Administering Centralized Users for an IP Office™ Platform Enterprise Branch

Release 11.1.1
Issue 7
February 2021

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

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

License type(s)

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

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

Cluster License (CL). End User may install and use each copy or an Instance of the Software only up to the number of Clusters as indicated on the order, Documentation, or as authorized by Avaya in writing with a default of one (1) Cluster if not stated.

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

Named User License (NU). End User may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. “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). End User 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”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

Transaction License (TR). End User may use the Software up to the number of Transactions as specified during a specified time period and as indicated in the order, Documentation, or as authorized by Avaya in writing. A “Transaction” means the unit by which Avaya, at its sole discretion, bases the pricing of its licensing and can be, without limitation, measured by the usage, access, interaction (between client/server or customer/organization), or operation of the Software within a specified time period (e.g. per hour, per day, per month). Some examples of Transactions include but are not limited to each greeting played/message waiting enabled, each personalized promotion (in any channel), each callback operation, each live agent or web chat session, each call routed or redirected (in any channel). End User may not exceed the number of Transactions without Avaya’s prior consent and payment of an additional fee.

Heritage Nortel Software

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

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

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

Contents

Part 1: Introduction ... 8
- **Chapter 1: Introduction** ... 9
  - Purpose ... 9
  - Document conventions ... 9
  - Change history ... 9
- **Chapter 2: IP Office as an enterprise branch overview** ... 11
  - Topology ... 11
  - New in this release ... 13
  - Branch deployment options ... 14
  - Supported telephones ... 15
  - Direct media setting on Avaya Aura® Communication Manager ... 15
- **Chapter 3: Centralized users** ... 17
  - Survivability operation ... 18
  - SIP controller monitoring ... 19
  - Failback policy ... 19
    - IP Office failback field descriptions ... 20
    - Configuring the global failback policy in System Manager ... 21
    - Configuring the failback policy in IP Office Manager ... 21
    - Starting a manual failback ... 22
  - ATA users ... 23
    - Communication Manager features ... 23

Part 2: Settings ... 27
- **Chapter 4: File server for settings and firmware files** ... 28
  - Enabling the DHCP server on the IP Office ... 28
  - About using external DHCP servers ... 29
  - Files and certificates required for the file server ... 29
    - Downloading the System Manager CA root certificate ... 29
  - Using a central file server for Centralized SIP phone files ... 30
  - Using System Manager File Transfer to load files to the IP Office system ... 30

Part 3: Supported Phones ... 32
- **Chapter 5: Supported phones in Centralized IP Office Branch deployments** ... 33
  - 9600 series SIP and Avaya H175 Video Collaboration Station endpoints deployed as Centralized users ... 33
    - Centralized 9600 series and Avaya H175 Video Collaboration Station settings ... 33
    - Parameters that must be configured for Centralized enterprise branch deployments ... 34
    - Additional parameters ... 37
    - Setting files and firmware for Centralized phones ... 38

SIP controller monitoring with Centralized 9600 series, J100 series SIP phones, and Avaya H175 Video Collaboration Station 45
1100 and 1200 series SIP phones deployed as Centralized users in IP Office Branch deployments 46
Configuring the 1100 and 1200 Series SIP phones in the Centralized branch model 47
Installing the 1100 Series SIP phone configuration files with the TFTP server 49
Sample configuration files for the 1100 and 1200 Series SIP phones 50
Ensuring consistent settings between the phones and IP Office for media security 54
B179 phones deployed as Centralized users in IP Office Branch deployments 56
Configuring B179 phone 56
Configuring B179 phone advanced settings 57
Adding Avaya Communicator for Windows as a Centralized user in the IP Office Branch environment 57
Files and certificates for Avaya Workplace Client for Windows 57
Setting up Avaya Workplace Client for Windows 59
Part 4: User administration 62
Chapter 6: User administration 63
Adding Centralized SIP users to System Manager 64
Adding ATA users to System Manager 68
Editing the IP Office Endpoint Profile for a user 71
Viewing Session Manager registered users 73
Part 5: Miscellaneous 74
Chapter 7: Resources 75
Documentation 75
Finding documents on the Avaya Support website 75
Training 75
Viewing Avaya Mentor videos 76
Additional IP Office resources 77
Support 77
Using the Avaya InSite Knowledge Base 78
Accessing Avaya DevConnect Application Notes 78
Appendix A: Communication Manager configuration example 79
Communication Manager configuration required for Centralized phone support 80
Verifying Communication Manager licenses 81
Configuring direct media on Communication Manager 81
Configuring trunk-to-trunk transfer 82
Configuring IP node names 82
Configuring IP codec set 82
Configuring IP network regions 82
SIP signaling group and trunk group 84
Configuring SIP signaling groups 84
Configuring SIP trunk groups 86

