog extension or analog fax device.

  Mixed enterprise branch deployment option — With this option, there are Centralized users and IP Office users in a single branch. The Centralized users get their telephony services delivered by the Communication Manager Feature Server or Evolution Server in the core and the IP Office users get their telephony services delivered by the local IP Office system.

Related Links

Supported telephones

IP Office deployed as a Centralized or Mixed enterprise branch supports the following centralized phones:

- The following Avaya 9600 series phones running SIP firmware:
    - 9620 SIP 2.6.12
    - 9630 SIP 2.6.12
    - 9640 SIP 2.6.12
    - 9650 SIP 2.6.12
    - 9601 SIP 6.4
    - 9608 SIP 6.4
    - 9611G SIP 6.4
    - 9621G SIP 6.4
    - 9641G SIP 6.4
- Avaya one-X® Communicator SIP 6.2 (audio only)
- E.129 series SIP 1.25.1.1
- B.179 series SIP 2.4 phones
- 11xx and 12xx series SIP 4.4 phones

> ⊛ **Note:**
>
> The 9600 series SIP phones and Avaya one-X® Communicator SIP are supported only as Centralized phones for use by Centralized users. They are not supported as IP Office phones for use by IP Office users.
>
> For more information about IP Office phones, see *Deploying Avaya IP Office™ Platform IP500/IP500 V2*, document number 15-601042.

Related Links

[Overview of IP Office as an enterprise branch](#) on page 13

Direct media setting on Avaya Aura® Communication Manager

In IP Office Centralized or Mixed enterprise branch deployments where there are Centralized users, you must enable the Initial IP-IP Direct Media parameter in Avaya Aura® Communication Manager. This is required to prevent media flow from unnecessarily crossing the WAN to a central

Communication Manager media resource. Enabling this parameter is especially important for the following types of calls:

- Calls between Centralized users within the branch
- Calls between Centralized users and local IP Office trunks

For more information, see Configuring direct media on Communication Manager on page 72.

Related Links

Overview of IP Office as an enterprise branch on page 13

Chapter 3: Centralized users

A Centralized user is a user whose call processing is controlled by Avaya Aura® Communication Manager Feature Server or Evolution Server in the enterprise core. During normal operation, the Centralized user gets their telephony features and services from core applications such as the Communication Manager Feature Server or Evolution Server. Through the core Avaya Aura® Session Manager the Centralized user can also access local PSTN trunks and services on the IP Office in the branch. If WAN connectivity to the Avaya Aura®Session Manager is lost, the Centralized user automatically gets basic services from the local IP Office. When connection to Avaya Aura®Session Manager is available again, failback occurs either automatically or by manual administrative action where call processing for the Centralized user is returned to being controlled by Avaya Aura®Session Manager.

A Centralized user must be configured on the Avaya Aura®Session Manager, on Communication Manager, and on the IP Office. On the IP Office, the Centralized user must have either a SIP extension, an analog extension, or analog fax device. There are two types of Centralized users:

- Centralized SIP user — a user configured as a Centralized user whose associated extension is a SIP extension.

- ATA user — a user configured as a Centralized user whose associated extension is an analog extension or analog fax device.

> **Note:**
>
> Along with standard analog phones, IP Office also introduces support for analog fax devices as ATA users.

Centralized phones are supported in branches that are deployed as a Centralized enterprise branch or Mixed enterprise branch. IP Office allows only the supported Centralized phones to register as centralized. When a Centralized phone tries to register to a SIP extension that is associated with a user that is configured as a Centralized user, IP Office checks the phone type and prevents registration if the phone is not supported.

Centralized phones register to Avaya Aura®Session Manager and receive services from the Communication Manager Feature Server or Evolution Server in the Avaya Aura® network at the central headquarters site but are physically located at the IP Office site. The Centralized phones are configured to use the local IP Office site to make and receive calls when connection to the Avaya Aura® network is not available. When this happens, the IP Office is acting as a survivable gateway for the phones. This can be in addition to trying to register with an alternate Avaya Aura® Session Manager.

Voicemail for the Centralized phones is provided by Avaya Aura® Messaging or Modular Messaging. When Avaya Aura® Messaging or Modular Messaging is used as the central voicemail system, at

each branch you have the option to still use the local Embedded Voicemail for auto attendant operation and for announcements to waiting calls or Voicemail Pro for customized call flow actions created for the mailbox. For more information about voicemail, see *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*, document number 18-603853.

Centralized phones can be provisioned from either a central HTTP server or from the IP Office located in the branch where the Centralized phones are located.

⚠️ **Warning:**

> **Telephony Feature Restrictions** — When registered with the IP Office system in survivability mode, the range of telephony features available to the Centralized phone will be limited compared to the features provided to the phone normally by the Communication Manager Feature Server or Evolution Server.

Survivability operation

During normal operation, Centralized phones register with Avaya Aura®Session Manager and receive services from the Communication Manager Feature Server or Evolution Server at headquarters. However, these phones can also be configured to automatically failover to their local IP Office system for survivable telephony services when the connection to the Avaya Aura® Session Manager is lost for any reason. When the Centralized phones lose their connection to Session Manager, this is referred to as the phones being in the Rainy day mode.

✳️ **Note:**

> Although the Centralized users in Rainy day mode receive their telephony services from the IP Office system, the features and functionality that are provided are *not* the same as those for the IP Office users. Not all IP Office features and functionality apply to the Centralized user. For more information, see Supported phones in Centralized deployments on page 31.

Each Centralized phone monitors its own connectivity to the Avaya Aura® Session Manager (and secondary Avaya Aura® Session Manager if configured). If it detects loss of connectivity, it automatically registers with the IP Office and switches to survivability operation. There will be a short unavailability of services while failing over.

With default timer settings on the phones and on the IP Office, the Centralized phones in the branch will be able to make and receive calls processed by the IP Office within 3 minutes after a WAN failure. When the failback policy is set to **Auto** and the phone detects that connection to the Avaya Aura® Session Manager is available again, it dynamically registers with it and switches back to normal operation. If the failback policy is set to **Manual**, failback to normal operation must be initiated manually when connectivity to Avaya Aura® Session Manager is restored. For more information about the failback policy, see About the global failback policy on page 19.

> ⓘ **Important:**
>
> **Branch Survivability Settings**. Centralized phones entering survivability mode with the branch occurs in parallel with the branch loosing whatever centralized call control and trunk services the branch is configured to receive from Avaya Aura® Session Manager. Therefore the calls and call routing applied to IP Office phones and Centralized phones might be limited.

SIP controller monitoring

Both the IP Office system and the Centralized phones perform monitoring of the Avaya Aura® Session Manager availability.

- **IP Office monitoring** — IP Office monitoring determines when the connection to the Session Manager is lost and when it is recovered. When IP Office determines that the connection is lost, it goes into Rainy day mode. In Rainy day mode, Session Manager handles calls differently and allows Centralized phones to register with it.

- **Centralized phone monitoring** — Centralized phone monitoring determines when it should failover to another SIP controller. For example, see [9600 Series SIP phone features available during failover](#) on page 41.

IP Office system line monitoring

The IP Office system sends regular OPTIONS messages to any SM Lines in its configuration. The Proactive Monitoring and Reactive Monitoring settings on the IP Office system's **Telephony > SM** tab set how often the OPTIONS messages are sent in seconds. The Proactive Monitoring setting is used for an SM Line currently thought to be in service. The Reactive Monitoring setting is used for an SM Line currently thought to be out of service. The Monitoring Retries option sets the number of times the IP Office system attempts to send an OPTIONS request to Session Manager before the SM Line is marked out-of-service. IP Office will set an SM Line out-of-service only after successive (as configured in the Monitoring Retries field) OPTIONS requests, each at regular (Proactive Monitoring) intervals, to the Session Manager have failed. An OPTIONS monitoring request is considered to have failed if no response is received with 32 seconds (SIP Timer F), or if a response is received with SIP response code 408, 500, 503 or 504. If a response is received from Session Manager with any other response code, then the OPTIONS monitoring is considered to have succeeded and the SM Line is treated as in service. An SM Line remains in service while the connection test mechanism is in progress.

Failback policy

The failback policy feature is used to determine how the Centralized SIP phones failback to normal operation after connectivity to Avaya Aura® Session Manager is restored. You must use two different parameters to configure this feature. One parameter is the global failback policy parameter that is configured through Avaya Aura® System Manager for the Session Manager and impacts all Session Manager SIP phones in the enterprise. The other parameter is the IP Office failback policy

parameter that is configured on each IP Office and impacts the operation of that IP Office. The settings for these two parameters must match.

The global failback policy parameter configured in System Manager can be set to Auto (the default) or Manual. The setting is applied to all phones in all branches in the network. It cannot be set per-branch. When set to Auto, the centralized SIP phones will automatically failback to normal (sunny-day) operation when connectivity to Session Manager is restored. In addition, for networks that include two Session Managers for redundancy, when connection to the primary Session Manager is lost, failback from the secondary Session Manager to the primary Session Manager will occur automatically when the primary Session Manager comes back into service.

When the global failback policy is set to Manual, the failback to normal operation must be initiated manually when connectivity to Session Manager is restored. For networks that include two Session Managers for redundancy, when connection to the primary Session Manager is lost, failback from the secondary Session Manager to the primary Session Manager must also be performed manually when the primary Session Manager comes back into service.

The option to set the global failback policy to Manual is provided because there may be occasions when you do not want the SIP phones to automatically failback to normal operation when connectivity to Session Manager is restored. For example, if the network is experiencing constant fluctuations causing frequent switching between the Sunny day and Rainy day mode with service interruptions during the transitions, you might want to first verify the network is stable before failback to normal operation occurs. When you set the global failback policy to Manual, you can manually initiate the failback after you determine that the network is stable.

Configuring the global failback policy in System Manager

Before you begin

Determine your global failback policy regarding phone failback before you perform this task. The setting configured in this task is applied to all phones in all branches in the network. The global failback policy is set to Auto by default. The setting can be changed to Manual if you determine you want to manually initiate phone failback after Session Manager returns to the in-service state.

Procedure

1. On the System Manager console, under **Elements**, click **Session Manager**.

2. In the left navigation pane, click **Session Manager Administration**.

3. In the **Global Settings** section, in the **Failback Policy** drop-down box, do one of the following:

   - Select **Auto** if you want the centralized SIP phones to automatically failback to normal operation when connectivity to Session Manager is restored. In addition, for networks that include two Session Managers for redundancy, failback from the secondary Session Manager to the primary Session Manager will occur automatically when the primary Session Manager comes back into service.

   - Select **Manual** if you do not want the centralized SIP phones to automatically failback to normal operation when connectivity to Session Manager is restored. The failback to

normal operation must be initiated manually when connectivity to Session Manager is restored.

4. Click **Save**.

Configuring the failback policy in IP Office Manager

About this task

The failback policy configured in IP Office Manager must match the global failback policy configured in Avaya Aura® System Manager.

Procedure

1. From the System Manager console, under **Elements**, select **IP Office**.

2. In the left navigation pane, click **System Configuration**.

3. On the **IP Office System Configuration** page, select the IP Office device whose system configuration you want to edit.

4. Click **Edit**.

   The IP Office Manager application is launched.

5. In the left navigation pane, click **System**.

6. Click the **Telephony** tab.

7. Click the **SM** tab.

8. In the **Failback Policy** drop-down box, do one of the following:

   • Select **Auto** if you want the centralized SIP phones to automatically failback to normal operation when connectivity to Session Manager is restored. In addition, for networks that include two Session Managers for redundancy, failback from the secondary Session Manager to the primary Session Manager will occur automatically when the primary Session Manager comes back into service.

   • Select **Manual** if you do not want the centralized SIP phones to automatically failback to normal operation when connectivity to Session Manager is restored. The failback to normal operation must be initiated manually when connectivity to Session Manager is restored.

9. Click **OK**.

10. Select **File > Save Configuration**.

    The reboot mode is set to Merge.

Initiating a manual failback

About this task

Use this task to initiate a manual failback for an IP Office after connection to Session Manager has been restored. When you perform this task, the manual failback is executed one time.

Procedure

1. On the System Manager console, under **Elements**, click **IP Office**.

2. In the left navigation pane, click **Initiate FailBack**.

3. On the **IP Office Manual FailBack** page, click the check box for the IP Office for which you want to initiate the failback.

   ✱ **Note:**

   Only IP Office systems whose failback policy is set to **Manual** will be listed.

4. To initiate the failback immediately, click **Now**.

5. To initiate the failback to occur at a specified time, click **Schedule**. Then do the following:

   a. Set the date and time when you want the failback to occur.

   b. Click **Schedule**.

ATA users

An Analog Terminal Adapter (ATA) user in the IP Office Branch is a Centralized user whose associated extension is an analog extension. To support the ATA functionality, IP Office acts as a SIP gateway for analog endpoints registering on their behalf to Avaya Aura® Session Manager.

This allows analog devices attached to the IP Office to be deployed as Centralized users, whose calls are handled by the Session Manager and Communication Manager in the Avaya Aura® core. They are administered as users on the Session Manager and on the Communication Manager in the Avaya Aura® core and are viewed by the Session Manager and Communication Manager as SIP users, even though they use analog devices on the IP Office.

Fax devices configurations

You can deploy analog phones or analog fax devices attached to the IP Office as ATA users. The configuration of a Centralized ATA user on Session Manager and Communication Manager is the same for a fax ATA user and a phone ATA user. This means, it will appear as a SIP phone to Session Manager and Communication Manager. The fax ATA user and a phone ATA user have an Analog extension on the IP Office. The recommended configuration of the "Equipment Classification" for the fax analog extension is "Standard Telephone" and not "Fax machine". The default ATA user template in System Manager can be used for fax ATA users and phone ATA users. The recommended configuration for fax support on the SM Line in the IP Office is *T.38*.

Alternatively, you can configure the fax support on the SM Line as *G711* or *T.38 fallback*. In this case, configure the "Equipment Classification" for the fax analog extension either as:

- *Standard Telephone* where IP Office performs fax tone detection.

- *Fax Machine* where IP Office avoids the renegotiation after detecting a fax tone. This is appropriate only for fax devices that do not include an attached handset and are never used to make or receive voice calls. Equipment classification as *Fax Machine* is not supported if the SM Line fax transport is *T38*.

Communication Manager features

Communication Manager in Avaya Aura® core provides several benefits for ATA users with analog phones. To invoke certain Communication Manager features during a call, the ATA user must press the **Flash** button on the analog phone and then dial the Feature Access Codes (FAC) configured on Communication Manager. To invoke Communication Manager features outside a call, the ATA user must dial the FAC configured on Communication Manager.

IP Office relays the dialed string from the analog phone into a **SIP INVITE** that is sent to Session Manager. Session Manager sends the **SIP INVITE** to Communication Manager. IP Office does not process the dialed string and does not identify the Communication Manager feature. IP Office only collects the dialed digit string of the FAC based on the configured value of the **Dial Delay Time** field under **System** > **Telephony**.

 Note:

To support the ATA feature, the recommended value of the **Dial Delay Time** field in the IP Office configuration is *4* seconds. This is the default value of the IP Office configuration item in the U.S. but this is not applicable to other countries.

For more information about the Communication Manager features, see *Avaya Aura Communication Manager Feature Description and Implementation*, document number 555-245-205.

The following Communication Manager features have been successfully tested from analog phones of IP Office ATA users:

Name	Description
Abbreviated Dialing (AD)	The AD feature reduces the number of digits to dial a call. Instead of dialing the entire number, a short code is dialed to access the number. The system then dials the stored number automatically. AD is sometimes called speed dialing.
Announcement Record/ Listen	The Announcements feature plays recordings for callers in the enterprise. ATA users can use FAC to record and manage announcements from analog phones.
Call Detail Recording (CDR) Account code	The CDR Account code feature provides the FAC used prior to entering an account code for CDR.

Name	Description
Call Forwarding	ATA users can use one of the following Call Forwarding capabilities to redirect any incoming calls to another destination: • **Activation** • **Deactivation** • **Busy/Don't Answer** • **All FAC**
Call Park	ATA uses can use the Call Park feature to park a call. ATA users can then use the Answer Back Access Code FAC to retrieve or answer a parked call.
Call Pickup	Using the Call Pickup feature, an ATA user can answer another user's call. To use this feature, the ATA user and the other user must be a part of the same call pickup group.
Directed Group Call Pickup	Using the Directed Group Call Pickup FAC, ATA users can answer a call that rings at another extension without being a member of the pickup group.
Enhanced (EC500) Activation Feature Access Code	The EC500 Activation Feature Access Code feature helps in the delivery of calls to a cell phone when the associated office telephone receives a call. The Enhanced EC500 Deactivation Feature Access Code disables the delivery of calls to the cell phone when the associated office telephone receives a call.
Extended Call Pickup	The Extended Call Pickup feature permits users in one pickup group to answer calls that come in for users in another pickup group. The feature allows the administrator to define one or more extended pickup groups and calls are "picked-up" by entering the Extended Call Pickup FAC and the 1-2 digit number to indicate the group of the ringing call to be picked up.
Hunt Group Busy	Hunt group members use the Hunt Group Busy Activation FAC to make the extension unavailable and the Hunt Group Busy Deactivation FAC to make the extension available.
Last Number Dialed (LND)	LND is also called Last Number Redial. ATA users can dial FAC to make a call to a number, which was last dialled instead of dialing the number again.
Limit Number of Concurrent Calls (LNCC)	The LNCC feature restricts the number of calls that can terminate on an active ATA terminal to a single call. When the LNCC feature is enabled and the user is on a call, subsequent incoming calls receive a

Name	Description
	busy signal or no coverage path, or follow the coverage path if administered.
Per-call CPN/Name Block	ATA users can use FAC to turn on/off Calling Party Number blocking for a trunk group if it has been disabled. When users dial this code, the calling party number is not sent to the public network.
Priority Calling	ATA users can use FAC to enable priority calling, which is a special type of call alert between internal telephone users, including the attendant. When the calling party uses Priority Calling, the called party hears a distinct ring.
Remote Send all Calls	To route ATA station calls to remote stations, and to activate or deactivate the Send All Calls feature, dial FAC. This feature requires console permissions.
Whisper Paging	ATA users can use FAC to place a page to another user's telephone when active on a call. Only the paged user hears the page not the other parties on the call.

The following features are tested from analog phones of IP Office ATA users without Communication Manager FAC:

Name	Description
Abort Transfer	The Abort Transfer feature stops the transfer operation whenever a user presses the **Flash** button in the middle of the transfer operation or when the user hangs up.
Authorization Codes	The Authorization Codes feature extends the control of calling privileges for system users.
Call transfer	ATA users can transfer a call using the following steps: 1. To place an active call on hold, press the **Flash** button on the analog phone. 2. Dial the second call and hang up. IP Office sends the appropriate message over the SM Line to preform call transfer.
Consultation hold	To make a consultation call to a different user and to place the active call on hold, an ATA station press the **Flash** button.
Hold/Resume	To place a call on hold or to resume a call, ATA users can press the **Flash** button on the analog phone. When the ATA users presses the **Flash** button, IP Office sends a corresponding **INVITE** with **send only/send recv** over the SM Line to Session

	Manager, which in turn delivers it to Communication Manager.

Chapter 4: File server for settings and firmware files

The Centralized SIP phones get their settings files and their firmware files from an HTTP file server. The file server can be set up in one of two ways. One way is to use a central file server in the data center for the Centralized SIP phones in the different branches. The other way is to use the IP Office in each branch as the file server for the Centralized SIP phones in that branch. Using a central file server provides the advantage of simpler centralized installation and maintenance. Using the IP Office in each branch provides an advantage primarily in terms of the WAN bandwidth usage for phone firmware upgrades where the firmware files are pushed to the branch only once and then loaded locally by multiple Centralized SIP phones in that branch. Regardless of the method chosen, the phones must be set up using DHCP to contact either the central file server or the local IP Office file server in their respective branch.

Enabling the DHCP server on the IP Office

About this task

A DHCP server has to be set up to provide the correct HTTP server address to the phones. Use this procedure to enable the DHCP server on the IP Office. This procedure must be performed for each IP Office.

Procedure

1. Start Manager and connect to the IP Office system.

2. In the left navigation pane, click **System**.

3. Click the **LAN** tab.

4. In the **LAN Settings** tab, under **DHCP Mode**, click **Server**.

5. Click the **Advanced** button.

6. Click the **Apply to Avaya IP Phones only** check box to select this option.

About using external DHCP servers

As an alternative to enabling the DHCP server on each IP Office system, external DHCP servers can be used. In this case, the DHCP server must be configured to provide the IP address of the HTTP file server in the DHCP response to the phone. The phones use Option 242 in the DHCP response, except the 11xx/12x and E.129 phones that use Option 66. If you cannot provide the IP address of the HTTP file server using DHCP, then you must manually input this address to every phone using the keypad interface of the phone.

Files and certificates required for the file server

You must load all the configuration files, firmware files, and certificates that are required by the Centralized SIP phones on the file server. If IP Office is used as the file server, load the files on the IP Office System SD card. You can place the files manually on the System SD card or load the files remotely using the System Manager file transfer mechanism. This mechanism allows you to load files to multiple IP Office systems in bulk. See Using the System Manager File Transfer feature to load files to the IP Office system on page 29. For more information, see the configuration files that are required by specific types of Centralized SIP phones in Supported phones in Centralized deployments on page 31.

Downloading the System Manager CA root certificate

About this task

Use this task to download the System Manager CA root certificate to the file server.

Procedure

1. On the System Manager console, under **Services**, click **Security**.

2. In the left navigation pane, click **Certificates > Authority**.

3. In the left navigation pane, under **CA Functions**, click **Basic Functions**.

4. Click the **Download pem file** link.

5. Save the file in the appropriate folder on the file server.

6. Rename the file to have a **.txt** extension.

Using a central file server for Centralized SIP phone files

About this task

You are able to use a central file server for the Centralized SIP phones, unless there is a mix of 96x0 H.323 phones and 96x0 SIP phones located in the enterprise branch deployment.

Procedure

1. Prepare all the required files on the central file server as appropriate.

2. Modify the DHCP server setting so that the DHCP responses to the phones provide the address of the central file server rather than that of the IP Office as the HTTP server.

3. If the IP Office will be used as the DHCP server for the phones, the following changes must be made to the IP Office system configuration:

   a. Open IP Office Manager and receive the IP Office configuration.

   b. In the left navigation pane, click **System**.

   c. Click the **System** tab.

   d. In the **HTTP Server Address IP** field, enter the IP address of the central file server.

   e. In the **Phone File Server Type** drop-down box, select **Custom**.

   f. Click **OK**.

Using System Manager File Transfer to load files to the IP Office system

About this task

System Manager provides a file transfer mechanism that allows you to remotely load files to multiple IP Offices in bulk. Use this procedure to send files from System Manager to the IP Office System SD card. The maximum file size allowed is 30 MB.

✳ Note:

The Embedded File Management feature in IP Office Manager can also be used to load files to the IP Office system. However, this method does not support pushing the files to multiple IP Offices in bulk.

✳ Note:

The System Manager file transfer feature does not support the transfer of nodal PLDS license files.

Procedure

1. On the System Manager console, under **Elements**, click **IP Office**.

2. In the left navigation pane, click **File Transfer**.

3. On the **IP Office File Transfer** page, in the **Select File Type** drop-down box, select **Other**.

4. For the **Upload Files To SMGR Repository** field, click the **Browse** button and select the file you want to upload.

5. In the **IP Office Destination Folder Location** field, enter the appropriate location. The default location is **SYSTEM\PRIMARY**.

6. Under **Device List**, click the check box for each IP Office to which you want to upload the file.

7. Click **Commit**.

8. Do one of the following:

   • Click **Now** to upload the files to the IP Office now.

   • Click **Schedule** to upload the files at a schedule time.

   ✱ **Note:**

   If you scheduled the file transfer, do not delete the file until the scheduled operation is completed. If the file is deleted prior to the completion of the scheduled operation, the operation will fail.

Chapter 5: Supported phones in Centralized IP Office Branch deployments

Deployment of phones as Centralized users is different than the deployment of phones as IP Office users. The operation of these phones when deployed as Centralized users is also different from the operation of the same types of phones, with the same firmware, when deployed as IP Office users.

When deploying phones as Centralized users, you must configure the phones as users on the central Avaya Aura® Session Manager and Avaya Aura® Communication Manager. You must also configure the phones as Centralized users on IP Office. During normal Sunny day operation, the phones register to the central Avaya Aura® Session Manager. The Avaya Aura® Communication Manager in the enterprise core handles call processing.

After losing WAN connectivity to Avaya Aura® Session Manager, the phones failover and register to the local IP Office for survivability in Rainy day mode. The phones fail back to Avaya Aura® Session Manager when connectivity becomes available.

9600 series SIP phones deployed as Centralized users in IP Office Branch deployments

IP Office Branch supports 9600 series phones running SIP firmware as Centralized users.

Centralized 9600 series SIP phone settings

Some of the settings used by the Centralized phones are set by Avaya Aura® Session Manager PPM, according to values administered in Avaya Aura® System Manager. Additional settings are set through the phones' settings file, which is loaded by each Centralized phone from the file server when the phone is started. The file server used for the Centralized phones can be a central file server or the IP Office in each branch.

The default phone settings file is `46xxsettings.txt` file. This file can be modified and renamed to provide customized settings for different phones. The settings file contains parameters that are used to customize the Centralized phones for an enterprise. For example, the settings file must include the address of the primary Session Manager with which the SIP phones must register. Since this address is different in each enterprise, this parameter must be customized for each enterprise.

The settings file can typically be the same for the Centralized phones in multiple branches when System Manager is used to provision the unique parameters required for each branch. One key parameter that must be different for the phones in each branch is the address of the survivable IP Office in the local branch. The User Management administration feature in System Manager enables this parameter to be pushed to the phones through the Session Manager PPM and thus does not have to be provisioned in the settings file. This allows the same settings file to be used for different branches in the enterprise.

An alternative to using Session Manager PPM to provision the unique parameters for each branch is to provision these parameters in the settings file. This alternative requires a different settings file for each branch and is not practical if a central file server with one common settings file is used to provision the Centralized phones. However, if the IP Office is used as the file server to provision the Centralized phones, it is possible to configure a different settings file for each branch. In addition to the address of the survivable IP Office in the local branch, there may be other parameters, such as time-zone, that are unique for each branch and would require configuration of different settings files.

For a description of all parameters in the `46xxsettings.txt` file, see *Avaya one-X*^{TM} *Deskphone SIP 9608, 9611G, 9621G, 9641G Administrator Guide*, document number 16–603813.

This topic provides a list of parameters in the settings file that must be configured for Centralized enterprise branch deployments. These parameters require changing the default setting. Also provided is a list of parameters that are relevant to enterprise branch deployments that, depending on the specific deployment, may require configuration.

Parameters that must be configured for Centralized enterprise branch deployments

- **SIMULTANEOUS_REGISTRATIONS**

  This parameter must be set to match the number of Session Managers.

  When there is a single Session Manager, the 9600 Series SIP phones perform alternate registration with either the Session Manager when available or the survivable IP Office. This is done by setting the SIMULTANEOUS_REGISTRATIONS parameter to 1.

  When operating in a network deployment that includes Session Manager redundancy, the phones will do simultaneous registration with both Session Managers (with the highest priority controller set as the active controller). This is done by setting the SIMULTANEOUS_REGISTRATIONS parameter to 2 (the number of Session Managers). Simultaneous registration is supported between Session Managers but not between an Session Manager and an IP Office.

- **SIP_CONTROLLER_LIST**

  This setting should contain the IP address, port, and transport method (TLS or TCP) for the primary Session Manager that the phone should use.

  ✳️ **Note:**

  The secondary Session Manager, if applicable, and the survivable IP Office are administered through the User Management feature in System Manager.

  As an alternative, if the address of the IP Office survivable server is not administered for the user from System Manager, this setting should be configured to contain a priority ordered list of SIP servers that the phone should use. Each entry should contain the server IP address, port and transport method (TLS or TCP). The multiple entries should be separated by a comma.

  - The list should contain the primary Session Manager as the first entry then the IP Office. If there is an additional Session Manager being used for redundancy it should be included

before the IP Office entry. Note that using this alternative means that the settings file will have to be different for each branch. Using different settings files for each branch is possible when the IP Office is used as the file server for the Centralized SIP phones. It is not practical, however, if using a central file server with a common settings file for the phones in different branches.

- The string below would set the phone's primary SIP controller to the Session Manager and the secondary controller to an IP Office used in the basic configuration example: `SET SIP_CONTROLLER_LIST 10.80.100.23:5061;transport=tls, 35.1.1.51:5060;transport=tcp`

⚠️ **Warning:**

If the port and transport are not specified for a controller, the default values of 5061 and TLS are used.

• **SIPDOMAIN**

This setting identifies the enterprise SIP domain. This must match a domain set in the Avaya Aura® domains settings.

• **TRUSTCERTS**

This setting identifies the list of trusted certificates. These certificates allow communication over TLS and must exist on the file server. (If the IP Office is used as the file server for the Centralized SIP phones, these certificates must exist on the System SD card.) This parameter may contain one or more certificate filenames, separated by commas without any intervening spaces. Files may contain only PEM-formatted certificates. Example: `SET TRUSTCERTS SmgrCARoot.txt,SIPProductCertificateAuthority.txt`

✳️ **Note:**

If the phones register using the TLS protocol, in order to register to IP Office in the Rainy day mode, the System Manager CA root certificate must be included in the TRUSTCERTS list and installed on the file server. This is required because the phones must trust the System Manager CA root certificate so they can verify the IP Office Identity Certificate that is signed by the System Manager CA. To download this certificate, see Downloading the System Manager CA root certificate on page 28.