Configuring route patterns..... 87
Configuring private numbering..... 87
Configuring AAR..... 88
ARS Access Code..... 88
Location specific ARS digit analysis..... 89
Global ARS Digit Analysis..... 89
Appendix B: Deleting users from System Manager when IP Office is unreachable..... 90
Deleting data from System Manager database..... 91
Appendix C: Removing an IP Office from System Manager 92
Glossary..... 93

Part 1: Introduction

Chapter 1: Introduction

Purpose

This document describes how to administer endpoints as Centralized users in an IP Office Branch solution. Before using this document, ensure that you have configured IP Office in the branch environment. For more information, see *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

Document conventions

The following table shows the terminology used in the IP Office Branch documentation for Centralized users with SIP and analog extensions:

Table 1: Documentation terminology

Terminology used	Definition
Centralized SIP user	Centralized user in the IP Office Branch with a SIP extension.
ATA user	Centralized user in the IP Office Branch with an analog extension or an analog fax device.

Change history

The following table describes major changes made in this document for each release:

Issue	Date	Summary of changes
Release 10.0, Issue 1	July 2016	• Added support for Avaya Workplace Client for Windows and Avaya H175 Video Collaboration Station as Centralized users. • Moved Resources out of Introduction to an independent chapter called Resources. • Updated references to release numbers and to other documents.

Table continues…

Issue	Date	Summary of changes
Release 11.0	May 2018	• Added support for new phones: - Avaya J169/J179 Phones (standard SIP phones only)
Release 11.0 FP4	May 2019	Updated content for Avaya Aura® System Manager Release 8.1 changes.
Release 11.1 FP1	Jan 2021	• Added support for new phone: - Avaya J189 Phone (standard SIP phones only)

Chapter 2: IP Office as an enterprise branch overview

You can deploy 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. You can implement an IP Office enterprise branch 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.

In addition to centralized SIP endpoints or centralized analog devices configured as ATA, 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, an IP Office Branch can effectively deliver a range of communication tools without complex infrastructure and administration.

IP Office is also supported in an Avaya Communication Server 1000 (CS 1000) branch environment. Only the Distributed enterprise branch option is supported. IP Office can be deployed as a new branch in an existing CS 1000 configuration with the addition of Avaya Aura® Session Manager to which IP Office connects through the SM Line for branch connectivity. Providing phone investment protection, IP Office can also be deployed as a replacement for Business Communications Manager (BCM) or Norstar in a branch office and connect to CS 1000 through Avaya Aura® Session Manager. IP Office cannot operate as a survivable gateway to CS 1000 endpoints as similar to Survivable Remote Gateway (SRG).

Topology

The IP Office Branch solution provides the flexibility to support independent, stand-alone IP Office branches as well as IP Office branches connected to an Avaya Aura® system. The Branch solution also supports CS 1000 integration. The following deployment options are available for the solution architecture:

- **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, IP Office Branches are not connected to an Avaya Aura® system and users cannot access any Avaya Aura® services.

- **Distributed enterprise branch deployment option**: All users in this deployment option are IP Office users. These IP Office users obtain telephony services from the local IP Office and not from Avaya Aura®. The IP Office systems in this deployment option can be connected to Avaya Aura® Session Manager and administrators can obtain Centralized management services through Avaya Aura® System Manager. The enterprise can choose to connect IP Office users in this deployment option to an IP Office voice mail system, Embedded Voicemail or Voicemail Pro, or a Centralized voice mail system, such as Avaya Aura® Messaging or Avaya Modular Messaging. IP Office users in this deployment also have access to some Centralized Avaya Aura® applications and services.