If the TRUSTCERTS parameter is included in the phone settings file and includes the SIP Product CA root certificate, in the TRUSTCERTS list, then you should obtain the certificate from System Manager and install it on the file server that is used by the phones. See Using the SIP Product CA root certificate on page 38.

• **TLSSRVRID** — This setting is used for TLS servers identification. If it is set to 1 then TLS/SSL connection will only be established if the server's identity matches the server's certificate. If it is set to 0 then connection will be established anyway. Recommended setting: `SET TLSSRVRID 0`

✳️ **Note:**

A setting of **0** does not disable verification of the certificate chain. It only disables verification of the identity in the server certificate.

- **MEDIAENCRYPTION** — This setting specifies media encryption (SRTP) options supported by the phone. Up to 2 options may be selected. Values are in comma-separated list. Options should match those specified in CM IP-codec-set form. Settings are:

  - 1 = aescm128-hmac80

  - 2 = aescm128-hmac32

  - 3 = aescm128-hmac80-unauth

  - 4 = aescm128-hmac32-unauth

  - 5 = aescm128-hmac80-unenc

  - 6 = aescm128-hmac32-unenc

  - 7 = aescm128-hmac80-unenc-unauth

  - 8 = aescm128-hmac32-unenc-unauth

  - 9 = none (default)

  Recommended setting: `SET MEDIAENCRYPTION 1,9`

- **CALLFWDSTAT**

  This parameter should be set only if local call forward is going to be configured for the phone in Rainy day. See [9600 Series SIP phone features available during survival mode](#) on page 42 for more information. The default setting is 0. The call forwarding mode is set by summing the following values:

  - 1 = permits unconditional call forward

  - 2 = permits call forward on busy

  - 4 = permits call forward on no answer

  Example of summing the values: a value of 6 allows call forwarding on busy and on no answer.

- **CALLFWDADDR**

  This parameter sets the address to which calls are forwarded when the CALLFWDSTAT parameter is not set to **0**. This parameter and the CALLFWDSTAT parameter should be set only if local call forward is going to be configured for the phone in Rainy day. See [9600 Series SIP phone features available during survival mode](#) on page 42 for more information.

- **CALLFWDDELAY**

  This setting sets the number of ring cycles before the call is forwarded to the forward or coverage address. It is required for local call forwarding on the phone in Rainy day when CALLFWDSTAT is configured. The default delay is one ring cycle.

Additional parameters that are relevant to enterprise branch deployments

- **DIALPLAN**

  During survivable mode, when registered to the IP Office system, the phone is not able to obtain dial plan information from the Session Manager as it would normally expect. This DIALPLAN string can be used to set what numbers are dialed immediately when matched without waiting for any dialing timeout. Multiple entries can be used, separated by the **|** character. For example, on a typical IP Office system, the following might be used: `SET DIALPLAN [2]xx|[8]xxxxx|[6]xxxxxx|9Z1xxxxxxxxx`

The first entry matches local extension numbers. The next two entries match numbers for other branches. The final entry matches US national number dialing.

- **DISCOVER_AVAYA_ENVIRONMENT**

  This setting is used by the phone to set whether it should request if the controller to which it has registered supports AST (Advanced SIP Telephony). IP Office systems do not support AST. However, since survivable phones connect in normal mode to Session Manager, the default setting DISCOVER_AVAYA_ENVIRONMENT 1 must be used.

- **ENABLE_REMOVE_PSTN_ACCESS_PREFIX**

  This setting enables the removal of the PSTN access prefix from collected dial strings when the phone is registered with a non-AST controller such as IP Office. Enabling this parameter (1) when the phone is communicating with an AST-capable controller has no effect. The default is 0 (do not remove prefix).

- **MSGNUM**

  This sets the number dialed when the **Message** button is pressed and the phone is in normal centralized mode. For example, the extension number for the Modular Messaging system.

- **PSTN_VM_NUM**

  This sets the number dialed when the **Message** button is pressed and the phone is in survivable mode. For example, a DID number for the Modular Messaging system.

- **RECOVERYREGISTERWAIT**

  This is the monitoring interval used by the phone when no available controller was detected by a previous monitoring check. The phone waits for a response from each controller in the SIP_CONTROLLER_LIST with the CONTROLLER_SEARCH_INTERVAL setting. The actual interval used is between 50% to 90% of the setting. Range 10 to 36000 seconds. Default 60 seconds.

- **ENABLE_PPM_SOURCED_SIPPROXYSRVR**

  This setting enables PPM as a source of SIP Proxy server information. Keep the default value for this setting. The default value is **1**. The default value of **1** enables the phone to acquire and use the information about the survivable IP Office that is configured from System Manager. This information is delivered to the phone via PPM. Recommended setting: `SET ENABLE_PPM_SOURCED_SIPPROXYSRVR 1`

Settings files and firmware for Centralized 9600 series SIP phones

Adding a NoUser Source Number to enable SIP firmware download

About this task

If the IP Office is used as the file server for the Centralized 9600 series SIP phones, then you must configure the NoUser Source Number parameter, ENABLE_SIP_FIRMWARE_DOWNLOAD, on the IP Office. This task is a system configuration task performed in the IP Office system configuration.

Procedure

1. From the System Manager console, under **Elements**, select IP Office.

2. In the left navigation pane, click **System Configuration**.

3. To edit the system configuration of an IP Office device, on the IP Office System Configuration page, select an IP Office device.

4. Click **Edit**.

   The IP Office Manager application is launched.

5. In the left navigation pane, click **User**.

6. In the middle User pane, click **NoUser**.

7. Click the **Source Numbers** tab and click **Add**.

8. In the **Source Number** field, enter ENABLE_SIP_FIRMWARE_DOWNLOAD.

9. Click **OK**.

10. To save the updates and return to System Manager, from the **File** menu, click **Save Configuration and Exit**.

File and certificates

The upgrade and settings files are provided in the following SIP software distribution packages:

- *Avaya one-X® Deskphone SIP 6.2.2 Software for the 9601/9608/9611G/9621G/9641G IP Deskphones*
- *Avaya one-X® Deskphone SIP 2.6.10 Software for 9600 IP Deskphones* (used for the 9620, 9630, 9640, and 9650 phones)

The SIP software distribution packages are available on the Avaya Support website at http://support.avaya.com/ and are used to upgrade the Centralized SIP phones from one release to the next. They are also used to convert the 9600 series phones from H.323 to SIP. See "About converting 9600 series phones from H.323 to SIP" below for more information.

Upgrade files

The various combination of 9600 series phones (96x1, 96x0, SIP, and H.323) may require different upgrade files to be placed on the IP Office System SD card. These files specify the firmware versions and settings files to load. Some of these files are auto-generated by IP Office and some are customized files. The upgrade files are:

- **96x1Supgrade.txt** – the 96x1 SIP phones require this file. It is included in the SIP software distribution package. In Mixed enterprise branch deployments where both Centralized SIP phones and H.323 IP Office phones are used, this upgrade file is edited. For more information, see "Settings Files" below.

- **96x1Hupgrade.txt** – the 96x1 H.323 phones require this file. This file is auto-generated by the IP Office and should not be changed.

- **96xxupgradeSIP.txt** – the 96x0 SIP phones require this file. This file is requested as a result of the phone requesting the 96xxupgrade.txt file from the IP Office. You create this file by renaming the 96xxupgrade.txt file that came in the SIP software distribution package. In Mixed enterprise branch deployments where both Centralized SIP phones and H.323 IP Office phones are used, this upgrade file is edited. For more information, see "Settings Files" below.

> **✳ Note:**
>
> If the IP Office is not being used as the file server, the 96xxupgradeSIP.txt file is not required. The 96xxupgrade.txt file that came with the 96x0 SIP firmware package should be placed on the file server as is.

- **96xxupgrade.txt** – the 96x0 H.323 phones require this file. This file is auto-generated by the IP Office and should not be changed.

9600 series phones which are intended to be Centralized SIP phones must have their SIG parameter set to SIP (2). The upgrade script looks at this setting to determine if SIP or H.323 firmware is required. For more information about the SIG parameter, see "9600 series phone changes for migration" in Chapter 3 in *Migrating an IP Office or B5800 Branch Gateway to an IP Office Enterprise Branch*, document number 15-604268.

Settings files

The 9600 series phones require a settings file. Historically, the 9600 Series phones have used the 46xxsettings.txt file. In Mixed enterprise branch deployments where there are both H.323 and SIP phones, a separate settings file is required for the phones since it is likely that SIP phones will need different settings than H.323 phones. The 46xxsettings.txt file is used for the H.323 phones and a new settings file, for example 96xxSIPsettings.txt, can be used for the SIP phones. This is implemented by editing the upgrade files. Each of the upgrade files listed above specifies a certain settings file. For example:

- **96xxSIPsettings.txt** – the 96x1Supgrade.txt and 96xxupgradeSIP.txt upgrade files specify the 96xxSIPsettings.txt file. This settings file contains the settings required by the Centralized SIP phones. The 96xxSIPsettings.txt file is not auto-generated. It is created by renaming the 46xxsettings.txt file to 96xxSIPsettings.txt, editing it for the Centralized SIP phones, and then manually loading it on the System SD card.

> **❗ Important:**
>
> There are 2 different versions of the 46xxsettings.txt file. One version is auto-generated by the IP Office system and supports only H.323 phones. The other version is available on the Avaya Support website. The version that is renamed 96xxSIPsettings.txt and edited for the SIP phones is the version on the Avaya Support website.

- **46xxsettings.txt** – the 96x1Hupgrade.txt and 96xxupgrade.txt upgrade files specify the 46xxsettings.txt file. This settings file contains the settings required by the H.323 phones. The 46xxsettings.txt settings file is auto-generated. It does *not* need to be configured or loaded on the System SD card.

For parameters that must be configured in the settings file for Centralized enterprise branch deployments, see Centralized phone settings on page 40.

Certificates

The following certificates must be downloaded from System Manager to the file server. They must also be included in the list of files installed on the file server.

- **System Manager CA root certificate** — If the phones register using the TLS protocol, in order to register to IP Office in Rainy day, the System Manager CA root certificate must be included in the list of files installed on the file server. This is required because the phones must trust the System Manager CA root certificate so they can verify the IP Office Certificate that is signed by the System Manager CA. The System Manager CA root certificate must also be downloaded to the file server.

- **SIP Product CA root certificate** — If the TRUSTCERTS parameter is included in the phone settings file, the SIP Product CA root certificate must be included in the list of files installed on the file server. The SIP Product CA root certificate must also be downloaded to the file server.

About converting 9600 series phones from H.323 to SIP

For information about converting the 9600 series phones from H.323 to SIP, including the procedures to edit the upgrade and settings files which are required to convert the phones, see "9600 series phone changes for migration" in Chapter 3 in *Migrating an IP Office or B5800 Branch Gateway to an IP Office Enterprise Branch*, document number 15-604268. The topics provided there include:

- Converting all 96x1 phones from H.323 to SIP

- Converting some 96x1 phones from H.323 to SIP

- Converting some or all 96x0 phones from H.323 to SIP

Using the SIP Product CA root certificate

About this task

Session Manager and other Avaya Aura® components, such as CE used demo certificates issued by the SIP Product CA. The demo certificate provides out of the box TLS communication with other Avaya products, such as Communication Manager and endpoints. From Session ManagerR6.3.8, the demo certificates are not installed by default. For new Session Manager installations, System Manager signs the SIP and HTTP certificates. The existing TLS connections to Centralized phones break if the System Manager CA is not installed on the phones. IP Office uses System Manager CA and gets its identity certificate using SCEP. You can install the demo certificates to restore a previously working environment. To install demo certificates, use `initTM`.

Use the following task to obtain the existing identity certificate from System Manager and to install it on the file server, which is used by phones:

Procedure

1. Type `https://<Session Manager IP Address>:5061` in your Firefox browser and press **Enter**.

2. From **Services** > **Inventory** > **Manage Elements**, select the Session Manager element.

3. Click **More Actions**.

4. Select **Configure Trusted Certificates**.

5. To export the **SECURITY_MODULE_SIP certificate**, where:CN=SIP Product Certificate Authority, OU=SIP Product Certificate Authority, O=Avaya Inc., and C=US, click **Export**.

About rebooting the phones

The phones must be rebooted to start the firmware download from the IP Office system. You can reboot the phones remotely from the Avaya Aura® System Manager in the NOC or by power cycling the phones.

Rebooting the phones from Avaya Aura® System Manager

About this task

You can upgrade up to 50 phones in each branch at once. Once these phones finish, another set of up to 50 phones can be rebooted to start the upgrade. If more than 50 phones try to download their firmware from IP Office at once, there is a risk that the download will not be successful on some of phones. If this occurs, the phones that failed to download successfully must be rebooted to try again.

❋ **Note:**

This procedure must be performed in sunny day conditions when the phones are registered to Session Manager.

Procedure

1. On the System Manager console, under **Elements**, click **Session Manager**.

2. Select **System Status > User Registrations**.

3. Use the **Advanced Search Criteria** option to find the phones to be upgraded.

   Using the **Location** search criteria and specifying the branch location may provide a convenient way to display all phones in a given branch, assuming **Location** is administered in System Manager for all users. Alternatively, other criteria can be used, including choosing the **Address** search criteria and specifying the leading digits that are common to and unique to the users in that branch, or choosing the **IP Address** search criteria and specifying the subnet IP address of the branch

4. In the list of users that is displayed, select the check box (on the left of each row) for the users to be rebooted.

   ❋ **Note:**

   Multiple users can be selected by checking the boxes of multiple entries on the list. For best results of the firmware download process, check multiple (up to 10) users from the list to reboot them together in one action.

5. Click the **Reboot** button that is located next to **AST Devices Notification** above the list of users.

   System Manager will notify Session Manager that will instruct each of the selected phones to reboot. After the reboot, the phone will get in DHCP the address of the local IP Office system in its branch as HTTP server, and will get its configuration files (upgrade and settings files) and then download its firmware file from the IP Office system. After the download completes successfully, the phone will automatically restart using the new firmware.

6. Confirm that the firmware upgraded correctly by choosing one of the following methods:

   • From the phone craft menu, do the following:

      a. Press the **Mute** button.

      b. Enter the password, `CRAFT#` (`27238#`)

      c. Scroll to the **View** option.

       • From the phone user menu, do the following:

         a. Select **Home** > **Network Information** > **IP Parameters**.

         b. Scroll right 4 pages.

    7. If the firmware download was not successful on a given phone, reboot the phone again.

Rebooting the phones by power cycling the phones

About this task

This procedure can be performed in Sunny day or Rainy day conditions. The phones do not need to be registered to Avaya Aura® Session Manager.

Procedure

To power cycle the phone, remove power to the phone, wait about one minute, then reapply power.