  With the Distributed branch deployment option, you can also connect CS 1000 to IP Office in the branch through Avaya Aura® Session Manager. Users still obtain telephony services from the local IP Office, but can use Avaya CallPilot® as their voice mail system. When connected to CS 1000, IP Office and CS 1000 interoperate as peers through Avaya Aura® Session Manager.

- **Centralized enterprise branch deployment option**: All users in the enterprise are Centralized users.

  Centralized users register to Avaya Aura® Session Manager and obtain telephony services from the Avaya Aura® Communication Manager Feature Server or Evolution Server in the enterprise core. If WAN connectivity to Avaya Aura® Session Manager is lost, the user automatically gets basic telephony services from the local IP Office. The telephony features provided by IP Office in survivability mode is limited compared to the features that are normally provided to the Centralized phone.

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

- **Mixed enterprise branch deployment option**: An enterprise branch with both Centralized users and IP Office users. Centralized users and IP Office users obtain the same telephony services described above. All users in this deployment option must use a Centralized voice mail system: Avaya Aura® Messaging or Avaya Modular Messaging.

The deployment options in the Branch solution allow you to start off with stand-alone IP Office systems and then slowly evolve the solution architecture into a Centralized environment as your enterprise grows.

The following image shows the topology of the solution architecture with the deployment options described above. This image does not show CS 1000 in the Distributed branch deployment.

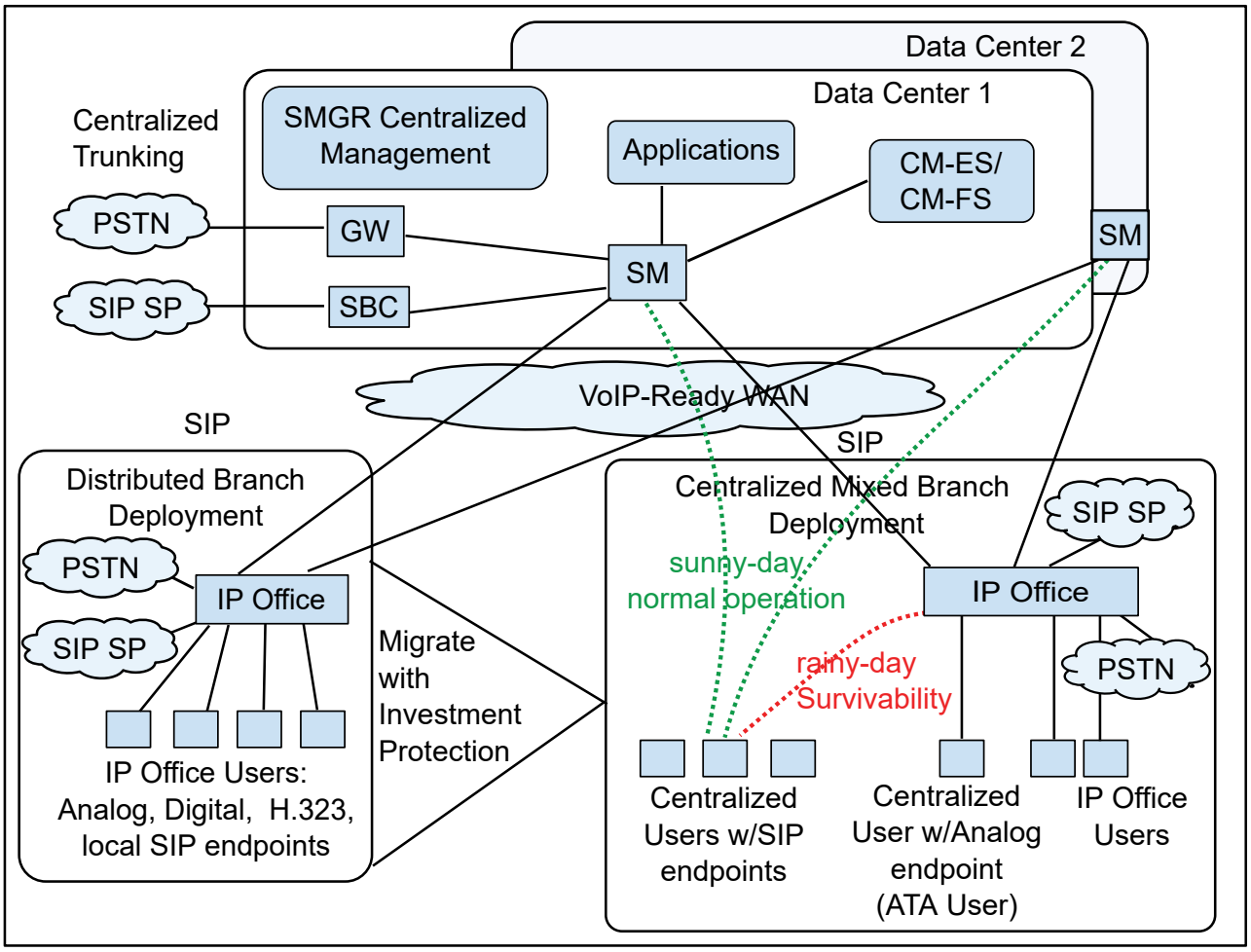

Figure 1: Topology of solution architecture

New in this release

IP Office Branch supports the deployment of the following as Centralized users:

- Avaya J129 IP Phone
- Avaya J139 IP Phone
- Avaya J159 IP Phone
- Avaya J169 IP Phone
- Avaya J179 IP Phone
- Avaya J189 IP Phone

Support for Avaya Aura® System Manager Release 8.1.

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. Existing IP Office systems can also 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 are 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 through the SM Line of IP Office system, that connects to Avaya Aura® Session Manager across the enterprise WAN. This connection allows 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.

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)
- B179 phone
- 11xx and 12xx series SIP 4.4 phones
- Avaya J100 Series IP Phones:
  - Avaya J129 IP Phone
  - Avaya J139 IP Phone
  - Avaya J159 IP Phone
  - Avaya J169/J179 IP Phone
  - Avaya J189 IP Phone

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*.

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 81.

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 IP Office in the branch. If WAN connectivity to 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 Avaya Aura® Session Manager, on Communication Manager, and on IP Office. On 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, 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.

Voice mail 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 voice mail

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 voice mail, see *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

Centralized phones can be provisioned from either a central HTTP server or from 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 is 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 IP Office Branch deployments on page 33.

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 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.

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.

IP Office failback field descriptions

Name	Description
Device Name	The name of the IP Office device with manual failback configuration.
IP Address	The IP address of the IP Office device with manual failback configuration.
System Type	The type of system associated with the IP Office device.
Last Operation on Device	The latest operation you performed on the IP Office device.
Status	The status of the operation that you performed last on the IP Office device.
System Configuration Template	The current IP Office System Configuration template that exists on the IP Office device.
Last Modified Time of System Configuration	The last time you modified the System Configuration template.
Last Backup Time	The last time you performed the backup operation for this system configuration.

Button	Description
Now	Click to initiate failback for the devices you have selected.
Schedule	Click to schedule failback for the devices you have selected.

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, in the **Elements** area, click **Session Manager**.
2. In the left navigation pane, click **Session Manager Administration**.
3. In the **Global Settings** area, in **Failback Policy**, click one of the following:
   - **Auto**: If you want the centralized SIP phones to failback automatically to normal operation when connectivity to Session Manager is restored. In addition, for networks that include two Session Manager servers for redundancy, failback from the secondary Session Manager to the primary Session Manager occurs automatically when the primary Session Manager is restored.
   - **Manual**: If you do not want the centralized SIP phones to failback automatically to normal operation when connectivity to Session Manager is restored. The failback to normal operation must be started manually when connectivity to Session Manager is restored.
4. Click **Save**.

Configuring the failback policy in IP Office Manager

Before you begin

Ensure that the failback policy configured in IP Office Manager matches with the global failback policy configured in Avaya Aura® System Manager.