SIP controller monitoring by Centralized 9600 series SIP phones

Each Centralized phone performs monitoring to determine which SIP controllers are available and, from the results, which controller to use as its active controller. Centralized 96x1 SIP phones do this as follows:

- Using the list of SIP controllers, the phone sends a SIP REGISTER (Adding bindings) message to each controller. The controller list is set by the SIP_CONTROLLER_LIST which lists controllers in priority order from highest priority first.

- The phone waits for a response from each controller within a set time. That time is set by the CONTROLLER_SEARCH_INTERVAL setting (default 4 seconds).

- The controller is considered available if a 200 OK response is received from it within the timer interval. Once a controller has been marked as available, the phone unregisters from it. IP Office only responds to this request if its SM Lines are out of service.

  - If the phone does not have a current controller, it will register with the highest ranked available controller.

  - If a higher ranked controller than the phone's current active controller is available, it will switch its active controller to the higher ranked available controller. This only applies if the FAILBACK_POLICY is set to **auto**.

  - While operating with its selected controller, the phone will continue monitoring the available controllers. It does this at regular intervals set by the REGISTERWAIT setting (default 300 seconds).

  - If no response is received from any controller, the phone retries monitoring. It does this at random intervals between 50 to 90% of the RECOVERYREGISTERWAIT setting (default 60 seconds).

- A Centralized phone can register with both the primary and secondary Session Managers, which are listed as the first two entries on the phone's list of SIP controllers. This is specified by setting the SIMULTANEOUS_REGISTRATIONS parameter to 2. Only the highest ranking controller is set as its active controller. If both Session Manager's are not available, the phone

will register with the IP Office, which is the third entry on the SIP controllers list. Note that the legacy setting SIPREGPROXYPOLICY in the phone settings file has no effect. It is always overridden by Session Manager PPM and set to the value simultaneous.

• A Centralized phone can register with both the primary and secondary Session Managers, which are listed as the first two entries on the phone's list of SIP controllers. This is specified by setting the SIMULTANEOUS_REGISTRATIONS parameter to 2. Only the highest ranking controller is set as its active controller. If both Session Manager's are not available, the phone will register with the IP Office, which is the third entry on the SIP controllers list. Note that the legacy setting SIPREGPROXYPOLICY in the phone settings file has no effect. It is always overridden by Session Manager PPM and set to the value simultaneous.

• A Centralized phone will not failover to another SIP controller while it has a connected call in progress. However, it will not be able to make or receive any additional calls while in this state. Once the existing call is completed, the phone will failover to the other SIP controller.

• In addition to the regular monitor checks, the phone will perform a monitoring check when any of the following events occur:

- It does not receive a response to an INVITE it send to its active controller within a set time. The time is set by the FAST_RESPONSE_TIMEOUT settings (default 4 seconds).

- It receives a TCP keep-alive failure or other socket error.

- If prompted by an administrator.

- If it receives an INVITE from a controller other than its active controller.

9600 Series SIP phone features available during failover

The following apply while a phone is in the process of failover to another SIP controller. Typically the failover process will be completed within 2 minutes.

• The phone will display the survivability ⚠ warning icon. In addition:

- If the extension is idle, it displays the message **Link recovery. Limited phone service. Calls may be lost**.

- If the user has a call in progress which continues, the survivability ⚠ warning icon is displayed along with the message `Limited phone service`. The only call control available is End Call. The phone will not failover until the call is ended.

- If the message `Acquiring Service...` is displayed it indicates that the phone could not detect any available SIP controller. It will not failover until an available controller is detected.

• During the failover:

- No new calls can be made or received.

- Held calls are lost during failover.

- Transfers are lost during failover.

9600 Series SIP phone features available in Rainy day mode

The following features are available on 9600 Series Centralized SIP phones when registered to IP Office in the Rainy day mode.

- Make or receive calls to or from other endpoints in the branch and to or from any type of local PSTN trunk

- Caller ID

- Multiple call appearances but not bridged appearances

- Call hold and consultative hold

- Music on hold

- Attended call transfer

- Unattended call transfer

- Three-party ad-hoc conferencing done locally on the phone, as well as capability to dial into Meet-Me conferencing on the IP Office up to 64-party conference

- Centralized voice mail coverage and access over PSTN, but no Message Waiting Indication (MWI)

- Automated Attendant

- Survivability mode indication on the phone screen

- Local telephone features: redial, mute, audio selection (speaker / headset / handset), Call Logs, Volume Control, local contacts, speed-dials, auto dials

- Station Message Detail Recording (SMDR) records stored on the IP Office for retrieval after WAN recovery

- Hunt groups

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

- Call Management

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

- Send call to mobile phone

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

- Call forwarding

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

- Authorization codes

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

❋ Note:

The 9600 Series SIP phones cannot dial the **#** symbol in the Rainy day mode. In the Rainy day mode, all features that require the **#** symbol to be dialed must be redefined.

1100 and 1200 series SIP phones deployed as Centralized users in IP Office Branch deployments

IP Office Branch supports the deployment of 1100 and 1200 Series SIP phones as Centralized users. Deployment of these phones as Centralized users is different than the deployment of the phones as IP Office users.

The phone features vary for the Rainy day and the Sunny day modes as follows:

- When operating as Centralized users in Sunny day mode, the features available on the 1100 and 1200 Series SIP phones are basic features and Avaya Aura® Communication Manager features invoked through Feature Access Codes (FACs) or Feature Name Extensions (FNEs), if configured. For a description of how the 1100 and 1200 Series SIP phones operate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager, see *1100 and 1200 SIP Deskphones on Avaya Aura®*.

- When operating as Centralized users in Rainy day mode, the features available on the 1100 and 1200 Series SIP phones are limited survivability features.

    For more information see, *Avaya IP Office™ Platform in a Branch Environment Reference Configuration*, document number- 15–604253.

1100 and 1200 series phone limitations:

The following are the limitations for the 1100 and 1200 series SIP phones in a Centralized IP Office branch environment:

- Ensure that the 1100 and 1200 series phones within a branch are all Centralized or all IP Office users, otherwise you must configure each phone manually.

- In the Rainy day mode, direct media with SRTP is not supported. In this scenario, media is anchored on IP Office.

- The address book feature of the phone varies for different servers. Hence, the contacts added to the phones while the phones are connected to Session Manager are unavailable when the phones are connected to IP Office, and vice versa.

- Install the security certificate manually. You must accept the authorization prompts from the phones to go ahead and install the certificate. If you do not provide any input, then the certificate does not get installed.

- 1100 and 1200 series phones support only two servers. You can deploy this phone as Centralized users in branches that connect to a single Session Manager and configure it with the local branch IP Office as the secondary server. However, you cannot deploy this phone as Centralized users in a branch that is configured to two Session Manager. If there are Centralized 1100 series or 1200 series phones in the branch, then you must not configure the IP Office and other Centralized phones in that branch to two Session Manager. If you configure the IP Office with two Session Manager, then the Centralized 1100 series and 1200 series phones will receive no service. This occurs if the primary Session Manager is down and the secondary Session Manager is still reachable from the IP Office. The Centralized 1100 series and 1200 series phones will not be able to register to the IP Office that will still be in Sunny day mode.

For more information on the 1100 and 1200 series SIP phones, see the following documents:

- *SIP Software for Avaya 1100 Series IP Deskphones–Administration*, document number NN43170– 17 600

- *SIP Software for Avaya 1200 Series IP Deskphones–Administration*, document number NN43170– 19 601

Factory settings:

If you want to return all the phone settings to the default settings, see "Factory Reset" in *IP Office Release 7.0 1100/1200 Series Phone Installation*.

Configuring the 1100 and 1200 Series SIP phones in the Centralized branch model

Before you begin

- You must have configured IP Office as part of a branch solution.

  For information on IP Office adding IP Office as a branch node, see *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

- Ensure that IP Office is available as a file server.

> 😊 **Note:**
>
> You can also use other file servers. When you are using a different file server, you must create the phone `.cfg` files and put the files on the file server. You can get the files from the firmware packages on the Avaya support site at support.avaya.com.

About this task

Use this procedure when you are configuring the 1100 and 1200 Series SIP phones as Avaya Aura® Session Manager phones.

Procedure

1. In Avaya Aura® System Manager, create the Centralized user profiles including the IP Office endpoint profile.

   System Manager provides user information to IP Office.

2. Prepare the `11xxsettings.txt` file and put the file on the file server.

   This action overrides the auto-generated file.

3. Prepare the `Profile` files for Session Manager and IP Office and put the files on the file server.

   The names of the files are `profile1.txt` and `profile2.txt`.

4. **(Optional)** Create the `FNESpeeddiallist.txt` file containing the FAC or FNE invocation strings and put the file on the file server.

   > 😊 **Note:**
   >
   > You must create these files to create the FNE or FAC, or IP Office short codes to store in the files.

5. **(Optional)** Create the `IPO_Speeddiallist.txt` file containing IP Office short codes for the phone features and put the file on the file server.

   > 😊 **Note:**
   >
   > You must create these files to create the FNE or FAC, or IP Office short codes to store in the files.

6. Configure the phone sets with the file server address using one of the following options:

   - If a different DHCP server is used for the phones, then configure DHCP server to send option 66 with the HTTP server address.
   - Enter the file server address into the phone manually

   > 😊 **Note:**
   >
   > If IP Office is used as the DHCP server for the phones, then you are not required to configure the phones because the **HTTP Server IP Address** field on the **System** tab is already set.

7. Install the System Manager CA root certificate on the phone sets using any of the following options:

   - Through SCEP protocol exchange between IP Office and System Manager, which is typically done in branch deployments. SCEP is enabled by the ICU.

     You can also the enable SCEP in the IP Office security settings.

     This action installs the certificate as the default option on IP Office. The auto-generated phone.`cfg` files, such as `1140eSIP.cfg`, on IP Office already contain the name of this certificate, so you do not have to add the file name manually. The certificate is provided by the IP Office core and you do not have to put the certificate on the IP Office SD card.

     ✱ Note:

       If IP Office is using a modified phone .`cfg` file, then add the **USER_KEYS** entry mentioned in the second option.

   - Get the certificate from System Manager manually and put the file on the file server. Reference the file in **USER_KEYS** in the phone .`cfg`.

   - For more information about modifying the Avaya Aura® Session Manager, see [Modifying the Avaya Aura Session Manager identity certificates](#) on page 56.

     ✱ Note:

       You cannot perform this task remotely because installing the certificate requires manual acceptance on the phone.

8. **(Optional)** Create IP Office short codes that align with the Avaya Aura® Communication Manager FAC or FNE codes to emulate the Communication Manager features.

   The Communication Manager FAC or FNE codes are put into the `FNE_Speeddiallist.txt` file, and the IP Office short codes are put into the `IPO_Speeddiallist.txt` file.

Related Links

[Sample configuration files for the 1100 and 1200 Series SIP phones](#) on page 47

Installing the 1100 Series SIP phone configuration files with the TFTP server

You can use any file server other than the IP Office file server for installing the 1100 and 1200 Series SIP phone configuration files. This topic is an example of using a third party TFTP server.

About this task

Use this procedure to install the 1100 series SIP phone configuration files while using the TFTP server.

✱ Note:

You can also use any other server besides the TFTP server. The procedure for configuring 1100 and 1200 phones with another file server might be different from this procedure if you are not using the IP Office file server.

Procedure

1. Get the configuration files.

2. Edit the `xxxxSIP.cfg` file, where *xxxx* is the name of the phone to force download the file settings.

3. Get the new firmware from the downloaded configuration files.

4. Run the TFTP application to start a TFTP server on a computer.

5. Set the TFTP default directory to the location that contains the following configuration files:

   - `11xxsettings.txt`
   - `11xxdialplan.txt`
   - `xxxxSIP.cfg`
   - `profile1.txt`
   - `profile2.txt`
   - `SIPxxxx04.04.xx.xx.bin`

6. On the 1100 Series SIP phone, configure the provisioning server URL to the IP address of the TFTP server.

   ✱ Note:

   If the DHCP server does not specify the HTTP server, then enter the HTTP server on the phone manually. This manual procedure applies to any file server used for configuring the 1100 Series SIP phones.

7. Apply the configuration and reboot the phone.

   When the 1100 SIP phone reboots, you get the new firmware.

8. Apply the configuration on the phone.

Sample configuration files for the 1100 and 1200 Series SIP phones

This section shows a sample configuration for the 1100 and 1200 series SIP phones.

❗ Important:

With the exception of the `.cfg` file and the firmware file, the other files can work with other phone types in this series, such as the 11xx/12xx.

These phones register to Avaya Aura® Session Manager in Sunny day mode, and failover to IP Office in a WAN outage between the branch and the core where Session Manager resides.

In this configuration, IP Office was configured as the DHCP server. IP Office provides the IP address for the IP Office configuration and the HTTP provisioning server IP address to the phones.

When the phones are configured with a provisioning server, the phones attempt to download a configuration file after the reboot. The configuration file depends on the model of the phone. For example, if you are using a 1140e telephone, this file is `1140eSIP.cfg` and if you are using a 1230 SIP telephone, the file is `1230SIP.cfg`. These configuration files then instruct the phones to download several different files, such as a dial plan file, certificates, and security polices that contain additional configuration information.

For the sample configuration, a file called `11xxsettings.txt` was created with additional settings for the SIP telephones. For survivability, the phones use profile files. The profile files are additional files that instruct the phone to use different parameters depending on whether:

- The phones are registered to the Session Manager signaling server
- The phones have failed over to IP Office.

For the sample configuration, these files are called `profile1.txt` and `profile2.txt.`

The sample configuration, settings, and profile files in the following table are for the 1140e SIP phone. For other phone models, the content of the files is the same except for the name and version of the firmware file. When these files are created, they must be uploaded to the HTTP provisioning server used by the SIP phones. In this sample configuration, IP Office is configured as the provisioning server.

Examples of file server content

Sample 1140eSIP.cfg configuration file

If you are using IP Office as the file server, then you do not have to do anything about this file. IP Office auto-generates the file and provides the file to the phone. However, if you are using a different file server other than IP Office, then ensure that the files are installed on the file server.

Text in the configuration file	Information specific to Session Manager and IP Office deployments
`[DEVICE_CONFIG]`	Instructs the phone to get the settings file through HTTP.
`DOWNLOAD_MODE    FORCED`	Instructs the phone to download and install the file for every reboot.
`VERSION    000001`	Use only if DOWNLOAD_MODE is set to AUTO.
`PROTOCOL    HTTP`	Instructs the phone to use HTTP to download from the provisioning server.
`FILENAME    11xxsettings.txt`	Displays the name of the settings file.
`[FW]`	Instructs the phone to install on the appropriate FW file if necessary.
`DOWNLOAD_MODE    AUTO`	
`VERSION    SIP1140e04.04.10.00`	
`PROTOCOL    HTTP`	
`FILENAME  SIP1140e04.04.10.00.bin`	
`[DIALING_PLAN]`	Defines the length and digits to dial without the caller needing to press the pound sign (#) to instruct the phone to start the call.
`DOWNLOAD_MODE    AUTO`	

Text in the configuration file	Information specific to Session Manager and IP Office deployments
VERSION 000001 PROTOCOL HTTP FILENAME 11xxdialplan.txt [LANGUAGE] DOWNLOAD_MODE AUTO DELETE_FILES YES VERSION 000001 PROTOCOL HTTP FILENAME Spanish.lng FILENAME French.lng FILENAME Portuguese.lng FILENAME Italian.lng FILENAME German.lng	
[USER_KEYS] DOWNLOAD_MODE AUTO VERSION 000002 PROTOCOL HTTP FILENAME default_ca.pem	PEM file certificates that the phone can use for TLS.