Procedure

1. On the System Manager console, in the **Elements** area, click **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 system runs IP Office Manager.
5. In the left navigation pane, click **System**.
6. Click the **Telephony** tab.
7. Click the **SM** tab.
8. In **Failback Policy**, click one of the following:
   - **Auto**: If you want the centralized SIP phones to failback automatically to normal operation when connectivity to Session Manager is restored. In addition, for networks that include two Session Manager servers for redundancy, failback from the secondary Session Manager to the primary Session Manager occurs automatically when the primary Session Manager is restored.
   - **Manual**: If you do not want the centralized SIP phones to failback automatically to normal operation when connectivity to Session Manager is restored. The failback to normal operation must be started manually when connectivity to Session Manager is restored.
9. Click **OK**.
10. Click **File** > **Save Configuration**.

    The reboot mode is set to **Merge**.

Starting a manual failback

About this task

Use this procedure to start a manual failback for an IP Office after restoring the connection to Session Manager. When you perform this task, execute the manual failback once.

Procedure

1. On the System Manager console, in the **Elements** area, click **IP Office**.
2. In the left navigation pane, click **Initiate FailBack**.
3. On the IP Office Manual FailBack page, select an IP Office for which you want to start the failback.

   Note:

   The page displays only those IP Office systems whose failback policies are set to **Manual**.
4. Click **Now** or **Schedule**.
5. **(Optional)** If you 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 Session Manager and Communication Manager as SIP users, even though they use analog devices on the IP Office.

IP Office sends SIP registrations to Session Manager on behalf of each configured ATA user. IP Office includes its own IP address in the Contact header of the SIP registration. IP Office also sends the SIP registration on the SM Line using the same TCP or TLS connection on which it sends other traffic on the SM Line.

If two SM Lines are configured on IP Office connecting to two Session Managers, IP Office sends the ATA user registrations to both Session Managers. IP Office Release 10.0 fixes an issue with this interaction that was found in earlier releases.

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 use 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 use 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*.

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.
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.

Table continues…

Name	Description
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 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.

Table continues…

Name	Description
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.

Part 2: Settings

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 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 30. 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 33.

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 except for 9608, 9611, 9621, 9641, H.323, and 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 Office servers 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 Office in bulk.
- The System Manager file transfer feature does not support the transfer of nodal PLDS license files.

Procedure

1. On the System Manager console, in the **Elements** area, click **IP Office**.
2. In the left navigation pane, click **File Transfer**.

3. On the IP Office File Transfer page, in **Select File Type** , 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.
   - Additional information about audio file transfer is available in *Avaya Aura® System Manager Online Help*.

Part 3: Supported Phones

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 and Avaya H175 Video Collaboration Station endpoints deployed as Centralized users

IP Office Branch supports 9600 series phones and Avaya H175 Video Collaboration Station endpoints running SIP firmware as Centralized users.

Centralized 9600 series and Avaya H175 Video Collaboration Station 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 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.

- The IP Office in each branch for 9600 series SIP. This option is not available for the Avaya H175 Video Collaboration Station.

The default phone settings file is `46xxsettings.txt` . 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 might include the address of the primary Session Manager with which the SIP phones must register.

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, so it 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.

9600 series SIP phones also offer an alternative, which is not available with the Avaya H175 Video Collaboration Station. Instead of using Session Manager PPM to provision the parameters for each branch, you can provision these parameters in the settings file. This alternative requires a different settings file for each branch. This alternative 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 might 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 the following documents:

- For 9600 series SIP phones: *Avaya one-X™ Deskphone SIP 9608, 9611G, 9621G, 9641G Administrator Guide*.
- For the Avaya H175 Video Collaboration Station: *Administering Avaya H100-Series Video Collaboration Stations*.
- For the Avaya J100 Series phone:
  - Avaya IP Office™ J100 Series Telephone User Guide
  - Avaya IP Office™ Platform SIP Telephone Installation Notes

Parameters that must be configured for Centralized enterprise branch deployments

The following sections provide a list of parameters in the settings file that must be configured for Centralized enterprise branch deployments. These parameters require changing the default setting.

SIMULTANEOUS_REGISTRATIONS

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

When there is a single Session Manager, the 9600 series, J100 series SIP phones, and Avaya H175 Video Collaboration Station 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 perform 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, which is the number of Session Manager servers. Simultaneous registration is supported between Session Managers but not between a Session Manager and an IP Office.

SIP_CONTROLLER_LIST

This parameter must contain the IP address, port, and transport method (TLS or TCP) for the primary Session Manager that the phone uses.

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 uses. Each entry should contain the server IP address, port, and transport method (TLS or TCP). Multiple entries must be separated by a comma.

The list must contain the primary Session Manager as the first entry then the IP Office. If there is an additional Session Manager for redundancy, it must be included before the IP Office entry.

Note:

Using this alternative means that the settings file must 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. This option is not practical, however, if you are using a central file server with a common settings file for the phones in different branches.

Example:

The following string sets the primary SIP controller of the phone to the Session Manager and the secondary controller to an IP Office used in the basic configuration.

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

TRUSTCERTS

This parameter 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 might contain one or more certificate filenames, separated by commas without any intervening spaces. Files might contain only PEM-formatted certificates.

For 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. 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 29.

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 can obtain the certificate from System Manager and install it on the file server that is used by the phones. For more information, see Using the SIP Product CA root certificate on page 43.

TLSSRVRID

This parameter is used for TLS server identification. If the value is set to 1, then the TLS/SSL connection is only established if the server identity matches the server certificate. If the value is set to 0, then the connection is established. The recommended setting is `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.

SUBSCRIBE_LIST_NON_AVAYA

In IP Office survivable mode, to support Reset and Re-register from System Status and System Monitor, it should be set as `SET_SUBSCRIBE_LIST_NON_AVAYA "reg, avaya-ccs-profile"`.

MEDIAENCRYPTION

This parameter specifies SRTP media encryption options supported by the phone. You can select up to two options with all values in a comma-separated list. The options you select must match those specified in Communication Manager IP-codec-set form. The available 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 can only be set if local call forwarding is configured for the phone in Rainy day. The default setting is 0. The call forwarding mode is set by summing the following values:

- 1 = permits unconditional call forwarding
- 2 = permits call forwarding on busy
- 4 = permits call forwarding on no answer

Example of summing 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 must be set only if local call forward is going to be configured for the phone in Rainy day.

CALLFWDDELAY

This parameter sets the number of ring cycles before the call is forwarded to the forward or coverage address. This parameter 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

The following additional parameters are relevant to enterprise branch deployments.

DIALPLAN

In the survivability mode, when registered to IP Office, the phone cannot obtain dial plan information from the Session Manager. This DIALPLAN parameter can be used to set which numbers are dialed immediately when matched without waiting for a dialing timeout. Multiple entries can be used, separated by the **|** character. For example, on a typical IP Office system, you can use the following:

```
SET DIALPLAN [2]xx|[8]xxxxx|[6]xxxxxx|9Z1xxxxxxxxxx
```

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 parameter is used to determine whether the controller to which the phone is registered supports Advanced SIP Telephony (AST). IP Office systems do not support AST. However, since survivable phones connect in normal mode to Session Manager, you must use the default value of 1.

ENABLE_REMOVE_PSTN_ACCESS_PREFIX

This parameter 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, with the value 1, has no impact when the phone is communicating with an AST-capable controller. The default value is 0, which means that the prefix is not removed.

MSGNUM

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

PSTN_VM_NUM

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

RECOVERYREGISTERWAIT

This parameter defines 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% and 90% of the setting. The range is between 10 and 36000 seconds, with the default being 60 seconds.

ENABLE_PPM_SOURCED_SIPPROXYSRVR

This parameter enables PPM as a source of SIP Proxy server information. Keep the default value of 1 for this parameter. The default value 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 through PPM. When IP Office is used as file server, the value should be set to 0. The recommended setting is:

```
SET ENABLE_PPM_SOURCED_SIPPROXYSRVR 1
```

Setting files and firmware for Centralized phones

Most of the procedures in this section apply to 9600 series, J100 series SIP phones, and Avaya H175 Video Collaboration Station endpoints. Differences are clarified within the procedures.