Sample 11xxsettings.txt configuration file

As shown in the `1140eSIP.cfg` file above, the phone is instructed to download a file called `11xxsettings.txt` as follows:

Text in the configuration file	Information specific to Session Manager and IP Office deployments
SIP_DOMAIN1 smec-st-sip.ca.avaya.com	This line displays the SIP Domain in use on Avaya Aura® Session Manager or IP Office
SERVER_IP1_1 10.136.100.61	This line displays the IP address of the Session Manager.
SERVER_IP1_2 135.55.86.86	This line displays the IP address of the IP Office.
PRIMARY_SERVER_PROFILE profile1.txt	This line specifies the name of the profile file to use in the Sunny day mode.
SECONDARY_SERVER_PROFILE profile2.txt	
SERVER_PORT1_1 5060	This line sets the SIP port for UDP used to register to the Session Manager.
SERVER_PORT1_2 5060	This line sets the SIP port for UDP used to register to the IP Office.
SERVER_TCP_PORT1_1 5060	This line sets the SIP port for TCP used to register to the Session Manager.
SERVER_TCP_PORT1_2 5060	This line sets the SIP port for TCP used to register to the IP Office.

Text in the configuration file	Information specific to Session Manager and IP Office deployments
`SERVER_TLS_PORT1_1 5061`	This line sets the SIP port for TLS used to register to the Session Manager.
`SERVER_TLS_PORT1_2 5061`	This line sets the SIP port for TLS used to register to the IP Office.

`SIP_UDP_PORT 5060`
 	
`SIP_TCP_PORT 5060`
 	
`SIP_TLS_PORT 5061`
	Settings that are common to Sunny day mode and IP Office in Rainy day mode

`AVAYA_AURA_MODE_ENABLE    YES`	
`IP_OFFICE_ENABLE          NO`	
`DEF_LANG            English`	
`FORCE_BANNER             YES`	Displays on the phone to indicate which server the phone is registered to
`LOGOUT_WITHOUT_PASSWORD   YES`	
`TIMEZONE_OFFSET       -18000`	
`FORCE_TIME_ZONE          YES`	
`DST_ENABLED              NO`	
`REDIRECT_TYPE       rfc3261`	
`EXP_MODULE_ENABLE        YES`	
`ENABLE_PRACK             YES`	
`CONN_KEEP_ALIVE          30`	
SRTP settings are common, but if necessary, move to individual profile files and edit.	

`SRTP_ENABLED            YES`
 	
`SRTP_MODE           BE-Cap Neg`
 	
`SRTP_CIPHER_1`
`AES_CM_128_HMAC_SHA1_80`
 	
`SRTP_CIPHER_2`
`AES_CM_128_HMAC_SHA1_32`	

List the enabled codecs are common but if necessary move to individual profile files and edit	

`AUDIO_CODEC1        G729`
 	
`AUDIO_CODEC2        PCMU`	

Sample profile1.txt profile file

As shown in the `11xxsettings.txt` file above, the phones are instructed to download files called `profile1.txt` and `profile2.txt`. The parameters of these files are as follows:

Text in the configuration file	Information specific to Session Manager and IP Office deployments
`USE_DEFAULT_DEV_CERT    YES`	
`ENABLE_SERVICE_PACKAGE  PPM`	
`ADDR_BOOK_MODE          LOCAL`	
`DISABLE_PRIVACY_UI      YES`	
`MKI_ENABLE              NO`	

Text in the configuration file	Information specific to Session Manager and IP Office deployments
`BANNER                  Aura SM`	
`VMAIL....<TBD>`	The voicemail access code depends on the Session Manager configuration.
`SPEEDLIST_KEY_INDEX  4`	Create speed dial button for the features.
`SPEEDLIST_LABEL      Features`	
`DEFAULT_SPEEDDIALLIST_FILE FNE_Speeddiallist.txt`	

Sample profile2.txt profile file

The parameters in the `profile2.txt` file are required when the phone registers to the IP Office. The parameters of this file are as follows:

Text in the configuration file	Information specific to Session Manager and IP Office deployments
`FAIL_BACK_TO_PRIMARY   YES`	
`DISABLE_PRIVACY_UI     NO`	
`BANNER    IP Office`	The voicemail access code depends on the IP Office configuration.
`VMAIL    *17`	Voicemail access code is typically *17.
`SPEEDLIST_KEY_INDEX  4`	Create speed dial button for the features
`SPEEDLIST_LABEL      Features`	
`DEFAULT_SPEEDDIALLIST_FILE IPO_Speeddiallist.txt`	

Sample FNESpeeddiallist.txt configuration file

The content of the `FNESpeeddiallist.txt` configuration file is as follows:

```
[key]
label=Call Pickup
target=*130@smec-st-sip.ca.avaya.com
```

⊛ **Note:**

The administrator can populate this file with the FAC or FNE codes for Avaya Aura® Communication Manager

Sample IPO_Speeddiallist.txt configuration file

The content of the `IPO_Speeddiallist.txt` configuration file is as follows:

```
[key]
label=Call Pickup
target=*30@smec-st-sip.ca.avaya.com
```

⊛ **Note:**

The administrator can populate this file with short codes for IP Office.

Ensuring consistent settings between the phones and IP Office for media security

About this task

Use the following procedure to ensure that the 1100 and 1200 series SIP phones deployed as Centralized users are configured consistently with the IP Office configuration for media security.

> **Note:**
>
> Use the following procedure only if you are using media security.

Procedure

1. Ensure that the **Allow Direct Media Path** and the **Re-invite Supported** check boxes are clear in the **VoIP** tab of the **Extension** records of the 1100 and the 1200 series SIP phone Centralized users.

   In Avaya Aura® System Manager, you must configure this setting in the user template that is used for adding these users.

   You can also view, or set this setting from the Endpoint Editor in the IP Office profile of the individual Centralized users in System Manager User Management.

2. Open the IP Office system configuration and click the **System** > **Telephony** > **VOIP Security** tab.

3. Ensure that the security settings applied to the telephone sets through the `11xxsettings.txt` file match the security settings specified on the **VOIP Security** tab as follows:

   - If the `11xxsettings.txt` file specifies **SRTP_ENABLED NO**, then ensure that **Media Security** is set to either **Disable** or **Best Effort**.

     > **Note:**
     >
     > **Best Effort** might be necessary to support security on the SM line.

   - If the `11xxsettings.txt` file specifies **SRTP_ENABLED YES** with **SRTP_MODE BE-Cap Neg**, then ensure that **Media Security** is set to **Best Effort**.

   - If the `11xxsettings.txt` file specifies **SRTP_ENABLED YES** with **SRTP_MODE SecureOnly**, then ensure that **Media Security** is set to **Enforce**.

4. If **Media Security** is set to **Best Effort** or **Enforce**, ensure that the **Media Security Options** section is set as follows:

   - **Encryptions**: The **RTP** check box is selected and the **RTCP** check box is clear.

   - **Authentication**: The **RTP** and the **RTCP** check boxes are selected.

   - **Replay Protection SRTP Window Size**: The value is set to 64.

   - **Crypto Suites**: The **SRTP_AES_CM_128_SHA1_80** and the **SRTP_AES_CM_128_SHA1_32** check boxes are selected.

E.129 series SIP phones deployed as Centralized users in IP Office Branch deployments

IP Office Branch supports the deployment of E.129 series phones as Centralized users. You can migrate existing E.129 series phones on Avaya Aura® to the branch environment, or deploy new E. 129 series phones as Centralized users in the branch environment.

E.129 phones are supported in both Sunny Day and Rainy Day. When operating as Centralized users in Rainy day mode, the features available on the phones are limited survivability features. For more information about supported Rainy Day features, see *Avaya IP Office™ Platform in a Branch Environment Reference Configuration*, document number- 15–604253.

Caveats and limitations

The following caveats and limitations exist for E.129 series phones deployed as Centralized users:

- Only one address book exists, and is shared between the Sunny Day and Rainy Day modes. Some address book entries might not work if there is no route to the destination. For example, routes that require Session Manager do not work in Rainy Day.

- E.129 series phones support a primary and a secondary call server, but not explicit fallback server. Therefore, to support the use of IP Office as a rainy-day fallback server, only one session manager can be configured on the primary call back server. The secondary call back server is used to identify IP Office. For example, in an Avaya Aura® only deployment, use the secondary server for a second session manager.

- You must use IP addresses, not FQDNs, between the primary Avaya Aura®and secondary IP Office servers.

- E.129 series phones support only one dial plan. This is generally the Avaya Aura® dial plan and not the IP Office dial plan.

- Ensure that the E.129 series phones within a branch are all Centralized or all IP Office users, otherwise you must configure each phone manually.

- E.129 series phones support only two servers. You can deploy this phone as Centralized users in branches that connect to a single Session Manager and configure it with the local branch IP Office as the secondary server. However, you cannot deploy this phone as Centralized users in a branch that is configured to two Session Manager. If there are Centralized E.129 series phones in the branch, then you must not configure the IP Office and other Centralized phones in that branch to two Session Manager. If you configure the IP Office with two Session Manager, then the Centralized E.129 series phones will receive no service. This occurs if the primary Session Manager is down and the secondary Session Manager is still reachable from the IP Office. The Centralized E.129 series phones will not be able to register to the IP Office that will still be in Sunny day mode.

Additional information

For general information about administering and using E.129 series SIP phones, see the following documents:

- *Administering Avaya E.129 SIP Deskphone*, document number 17-604348.
- *Using Avaya E.129 SIP Deskphone*.

E.129 series phone limitations

E.129 phones support only two servers. You can deploy this phone as Centralized users in branches that connect to a single Session Manager and configure it with the local branch IP Office as the secondary server. However, you cannot deploy this phone as Centralized users in a branch that is configured to two Session Manager. If there are Centralized E129 phones in the branch, then you must not configure the IP Office and other Centralized phones in that branch to two Session Managers.

If you configure the IP Office with two Session Managers, then the Centralized E129 phone will receive no service. This occurs if the primary Session Manager is down and the secondary Session Manager is still reachable from the IP Office. The Centralized E129 phone will not be able to register to the IP Office that will still be in Sunny day mode.

Configuring E.129 series phones as Centralized users

Before you begin

- Ensure that an SM Line exists between IP Office and Session Manager.

- You do not need to load a separate root certificate for E.129 phones. However, identity certificates must contain the following information:

  - Subject Alternative Names containing either a **DNS** or SIP URI entry with the **IP address** of the IP Office or both.

  - You can add this information through IP Office Manager**Security Administration**.

  - The **DNS Name** and **IP Address** Subject Alternative Name fields provided must match option P47 on the SIP server.

  - To support the E.129 with TLS/SRTP in rainy day, add the following Subject Alternative Names in the IP Office Manager Security Administration:

    ```
    DNS: Enter the FQDN of IP Office, DNS: Enter the IP address of IP Office, IP:
    Enter the IP address of IP office
    ```

- Ensure that you have an available file server. You can use IP Office as your file server.

- Ensure you have the `cfg.xml` configuration file for the E.129 series phones that you are migrating to the branch environment. The configuration file can be put on Avaya Aura® or IP Office. The preferred location is IP Office.

Procedure

1. In System Manager, create Centralized users, including the IP Office endpoint profile.

   System Manager pushes user information to IP Office.

2. Prepare the `cfg.xml` configuration file and place the file on your file server.

> **❶ Important:**
>
> The primary and secondary servers must be IP addresses and not FQDNs. If you use FQDNs, and access to the DNS server is lost, long delays occur when the phone attempts name resolution.

The edited `cfg.xml` file replaces the auto-generated file if you are using IP Office as your file server.

3. To enable TLS, edit the following entries in the `cfg.xml` configuration file:

```
<!-- SIP Transport. 0 - UDP, 1 - TCP, 2 - TLS/TCP. Default is 0 -->
<P130>2</P130>

<!-- Use Actual Ephemeral Port in Contact with TCP/TLS. 0 - No, 1 - Yes. Default
is 0 -->
<P2331>1</P2331>

<!-- SIP URI Scheme when using TLS. 0 - sip, 1 - sips. Default is 1 -->
<P2329>0</P2329>
```

4. To enable SRTP, edit the following entry in the `cfg.xml` configuration file:

```
<!-- SRTP Mode. 0 – Disabled, 2 - Enabled and forced. Default is 0 -->
<P183>2</P183>
```

When using SRTP, the IP Office media security settings must match the security settings on the settings file as shown in the table. The IP Office media security settings are on the **System** > **VoIP Security** tab.

IP Office System Media Security	cfg.xml
Best effort	SRTP enabled and enforced
Disabled	SRTP disabled
Enforce	SRTP enabled and enforced

5. Configure the E.129 phone sets with the IP address of the file server using one of the following methods:

   • Use `Option 66` on the DHCP server.

   • Manually enter the IP address on the phone.

6. Reboot the E.129 series phones.

   The phones download new settings and register to the Avaya Aura® Session Manager.

Examples of file server content for E.129 phones

Sample cfg.xml file

Examples of changes you can make to the `cfg.xml` file include the following:

```
<!-- SIP Server -->
<P47>10.136.66.82</P47>

<!-- Secondary SIP Server -->
<P2312>135.55.86.86</P2312>

<!-- Firmware Server Path -->
```

```
<P192>135.55.86.86</P192>

<!-- Config Server Path -->
<P237>135.55.86.86</P237>
```

Modifying the Avaya Aura® Session Manager identity certificate

About this task

When the E.129 phone tries to register with Avaya Aura® Session Manager, the URI of the Session Manager identity certificate must match the URI of the phone. Use the following task to modify the Avaya Aura® Session Manager identity certificate:

Procedure

1. In Avaya Aura® System Manager **Inventory** > **Manage Elements**, select the Avaya Aura® Session Manager instance.

2. In **More Actions** > **Configure Identity Certificates** > **Security Module SIP**, click **Replace**.

   If the **Subject Alternative Name** is missing, you can choose to replace with an internal CA signed certificate or import a third party certificate.

3. In **Subject Alternative Name**, select **URI**.

4. In **IP**, type the IP address of the Avaya Aura® Session Manager.

5. Click **Commit**.

   ✱ **Note:**

   Restart **Security Module SIP** to apply the certificate.

Result

The phone approves the modified certificate that contains a matching URI.

B.179 series SIP phones deployed as Centralized users in IP Office Branch deployments

Configuring B.179 phones

About this task

IP Office deployed as a Branch supports B.179 R2.4 phones as Centralized users. The configuration of the Centralized B.179 phone is done through the phone's built-in configuration tool that is available through a web browser and not through a configuration file. The B.179 phone does not support manual failback. Therefore, when a deployment includes a B.179 phone as a Centralized User, the failback policy must be automatic.

Procedure

1. From **Settings** > **SIP** > **Primary account**, type the account name.

2. In **User**, type the extension number of the user phone as configured in Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and IP Office.

3. In **Registrar**, type the SIP domain name of the enterprise.

4. In **Proxy**, type the IP address of the primary Avaya Aura® Session Manager.

   ⊛ **Note:**

   The IP address must be the same for all phones in different branch offices.

5. Set the **Registration interval** to the appropriate value.

   ⊛ **Note:**

   The recommended **Registration interval** value is 60.

6. In **Settings** > **SIP** > **Fallback account**, type the account name.

7. In **User**, type the extension number of the user phone as configured in Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and IP Office.

8. In **Registrar**, type the SIP domain name of the enterprise.

9. In **Proxy**, type the IP address of the local IP Office in the branch.

   ⊛ **Note:**

   This value must be the same if there are multiple B.179 phones in the same branch. The value is different between different branches.

10. In **Registration interval**, it is recommended to set it to 60.

Next steps

If the deployment includes a secondary Avaya Aura® Session Manager, enter the IP address of the secondary account in **Secondary account** > **Proxy**. This must be the same for all phones in different branch offices.

Configuring B.179 phone advanced settings

Procedure

1. In **Settings** > **SIP** > **Advanced**, select **Allow Contact Rewrite** as **Yes**.

2. In the **Transport** section, select one of the following protocols:

   • UDP
   • TCP
   • TLS
   • SIPS

3. In the **TLS settings** section, select **Verify Server** as **On**.

4. In **Settings** > **SIP** > **Advanced**, set **Transport** to **TLS** or **SIPS**.

5. To select SRTP as mandatory or optional, choose one of the following options:

   • In **Settings** > **Media** > **Security**, set **SRTP** to **Mandatory**.

   • In **Settings** > **Media** > **Security**, set **SRTP** to **Optional**

6. In **Settings** > **Media** > **Security**, set **SRTCP** to **Not encrypted**.

7. In **Settings** > **Media** > **Security**, set **Secure signalling** to **TLS** or **SIPS**.

Chapter 6: User administration

This chapter provides the procedures to administer Centralized users from Avaya Aura® System Manager. All Centralized users are added to Session Manager to enable centralized user management. Centralized users are configured with a Session Manager profile, a Avaya Aura® Communication Manager Endpoint Profile, and an IP Office Endpoint profile that is based on a Centralized user template. Configuration of the Session Manager profile and Communication Manager Endpoint Profile enable the Centralized users to have their call processing controlled by Session Manager in the enterprise core and get their telephony features from the Communication Manager feature server in the enterprise core. Configuration of the IP Office Endpoint profile for the Centralized users enables them to have basic survivable call processing on the IP Office in the Rainy day mode.

> ✳ **Note:**
>
> If the IP Office is not managed from System Manager, you are able to administer users from IP Office Manager.

There are two types of Centralized users:.

- Centralized SIP user — a user configured as a Centralized user whose associated extension is a SIP extension.
- ATA user — a user configured as a Centralized user whose associated extension is an analog extension or analog fax device.

Centralized users must have either a SIP extension, an analog extension, or an analog fax device on the IP Office. When adding a Centralized SIP user, System Manager adds the user and the corresponding extension to the IP Office. When adding a Centralized analog user (ATA user), you must specify the module and analog port with which the ATA user is associated. System Manager then associates this user with the extension that IP Office has for that analog port. Note that an extension is always created automatically by IP Office for each physical analog or digital station port on the IP Office hardware.

Related Links

Adding Centralized SIP users to System Manager

About this task

When you add a Centralized SIP user to System Manager, you must configure a Session Manager Profile, a CM Endpoint Profile, and an IP Office Endpoint Profile on System Manager. When you configure a CM Endpoint Profile for the user and click **Commit & Continue** to save the changes, the user is identified as a Centralized user.

Procedure

1. On the System Manager console, under **Users**, click **User Management**.

2. In the left navigation pane, click **Manage Users**.

3. On the **User Management** page, click **New**.

4. On the **New User Profile** page, in the **Identity** section, do the following:

   a. In the **Last Name** field, enter the user's last name.

   > ⊛ **Note:**
   >
   > Depending on how the branches and stations in your system are named and organized, you could enter a location name in this field, for example `Chicago 25`. Then in the next field, **First Name**, you could enter a location within that branch, for example `cashier`.

   b. In the **First Name** field, enter the user's first name.

   c. In the **Middle Name** field, enter the user's middle name.

   d. In the **Description** field, enter a description of this user profile.

   e. In the **Login Name** field, enter the extension user login in the format, username@domainname.com or extension@domainname.com. For example, nsmith@avaya.com or 5002432@avaya.com.

      For survivability mode operation with an IP Office system, the user name without the domain name should match the user name configured in the branch system.

   f. In the **Authentication Type** drop-down box, accept the default setting, **Basic**.

   g. In the **Password** field, enter the password required to log into System Manager for personal web configuration.

   h. In the **Confirm Password** field, enter the password again.

   i. In the **Localized Display Name** field, enter the name to be used as the calling party.

   j. In the **Endpoint Display Name** field, enter the user's full name.

   k. In the **Title** field, enter the user's title if applicable.

   l. In the **Language Preference** drop-down box, select the appropriate language.

   m. In the **Time Zone** drop-down box, select the user's time zone.

   n. In the **Employee ID** field, enter the user's employee ID.

o. In the **Department** field, enter the user's department.

p. In the **Company** field, enter the name of the user's company.

q. To add a postal address for this user, do the following:

   a. Expand the **Address** section.

   b. Click **New**.

   c. On the **Add Address** page, complete the fields as appropriate.

r. To add multiple phone numbers for this user, do the following:

   a. Expand the **Phone Details** section.

   b. Complete the fields as appropriate.

   c. Click **Add**.

5. To specify a localized language, expand the **Localized Names** section, and do the following:

   a. Click **New**.

   b. In the **Language** drop-down box, select the language for displaying the user name.

   c. In the **Display Name** field, enter the user's name.

   d. Click **Add**.

6. Click the **Communication Profile** tab to expand that section, and do the following:

   a. In the **Communication Profile Password** field, enter the appropriate communication profile password.

   b. In the **Confirm Password** field, enter the password again.

   c. Accept the default values for the **Name** field and **Default** check box.

7. Expand the **Communication Address** section, and do the following:

   a. Click **New**.

   b. In the **Type** drop-down box, select **Avaya SIP**.

   c. In the **Fully Qualified Address** field, enter the extension and select the domain from the drop-down box.

   d. Click **Add** to add the record.

8. Click the **Session Manager Profile** check box, and do the following:

   a. In the **Primary Session Manager** drop-down box, select the Session Manager instance that should be used as the home server for the currently displayed communication profile.

   b. In the **Secondary Session Manager** drop-down box, select the Session Manager instance that should be used as the backup server for the currently displayed communication profile.

   c. In the **Survivability Server** drop-down box, select the IP Office in the user's branch as the survivability server for the currently displayed communication profile.

d. In the **Max. Simultaneous Devices** drop-down box, select the appropriate number. This is the maximum number of endpoints that can be registered at the same time using this communication profile.

e. For the **Block New Registration When Maximum Registrations Active?** check box, accept the default, unchecked.

f. In the **Origination Sequence** drop-down box, select the Communication Manager Feature Server or Evolution Server.

g. In the **Termination Sequence** drop-down box, select the Communication Manager Feature Server or Evolution Server.

h. In the **Home Location** drop-down box, select the location of the IP Office branch in which the Centralized user is located.

i. In the **Conference Factory Set** drop-down box, select a Conference Factory set to enable media-capability based selection for routing to conferencing SIP entities.

9. Click the **CM Endpoint Profile** check box, and do the following:

a. In the **System** drop-down box, select the appropriate Communication Manager entity.

b. In the **Profile Type** drop-down box, accept the default setting, **Endpoint**.

c. For the **Use Existing Endpoints** check box, do one of the following:

a. If you previously created the SIP extension in Communication Manager, check this check box.

b. If it is a new extension that has not been created before, leave this check box unchecked.

d. In the **Extension** field, enter the same extension number you added in the **Fully Qualified Address** field in Step 7c above.

> ✳ **Note:**
>
> The Communication Manager extension number for a Centralized user must be the same as the extension number entered in the Communication Address section above.

e. In the **Template** drop-down box, select an appropriate template matching the telephone type as configured on Communication Manager.

System Manager auto-populates the **Port** field when a template is selected.

f. In the **Set Type** field, accept the default.

g. In the **Security Code** field, enter the security code.

h. In the **Voice Mail Number** field, enter the number used to access the voicemail system.

i. In the **Preferred Handle** drop-down box, select the appropriate handle.

j. Check the **Enhanced Callr-Info display for 1-line phones** check box to select this option.

k. Check the **Delete Endpoint on Unassign of Endpoint from User or on Delete Users** check box to select this option.

l. For the **Override Endpoint Name** check box, accept the default, checked.

m. Click **Commit & Continue**.

> ✳ **Note:**
>
> Be sure to click **Commit & Continue** before continuing with the Step 10. When you click **Commit & Continue**, System Manager automatically populates the **Extension** and **Set Type** fields when you configure the IP Office Endpoint Profile.
>
> You do not need to configure the Messaging Profile section for IP Office at this time.

10. Click the **IP Office Endpoint Profile** check box, and do the following:

a. In the **System** drop-down box, select the IP Office in the user's branch.

b. In the **Template** drop-down box, select the appropriate template. The templates listed in this drop-down box are Centralized User templates.

   When you select a template, the **Set Type** field is automatically populated based on the template selected. The **Set Type** field is read-only.

c. For the **Use Existing Extension** check box, accept the default, unchecked.

d. For the **Extension** field, accept the extension number that appears. System Manager automatically populated the **Extension** field with the extension you specified when you configured the **CM Endpoint Profile**.

e. For the **Delete Extension On User Delete** check box, accept the default, unchecked.

> ✳ **Note:**
>
> For users with IP Office endpoint profile, adding, deleting, or editing the user in System Manager should be done only when the respective IP Office is reachable. Such changes in System Manager will automatically and consistently update the data in both System Manager and IP Office. If you cannot reach the IP Office permanently and if System Manager has stale user records, then set the **force_delete_user** property to *True* to delete such users from the System Manager database. After the user is deleted, set the **force_delete_user** property to *False* and restart the Jboss server.
>
> If you delete users from System Manager when IP Office is temporarily unreachable, it would result the deletion of data from System Manager. However, as the IP Office is not reachable, the data from IP Office will not be deleted. The data needs to be deleted using the **Unrestricted mode** from IP Office Manager. After data from IP Office is deleted, you need to synchronize the users and the system configuration.

11. Click **Commit**.

A Centralized user is added on the IP Office and is associated with a user in System Manager.

12. Repeat this procedure for each Centralized user you want to add.

Related Links

Adding ATA users to System Manager

About this task

When you add an ATA user to System Manager, you must configure a Session Manager Profile, a Communication Manager Endpoint Profile, and an IP Office Endpoint Profile on System Manager. When you configure a Communication Manager Endpoint Profile for the user and click **Commit & Continue** to save the changes, the user is identified as a Centralized user.

Procedure

1. On the System Manager console, under **Users**, click **User Management**.

2. In the left navigation pane, click **Manage Users**.

3. On the **User Management** page, click **New**.

4. On the **New User Profile** page, in the Identity section, do the following:

   a. In the **Site** drop-down box, select the appropriate site.

   b. In the **Last Name** field, enter the user's last name.

   > ⭐ **Note:**
   >
   > Depending on how the branches and stations in your system are named and organized, you could enter a location name in this field, for example `Chicago 25`. Then in the next field, **First Name**, you could enter a location within that branch, for example `cashier`.

   c. In the **First Name** field, enter the user's first name.

   d. In the **Middle Name** field, enter the user's middle name.

   e. In the **Description** field, enter a description of this user profile.

   f. In the **Login Name** field, enter the extension user login in the format, username@domainname.com or extension@domainname.com. For example, nsmith@avaya.com or 5002432@avaya.com.

   g. In the **Authentication Type** drop-down box, accept the default setting, **Basic**.

   h. In the **Password** field, enter the password required to log into System Manager for personal web configuration.

   i. In the **Confirm Password** field, enter the password again.

   j. In the **Localized Display Name** field, enter the name to be used as the calling party.

   k. In the **Endpoint Display Name** field, enter the user's full name.

l. In the **Title** field, enter the user's title if applicable.

m. In the **Language Preference** drop-down box, select the appropriate language.

n. In the **Time Zone** drop-down box, select the user's time zone.

o. In the **Employee ID** field, enter the user's employee ID.

p. In the **Department** field, enter the user's department.

q. In the **Company** field, enter the name of the user's company.

r. To add a postal address for this user, do the following:

   a. Expand the **Address** section.

   b. Click **New**.

   c. On the **Add Address** page, complete the fields as appropriate.

s. To add multiple phone numbers for this user, do the following:

   a. Expand the **Phone Details** section.

   b. Complete the fields as appropriate.

   c. Click **Add**.

5. To specify a localized language, expand the **Localized Names** section, and do the following:

   a. Click **New**.

   b. In the **Language** drop-down box, select the language for displaying the user name.

   c. In the **Display Name** field, enter the user's name.

   d. Click **Add**.

6. Click the **Communication Profile** tab to expand that section, and do the following:

   a. In the **Communication Profile Password** field, enter the appropriate communication profile password.

   b. In the **Confirm Password** field, enter the password again.

   c. Accept the default values for the **Name** field and **Default** check box.

7. Expand the **Communication Address** section, and do the following:

   a. Click **New**.

   b. In the **Type** drop-down box, select **Avaya SIP**.

   c. In the **Fully Qualified Address** field, enter the extension and select the domain from the drop-down box.

   d. Click **Add** to add the record.

8. Click the **Session Manager Profile** check box, and do the following:

   a. In the **Primary Session Manager** drop-down box, select the Session Manager instance that should be used as the home server for the currently displayed communication profile.

b. In the **Secondary Session Manager** drop-down box, accept the default **(None)**.

c. In the **Survivability Server** drop-down box, accept the default **(None)**.

d. In the **Max. Simultaneous Devices** drop-down box, select the appropriate number. This is the maximum number of endpoints that can be registered at the same time using this communication profile.

e. For the **Block New Registration When Maximum Registrations Active?** check box, accept the default, unchecked.

f. In the **Origination Sequence** drop-down box, select the Communication Manager Feature Server or Evolution Server.

g. In the **Termination Sequence** drop-down box, select the Communication Manager Feature Server or Evolution Server.

h. In the **Home Location** drop-down box, select the location of the IP Office branch in which the ATA user is located.

i. In the **Conference Factory Set** drop-down box, select a Conference Factory set to enable media-capability based selection for routing to conferencing SIP entities.