Adding a NoUser Source Number to enable SIP firmware downloads for 9600 series SIP phones

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.

Note:

This procedure is not required for the Avaya H175 Video Collaboration Station.

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 for 9600 series, J100 series, and Avaya H175 Video Collaboration Station endpoints are provided in the SIP software distribution packages. These 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.

Files and certificates for 9600 and Avaya J100 Series IP Phonesseries phones

The 9600 series phones use the following SIP software distribution packages:

Phones	Software packages
9601/9608/9611G/9621G/9641G IP Deskphones	Avaya one-X® Deskphone SIP 7.1 Software
9600 IP Deskphones used for the 9620, 9630, 9640, and 9650 phones	Avaya one-X® Deskphone SIP 7.1 Software
Avaya J100 Series IP Phones (J129/J139/J159/J169/J179/J189)	J129, J139, J159, J169, J179- SIP 4.0.4.0 Software J189- SIP 4.0.7.0 Software

Phone conversion from H.323 to SIP

For information about converting the 9600 series phones from H.323 to SIP and editing the upgrade and settings files, see *Migrating an IP Office or B5800 Branch Gateway to an IP Office Enterprise Branch*.

Files and certificates for the Avaya H175 Video Collaboration Station

For information about downloading the setting files and firmware for the Avaya H175 Video Collaboration Station, see *Installing and Maintaining Avaya H100-Series Video Collaboration Stations*. The Avaya H175 Video Collaboration Station cannot be upgraded directly from IP Office because the firmware file size is 250 MB, which is not supported on the IP Office file system. The Avaya H175 Video Collaboration Station downloads only the latest version of the firmware from the FTP server.

Upgrade files

Upgrade files for 9600 series phones

The various combination of 9600 series phones, including SIP, and H.323, might 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 9608, 9611, 9621, and 9641 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.
- `96x1Hupgrade.txt` – The 9608, 9611, 9621, and 9641 H.323 phones require this file. This file is auto-generated by the IP Office and must not be changed.
- `96xxupgradeSIP.txt` – Except for 9608, 9611, 9621, and 9641, the 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.

  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 except for 9608, 9611, 9621, and 9641 SIP firmware package must be placed on the file server as is.

- `96xxupgrade.txt` – Except for 9608, 9611, 9621, and 9641, the H.323 phones require this file. This file is auto-generated by the IP Office and must 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 *Migrating an IP Office or B5800 Branch Gateway to an IP Office Enterprise Branch*.

Upgrade file for the Avaya H175 Video Collaboration Station

The Avaya H175 Video Collaboration Station requires the `H1xxSupgrade.txt` file. This file is included in the SIP software distribution package and specifies the firmware version and settings file to load.

Upgrade file for the J100 series phone

The J100 series phone requires the `J100Supgrade.txt` file. This file is included in the SIP software distribution package and specifies the firmware version and settings file to load.

Settings files

The 9600 series, J100 series for J129, J139, J159, J169/J179, J189 phones, and Avaya H175 Video Collaboration Station endpoints require the `46xxsettings.txt` file for Centralized users. This file is available on the Avaya Support website at https://support.avaya.com/.

Setting files for 9600 series phones

In Mixed enterprise branch deployments where there are both H.323 and SIP phones, a separate settings file is required for the 9600 series phones because SIP phones need different settings than H.323 phones. The `46xxsettings.txt` file is used for the H.323 phones and a new settings file, such as `96xxSIPsettings.txt`, can be used for the SIP phones. You must edit the upgrade files so each file specifies a particular 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. You can create this file 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 two versions of the `46xxsettings.txt` file. One version is auto-generated by IP Office 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. This file 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 SIP controller monitoring with Centralized 9600 series, J100 series SIP phones, and Avaya H175 Video Collaboration Station on page 45.

Settings file for J100 series phone

Mixed deployments will be supported with J139, J159, J169/J179, J189 phones.This means there will be support in the same branch for a J139, J159, J169/J179, J189 phone deployed as Centralized user and another J139, J159, J169/J179, J189 phone deployed as IP Office user.