9. Click the **CM Endpoint Profile** check box, and do the following:

a. In the **System** drop-down box, select the appropriate Communication Manager entity.

b. In the **Profile Type** drop-down box, accept the default setting, **Endpoint**.

c. Check the **Use Existing Endpoints** check box to select this option.

d. In the **Extension** field, enter the same extension number you added in the **Fully Qualified Address** field in Step 7c above.

   > ✱ **Note:**
   >
   > The Communication Manager extension number for a Centralized user must be the same as the extension number entered in the Communication Address section above.

e. In the **Template** drop-down box, select an appropriate template matching the telephone type as configured on Communication Manager.

   System Manager auto-populates the **Port** field when a template is selected.

f. In the **Set Type** field, accept the default.

g. In the **Security Code** field, enter the security code.

h. In the **Voice Mail Number** field, enter the number used to access the voicemail system.

i. In the **Preferred Handle** drop-down box, select the appropriate handle.

j. Check the **Enhanced Callr-Info display for 1-line phones** check box to select this option.

k. Check the **Delete Endpoint on Unassign of Endpoint from User or on Delete Users** check box to select this option.

l. For the **Override Endpoint Name** check box, accept the default, checked.

    m. Click **Commit & Continue**.

> ✳ **Note:**
>
> Be sure to click **Commit & Continue** before continuing with the Step 10. When you click **Commit & Continue**, System Manager automatically populates the **Extension** and **Set Type** fields when you configure the IP Office Endpoint Profile.
>
> You do not need to configure the Messaging Profile section for IP Office at this time.

10. Click the **IP Office Endpoint Profile** check box, and do the following:

    a. In the **System** drop-down box, select the IP Office in the user's branch.

    b. In the **Template** drop-down box, select the appropriate template.

> ✳ **Note:**
>
> System Manager automatically populates the **Set Type** field based on the type of user template selected. This field is read-only.

    c. For the **Use Existing Extension** check box, accept the default, unchecked.

    d. For the **Extension** field, accept the extension number that appears. System Manager automatically populated the **Extension** field with the extension you specified when you configured the **CM Endpoint Profile**.

    e. For the **Delete Extension On User Delete** check box, accept the default, unchecked.

11. Click **Commit**.

An ATA user is added on the IP Office and is associated with a user in System Manager.

12. Repeat this procedure for each ATA user you want to add.

Related Links

Editing the IP Office Endpoint Profile for a user

About this task

Use this procedure to edit an IP Office Endpoint Profile for a Centralized user.

> ✳ **Note:**
>
> If you are using Avaya Aura® System Manager to edit an existing B5800 Branch Gateway R6.2 user and the System Manager version is R6.3.2, you must ensure that the **Local Number Length** field is configured correctly in IP Office Manager. If it is not, you will not be able to modify the extension. An error message will appear that indicates the extension length is invalid. For information on how to configure the **Local Number Length** field in IP Office Manager, see Setting the branch prefix and local number length for extension numbering in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

Procedure

1. On the System Manager console, under **Users**, click **User Management**.

2. In the left navigation pane, click **Manage Users**.

3. From the list of users on the User Management page, select the user you want to edit.

4. Click **Edit**.

5. Click the **Communication Profile** tab to expand that section.

6. Expand the **Communication Address** section.

7. Expand **IP Office Endpoint Profile**.

8. To apply a different template to this user, in the **Template** drop-down box, select the appropriate template.

9. To change the extension assigned to this user, do one of the following:

   - Click the **Use Existing Extension** check box, and select an unassigned extension from the drop-down box.

   - Select a module-port combination from the **Module-Port** drop-down box and enter the new extension in the **Extension** field.

     > ✳ **Note:**
     >
     > The module-port combination is valid only for digital and analog set types.

10. To change the **Module-Port** or Extension type of a user, do the following:

    a. Clear the **IP Office Endpoint Profile** check box to remove the IP Office Endpoint profile of the user and click the **Commit & Continue** button

    b. Select the **IP Office Endpoint Profile** check box to reassign the IP Office Endpoint profile with new **Module-Port** or Extension type and click **Commit**.

11. To change other parameters for this user, click the **Endpoint Editor** button.

    IP Office Manager is launched where you can edit the user and extension fields for this user.

12. Update the fields as appropriate.

13. Click **Save**.

    You return to the edit user window in System Manager.

14. Click **Commit**.

Related Links

Viewing Session Manager registered users

Procedure

1. On the System Manager console, under **Elements**, click **Session Manager**.

2. In the left navigation pane, click **System Status > User Registrations**.

   The list of registered users appears.

3. To see the complete registration status of an individual user, click **Show** in the Details column for the user you want to view.

Related Links

User administration on page 59

Appendix A: Communication Manager configuration example

During normal operation, calls made by a Centralized phone are received by the Avaya Aura®Session Manager and passed to the extension's Communication Manager Feature Server or Evolution Server. The Communication Manager Feature Server or Evolution Server then sends the call back to the Avaya Aura®Session Manager for routing elsewhere in the Avaya Aura® network.

In this example, a Centralized phone at branch 811 dials an external number in local area code 908. This happens to be local to branch 811, so we want Avaya Aura®Session Manager and Communication Manager Feature Server or Evolution Server to route the call to that branch to be dialed as a local PSTN call.
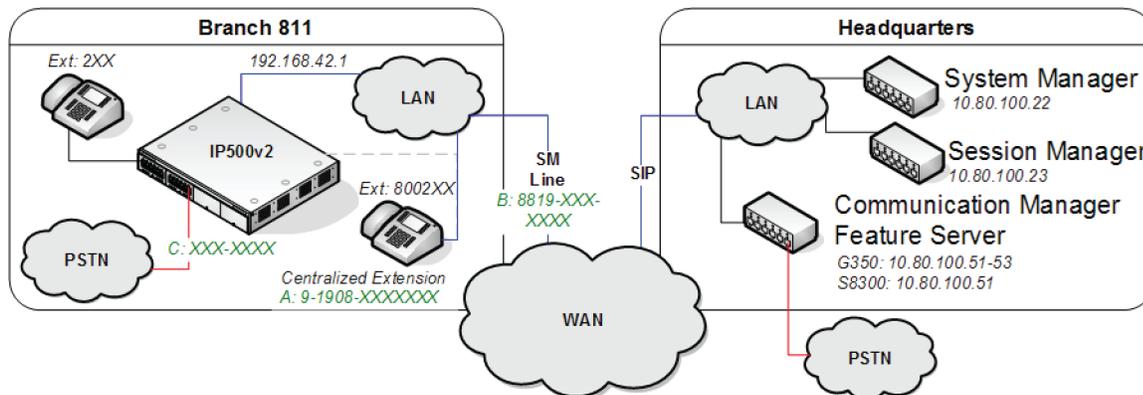

Figure 1: Communication Manager configuration example

For this example, the call routing is as follows:

1. The Centralized phone co-located at branch 811 dials 9-1908-555-1111 (A).

2. This sends a SIP INVITE to the Avaya Aura® Session Manager. The IP Office system at branch 811 is not involved.

3. The Avaya Aura® Session Manager identifies that the call is from an extension that matches an assigned Communication Manager Feature Server or Evolution Server extension and so forwards the SIP INVITE to the Communication Manager Feature Server or Evolution Server.

4. The Communication Manager Feature Server or Evolution Server receives the SIP INVITE from Avaya Aura® Session Manager on a SIP trunk group number (for this example 42).

5. The Communication Manager Feature Server or Evolution Server identifies the IP address of the extensions as an IP address mapped to IP Network Region 11 and Location 11.

6. The leading 9 in the dialed digit string matches the ARS Access Code. The 9 is removed from the dialed digit string.

7. The ARS Digit Analysis Table for Location 11 is queried for a match on the remaining digits 19085551111.

8. A match on 1908 is found, specifying Route Pattern 11.

9. Route Pattern 11 routes the call to SIP Trunk Group Number 32. This connects the Communication Manager Feature Server or Evolution Server to the Avaya Aura®Session Manager and is specifically configured for routing local PSTN calls to branches.

10. The Communication Manager Feature Server or Evolution Server sends a new SIP INVITE to Avaya Aura®Session Manager over SIP Trunk Group Number 32 with the dialed digits of 19085551111.

11. Avaya Aura® Session Manager finds a configured Dial Pattern that matches the dialed number 19085551111 with associated Routing Policy that routes the call to the IP Office at branch 811.

12. Avaya Aura® Session Manager forwards the SIP INVITE with dialed digits string 19085551111 to the IP Office in branch 811.

13. Avaya Aura® Session Manager adds an adaptation to ensure correct routing.

   For example, to use local trunks, a local IP Office user will dial **9** + PSTN number or **0** + PSTN number. For a Centralized user to use local trunks, Session Manager adds the short code (for example, **9** or **0**) that the local IP Office user dials to access the local trunk.

14. The IP Office internally routes the call to one of its PSTN trunks.

Communication Manager configuration required for Centralized phone support

The topics in this section provide the Communication Manager procedures required to configure support for Centralized phones. They are provided here as a reference for the Communication Manager configuration required to implement the PSTN call flow described in Communication Manager configuration example on page 70.

The procedures are provided using the Communication Manager SAT commands. However, you can use a different administrative interface, such as System Manager, to perform this configuration.

Verifying Communication Manager licenses

The license file installed on the Communication Manager system controls the maximum capacities permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

1. Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features required for this scenario.

2. Enter the **display system-parameters customer-options** command.

3. Navigate to Page 2 and compare the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column to verify that there is sufficient remaining capacity for SIP trunks.

   The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

Configuring direct media on Communication Manager

Use this procedure to enable the Initial IP-IP Direct Media parameter in Avaya Aura® Communication Manager. In IP Office Centralized or Mixed enterprise branch deployments where there are Centralized users, this is required to prevent media flow from unnecessarily crossing the WAN to a central Communication Manager media resource.

1. Enter the **change signaling-group n** command where **n** is the SIP signaling group that connects Communication Manager to Session Manager. Then do the following:

   a. In the **Direct IP-IP Audio Connections** field, enter `yes`.

      Setting this field to **yes** allows shuffling between endpoints and between endpoints and the local PSTN trunk. This frees resources from the central gateway.

   b. In the **Initial IP-IP Direct Media** field, enter `yes`.

      Setting this field to **yes** allows the phones to use their own resources to originate a call rather than use resources from the central gateway.

2. Enter the **change ip-network-region n** command where **n** is the network region in which the system resides. Then do the following:

   a. In the **Intra-region IP-IP Direct Audio** field, enter `yes`.

   b. In the **Inter-region IP-IP Direct Audio** field, enter `yes`.

      Setting these fields to **yes** frees DSP resources for calls in the same region or for calls between different network regions.

Configuring trunk-to-trunk transfer

Use this procedure to configure Communication Manager to allow trunk-to-trunk transfers.

1. Enter the **change system-parameters features** command.

2. In the **Trunk-to-Trunk Transfer** field, enter the appropriate number.

   ✱ **Note:**

   If the **Trunk-to-Trunk Transfer** field is set to **all**, this will enable all trunk-to-trunk transfers on a system-wide basis.

   Note that this feature poses significant security risk, and must be used with caution. As an alternative, the trunk-to-trunk feature can be implemented using **Class Of Restriction** or **Class Of Service** levels.

Configuring IP node names

Use this procedure to add Avaya Aura®Session Manager as an IP node.

1. Enter the **change node-names ip** command.

2. In the **Name** field, enter a name for this IP node.

3. In the **IP Address** field, enter the IP address of the Avaya Aura® Session Manager's Security Module (SM-100) interface.

Configuring IP codec set

If necessary, configure an IP codec set for use with SIP calls.

1. Enter the **change ip-codec-set n** command, where **n** is the codec set number to be used.

2. In the **Audio Codec** field, enter the desired audio codec type.

3. Retain the default values for the remaining fields.

Configuring IP network regions

An IP address map can be used for network region assignment. The network region assignment can be used to vary behaviors within and between regions. Typically, though this can be varied, each location will match an IP region and vice versa.

The following screen illustrates a subset of the IP network map used for this example configuration. Branch 811 has IP addresses in 192.168.42.0/24 assigned to network region 11.

```
display ip-network-map                                      Page   1 of  63
                          IP ADDRESS MAPPING

                                        Subnet Network      Emergency
  IP Address                            Bits   Region  VLAN Location Ext
  --------------------------------------------- ------ ------- ---- -------------
  FROM: 10.1.2.0                        /24    1       n
    TO: 10.1.2.255
  FROM: 10.32.1.0                       /24    1       n
    TO: 10.32.1.255
  FROM: 10.32.2.0                       /24    1       n
    TO: 10.32.2.255
  FROM: 192.168.42.0                    /24    11      n
    TO: 192.168.42.255
```

The following screens illustrate important aspects of the settings for each IP Network Region. The IP Network Region for each branch is mapped to the matching location. The values used for Branch 812 in IP Network Region 12 are shown below.

```
display ip-network-region 12                               Page   1 of  19
                           IP NETWORK REGION
  Region: 12
Location: 12          Authoratative Domain: example.com
    Name: Branch 811
MEDIA PARAMETERS                 Intra-region IP-IP Direct Audio: yes
      Codec Set: 1               Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
```

- The **Authoritative Domain** matches the SIP domain configured in the Avaya Aura®Session Manager and the IP Office.

- The **Codec Set** for intra-region calls is set to the codec set created for SIP calls.

- The **Intra region IP-IP Direct Audio** and **Inter region IP-IP Direct Audio** parameters are set to **yes** to allow direct media paths within and between regions. This minimizes the use of media resources in the Media Gateway.

The connectivity between network regions is specified under the Inter Network Region Connection Management heading, beginning on Page 3. Codec set 1 is specified for connections between network region 11 and network region 1.

```
display ipnetwork-region 12                          Page   3 of  19

  Source Region: 11    Inter Network Region Connection Management   I        M
                                                                    G   A    e
  dst codec direct  WAN-BW-Limits   Video        Intervening   Dyn  A   G    a
  rgn  set   WAN   Units   Total Norm  Prio Shr Regions        CAC  R   L    s
  1    1     y     NoLimit                                          n  all
  2
  3
  4
  5
  6
  7
  8
  9
 10
 11    1                                                             all
 12    1                                                             all
```

The ip-network-region form for Network Region 1 needs to be similarly configured. Network region 1 is for phones and servers as well as Session Manager at the central location.

SIP signaling group and trunk group

For this example configuration, two SIP signaling groups and two associated trunk groups are used between Communication Manager and Avaya Aura® Session Manager in the example configuration.

The primary SIP trunk group and its associated signaling group are used for regular call signaling and media transport to/from SIP phones registered to Avaya Aura® Session Manager including Centralized phones at the branches. The secondary SIP trunk group and its associated signaling group are used for routing calls from branch phones to native (non-toll) PSTN destinations.

Note that a single trunk group could be used for both purposes. However, the use of two trunk groups provides added flexibility to change trunk parameters independently. Tracing call legs within Communication Manager is also simplified.

Configuring SIP signaling groups

For Communication Manager to act as a Communication Manager Feature Server supporting Centralized phones, an IMS enabled SIP trunk to Avaya Aura®Session Manager is required.

1. Enter the **add signaling-group n** command, where **n** is an available signaling group number.
2. Enter the following values for the specified fields and retain the default values for all remaining fields.

    a. In the **Group Type** field, enter `sip`.
    b. In the **Transport Method** field, enter `tls`.

     c. In the **IMS Enabled?** field, enter `y`.

     d. In the **Near-end Node Name** field, enter the IP node name added for the Communication Manager Feature Server or Evolution Server.

     e. In the **Far-end Node Name** field, enter the IP node name added for the Avaya Aura®Session Manager.

     f. In the **Near-end Listen Port** field, enter `5061`.

     g. In the **Far-end Listen Port** field, enter `5061`.

     h. In the **Far-end Network Region** field, enter the IP network region number assigned to the Avaya Aura®Session Manager.

     i. In the **Far-end Domain** field, enter the SIP domain name.

     j. In the **DTMF over IP** field, enter **rtp-payload**.

The screen below shows signaling group 42 which is used in the example configuration as the primary signaling group.

```
add signaling-group 42
                         SIGNALING GROUP

 Group Number: 42              Group Type: sip
                         Transport Method: tls
  IMS Enabled? y


   Near-end Node Name: cm                 Far-end Node Name: sm1
 Near-end Listen Port: 5061             Far-end Listen Port: 5061
                                      Far-end Network Region: 1
                                             Far-end Domain: example.com


                                        Bypass If IP Threshold Exceeded? n
 Incoming Dialog Loopbacks: eliminate          RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload         Direct IP-IP Audio Connections? y
```

The screen below shows signaling group 32 which is used in the example configuration as the "Secondary" signaling group to be associated with trunk group 32 for routing local PSTN calls from branch phones to Avaya Aura® Session Manager. Note that all the settings for this signaling group are identical to those for signaling group 42 except the **Transport Method** is set to **tcp** (the port numbers will change automatically to **5060**).

```
add signaling-group 32
                            SIGNALING GROUP

 Group Number: 32                 Group Type: sip
                            Transport Method: tcp
   IMS Enabled? y



    Near-end Node Name: cm               Far-end Node Name: sm1
 Near-end Listen Port: 5060             Far-end Listen Port: 5060
                                      Far-end Network Region: 1
                                              Far-end Domain: example.com


                                        Bypass If IP Threshold Exceeded? n
 Incoming Dialog Loopbacks: eliminate            RFC 3389 Comfort Noise? n
            DTMF over IP: rtp-payload       Direct IP-IP Audio Connections? y
```

Configuring SIP trunk groups

Next, SIP trunk groups need to be added.

1. Enter the **add trunk-group n** command, where **n** is an available trunk group number to add to SIP trunk groups.

2. Enter the following values for the specified fields, and retain the default values for the remaining fields.

   a. In the **Group Type** field, enter `sip`.

   b. In the **Group Name** field, enter a description for the trunk group.

   c. In the **TAC** field, enter an available trunk access code as per the dial plan.

   d. In the **Service Type** field, enter `tie`.

   e. In the **Signaling Group** field, enter the signaling group number .

   f. In the **Number of Members** field, enter the number that is equal to the maximum number of concurrent calls supported.

```
add trunk-group 42                                   Page   1 of   21
                            TRUNK GROUP

 Group Number: 42            Group Type: sip          CDR Reports: y
   Group Name: SIP endpoints        COR: 1     TN: 1      TAC: *142
     Direction: two-way       Outgoing Display? n
  Dial Access? n                                Night Service:
 Queue Length: 0
 Service Type: tie              Auth Code? n

                                         Signaling Group: 42
                                       Number of Members: 20
```

Navigate to Page 3, and enter **private** for the **Numbering Format** field as shown below. Use default values for all other fields.

```
add trunk-group 42                                         Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n                    Measured: none
                                                       Maintenance Tests? y


                 Numbering Format: private
                                               UUI Treatment: service-provider

                                               Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n
```

The trunk group 32 used for routing local PSTN calls from branch phones is similarly configured.

Configuring route patterns

Configure a route pattern to correspond to each of the two newly added SIP trunk groups.

1. Enter the **change route-pattern n** command, where **n** is an available route pattern.

2. Enter the following values for the specified fields, and retain the default values for the remaining fields.

   a. In the **Pattern Name** field, enter a descriptive name for the route pattern.

   b. In the **Grp No** field, enter the trunk group number configured in

   c. In the **FRL** field, enter the Facility Restriction Level that allows access to this trunk, **0** being least restrictive.

Configuring private numbering

1. Enter the **change private-numbering 0** command to define the calling party number to be sent

2. Add an entry for the

In the example shown below, all calls originating from a 3-digit extension beginning with 2 and routed across any trunk group (shown by the **Trk Grp(s)** setting being blank) will result in a 3-digit calling number. The calling party number will be in the SIP **From** header.

```
change private-numbering 0                                   Page   1 of   2
                        NUMBERING - PRIVATE FORMAT

Ext Ext              Trk           Private         Total
Len Code             Grp(s)        Prefix          Len
 3   4                                              3       Total Administered: 1
                                                              Maximum Entries: 540
```

Configuring AAR

1. Enter the **change aar analysis** command to add an entry for the extension range corresponding to the branch Centralized phones.

2. Enter the following values for the specified fields, and retain the default values for the remaining fields.

   a. In the **Dialed String** field, enter the dialed prefix digits to match on.

   b. In the **Total Min** field, enter the minimum number of digits.

   c. In the **Total Max** field, enter the maximum number of digits.

   d. In the **Route Pattern** field, enter the route pattern number configured for these extensions.

   e. In the **Call Type** field, set this to **aar**.

```
change aar analysis 4                                      Page   1 of   2
                        AAR DIGIT ANALYSUS TABLE
                             Location: all              Percent Full:    2

          Dialed            Total      Route   Call    Node    ANI
          String          Min  Max   Pattern  Type    Num     Reqd
     4                      3    3      42     aar             n
    49998                   5    5      32     aar             n
    50000                   5    5       1     aar             n
```

ARS Access Code

The example configuration designates **9** as the ARS Access Code. This is shown below on Page 1 of the **change feature-access-codes** form. Calls with a leading 9 will be directed to the ARS routing table.

```
change feature-access-codes                                Page   1 of   8
                          FEATURE ACCESS CODE (FAC)
          Abbreviated Dialing List1 Access Code:
          Abbreviated Dialing List2 Access Code:
          Abbreviated Dialing List3 Access Code:
  Abbreviated Dial - Prgm Group List Access Code:
                    Announcement Access Code: *56
                    Answer Back Access Code:
                       Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
      Auto Route Selection (ARS) - Access Code: 9    Access Code 2:
              Automatic Callback Activation: *57   Deactivation: *58
```

Location specific ARS digit analysis

Location based analysis is used before global analysis. Using it we could apply rules that only apply to calls from Centralized phones at location 11. For example, the pattern below routes calls prefixed 1908 from location 11 back to the Avaya Aura® Session Manager using Route Pattern 32 on page 78 when a match occurs.

The **change ars analysis location x y** command is used to make location specific routing entries where the **x** is the location number and the **y** is the dialed digit string to match on.

```
change ars analysis location 11 1908                          Page   1 of   2
                        ARS DIGIT ANALYSIS TABLE
                          Location:   11          Percent Full:   2

         Dialed           Total      Route     Call   Node  ANI
         String         Min  Max   Pattern    Type    Num   Reqd
     1908               11   11      32        natl          n
```

However for our example, we want to route any dialing prefixed with 1908, regardless of location, which we can do in the Global ARS Digit Analysis on page 80.

Global ARS Digit Analysis

For this example we want all outgoing external calls prefixed with 1908 to be routed back to the Avaya Aura® Session Manager, regardless of the location of the Centralized phone making the call.

The **change ars analysis y** command is used to make global routing entries where the **y** is the dialed digit string to match. A match on this table can occur if there is no match on the ARS Location Specific ARS Analysis on page 80.

The global ARS table as used in the example configuration is shown below. Long distance calls, 1 + 10 digits, will match the Dialed String of 1 with 11 digits and select Route Pattern 3 on page 78.

Route Pattern 3 is configured to use a Trunk Group that connects to the Communication Manager Feature Server or Evolution Server at the headquarters location for PSTN calls to and from that site.

```
display ars analysis 1                                        Page   1 of   2
                        ARS DIGIT ANALYSIS TABLE
                          Location:   all          Percent Full:   2

         Dialed           Total      Route     Call   Node  ANI
         String         Min  Max   Pattern    Type    Num   Reqd
     1                 11   11      3         hnpa          n
     101xxxx0          8    8      deny       op            n
     101xxxx0          18   18     deny       op            n
     1908              11   11      32        natl          n
```

Glossary

9600 series H.323 phones

This term describes the 9600 series IP Deskphones running H.323 firmware. When running H.323 firmware, these phones are used as IP Office phones in a Distributed enterprise branch deployment. The following 9600 series phones can run H.323 firmware and are supported for use by IP Office users: 9620, 9630, 9640, 9650, 9608, 9611G, 9621G, and 9641G.

9600 series SIP phone

This term describes the 9600 series IP Deskphones running SIP firmware. When running SIP firmware, these phones are used as Centralized phones in a Centralized enterprise branch deployment. The following 9600 series phones can run SIP firmware and are supported for use by Centralized users: 9620, 9630, 9640, 9650, 9601, 9608, 9611G, 9621G, and 9641G.

Branch office

A geographic office location for an enterprise other than the main enterprise location. A branch office is typically smaller and has fewer employees than the main office for an enterprise. A branch office is involved in business activities related to the local market's needs.

Centralized enterprise branch deployment option

This term describes deployments where all users in a branch are Centralized users. See Centralized user.

Centralized management

This term is used to describe a central management system that delivers a set of shared management services and provides a single access interface to administer multiple branch locations and multiple distributed IP Office users.

Centralized phone

This term describes a phone that is used by a Centralized user. See Centralized user.

Centralized trunking

This term describes routing outgoing external calls from the branch sites to the central site in order to utilize the central sites PSTN trunks. The same applies for distributing incoming PSTN calls from the central site to the appropriate branches.

Centralized user

This term describes a user whose call processing is controlled by Avaya Aura® Communication Manager Feature Server or Evolution Server in the enterprise core. During normal operation, the Centralized user gets their telephony features and services from core applications such as the Communication Manager Feature Server or Evolution Server. Through the core Avaya Aura® Session Manager, the Centralized user can also access

local PSTN trunks and services, such as local paging, local auto-attendant, and local Meet-me conferencing, on the IP Office in the branch. If WAN connectivity to the Avaya Aura®Session Manager is lost, the Centralized user automatically gets basic services from the local IP Office. When connection to Avaya Aura®Session Manager is available again, failback occurs either automatically or by manual administrative action where call processing for the Centralized user is returned to being controlled by Avaya Aura®Session Manager.

A Centralized user must be configured on the Avaya Aura®Session Manager, on Communication Manager, and on the IP Office. On the IP Office, the Centralized user must have either a SIP extension or an analog extension. There are two types of Centralized users:

- Centralized SIP user — a user configured as a Centralized user whose associated extension is a SIP extension.

- ATA user — a user configured as a Centralized user whose associated extension is an analog extension or analog fax device.

✱ Note:

Standard analog phones and fax are supported for use by ATA users.

Distributed enterprise branch deployment option	This term describes deployments where all users in a branch are IP Office users. See IP Office user.
Distributed trunking	This term describes the scenario where each branch retains and uses its own PSTN trunks for incoming and outgoing external calls.
E.164 format	E.164 is a numbering format recommended by the International Telecommunications Union - Telecommunications (ITU-T). E.164 can have a maximum of 15 digits and is preceded by a +.
Extension	This term describes a unique number supported within the dial-plan that is assigned to a user. An extension also has associated endpoint(s) configured, where the endpoint can be either a hard device such as a telephone or a soft client running on a PC, mobile device, or tablet.
Failback	This term is used for the situation where a centralized extension that is working with a survivability call controller detects that its normal call controller is available again. The extension will go through a process of failback to its normal call controller.
Failover	This term is used for the situations where a centralized extension's preferred call controller is no longer available. The extension will go through a process of failover to the first available of its configured alternate call controllers which then provides survivability services to the extension.

IP Office phone	This term describes a phone that is used by an IP Office user. See IP Office user.
IP Office user	This term describes a user who gets their telephony features and services from the local IP Office. IP Office users were formerly referred to as distributed users, local users, or native users.
	IP Office users with non-IP phones are connected to the IP Office while IP Office users with IP and SIP endpoints can be administered with IP Office as their controller. Access to and from the rest of the Avaya Aura® network is via the IP Office system's SM Line, which connects to Avaya Aura® Session Manager across the enterprise WAN. This connection allows for VoIP connectivity to other sites in the enterprise, to centralized trunking, and to centralized applications such as conferencing and messaging.
Local management	This term is used to describe managing an IP Office device using the local IP Office Manager application.
Mixed enterprise branch deployment option	This term describes deployments where there are Centralized users and IP Office users in a single branch. The Centralized users get their telephony services delivered by the Communication Manager Feature Server or Evolution Server in the core and the IP Office users get their telephony services delivered by the local IP Office.
Mixed mode trunking	The flexibility of Avaya Aura® Session Manager is such that both centralized and distributed trunking can be used. For example, routing all national and international calls via centralized trunking at the headquarters site while still allowing local calls via the branch sites.
PSTN	Public Switched Telephone Network. The PSTN is the international telephone system.
Rainy day	This term refers to a loss of network connectivity from the branch to the core data center.
SM Line	This term is used to describe a customized type of IP Office SIP trunk that is configured on the IP Office to connect to Avaya Aura® System Manager.
Stand-alone IP Office branch option	Independent IP Office systems are deployed within the network. These IP Office systems are not connected to each other or to anything else in the network. With this option, there is no Avaya Aura® system deployed in the network and users cannot access any Avaya Aura® services.
Sunny day	This term refers to full network connectivity from the branch to the core data center.
Survivability	This term describes centralized extensions when working after failover. The range of functions available to the phones in this state depend largely on

those configured for them on the branch system and will not match those available from the headquarters system during normal operation.

Survivable extension   This term is used to describe an extension which, though physically located at a branch site, receives its' telephony services from the central or headquarters site and operates in a Centralized enterprise branch. A survivable extension is also called a centralized extension.

Tail-End-Hop-Off   Part of mixed mode trunking, this describes scenarios where certain calls at other branches or the headquarters site are routed to the PSTN of another branch.

Index

S

T

U

V

W