When IP Officeis acting as the provisioning server

- Phones need to be configured with different groups using “GROUP” setting on the phone.
  - The GROUP parameter can be configured on the phone using this path: **Phone** > **Administrator** > **Group**.
  - Default value for GROUP parameter is 0.
  - Centralized users need to configure GROUP parameter in phone with values from 1 to 5 and Distributed (IP Office) users will be part of GROUP 0 by default.
- 46xxsettings file will have GET request for centralized settings file (`46xxBranchsettings.txt`) when `NUSN : BRANCH_PHONES_GROUP` is configured.
  - `BRANCH_PHONES_GROUP` can take values from 1 to 5, default being 0. For example — `BRANCH_PHONES_GROUP=1, BRANCH_PHONES_GROUP=2`
  - If `BRANCH_PHONES_GROUP` is configured with value other than 1 to 5, the setting will be reset to default value 0.
  - For the existing 9608,9611,9621, 9641 phones when `BRANCH_PHONES_GROUP` is configured (value between 1 to 5)
    - `96x1Hupgrade.txt` file would be auto-generated with a GET request to load the `96x1Supgrade.txt`
    - `96xxupgrade.txt` file would be auto-generated with a GET request to load the `96xxupgradeSIP.txt` file.
- 46xxBranchsettings file for Centralized J139, J159, J169/J179, J189 phone, like for other Centralized phones, is not auto-generated by IP Office and has to be edited manually with required parameters for branch deployment.
  - Manually edited `46xxBranchsettings` file should be uploaded on the IP Office System SD card in case of 500v2 deployments in the path: **File** > **Advanced** > **Embedded File Advancement** > **System SD** > **System** > **Primary**
  - Manually edited `46xxBranchsettings` file should be uploaded to disk in case of Server edition deployments in the path: **File** > **Advanced** > **Embedded File Advancement** > **System SD** > **System** > **Primary**

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. 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.

Using the SIP Product CA root certificate

About this task

Session Manager and other Avaya Aura® components use 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 Avaya endpoints.

From Session Manager, the demo certificates are not installed by default. For new Session Manager deployments, 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 this procedure to obtain the existing identity certificate from System Manager and install it on the file server that is used by phones.

Procedure

1. Type `https://<Session Manager IP Address>:5061` in your 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**, click **Export**.

   In this certificate:

   - CN is the SIP Product Certificate Authority.
   - OU is the SIP Product Certificate Authority.
   - O is the Avaya Inc.
   - C is the US.

Centralized phone reboots

The Centralized 9600 series 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 centralized 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, the download might fail on some of the phones.

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 **Advanced Search Criteria** to find the phones to be upgraded.

   Using the **Location** search criteria and specifying the branch location might 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, you can also choose 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:

   For best results of the firmware download process, select up to 10 users from the list to reboot together in one action.
5. Click **Reboot** next to **AST Devices Notification** above the list of users.

   Each of the selected phones are rebooted. After the reboot, the phone obtains the address of the local IP Office and its configuration files. Then the phone downloads firmware files from the IP Office. After the download is completed, the phone automatically restarts using the new firmware.
6. Confirm that the firmware upgraded correctly using one of the following methods:
   - Use the phone CRAFT menu by pressing **Mute** and entering `CRAFT#` or `27238#`.
   - Use the phone user menu by selecting **Home** > **Network Information** > **IP Parameters**
7. **(Optional)** 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

1. To power cycle the phone, remove power to the phone.
2. Wait for a minute, and then reapply power.

SIP controller monitoring with Centralized 9600 series, J100 series SIP phones, and Avaya H175 Video Collaboration Station

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 9608, 9611, 9621, and 9641 phones SIP phones do the following:

- 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 from the highest to the lowest priority.
- The phone waits for a response from each controller within a set time. That time is set by the CONTROLLER_SEARCH_INTERVAL parameter. The default value is 4 seconds.
- The controller is considered available if a `200 OK` response is received within the timer interval. When 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 the selected controller, the phone will continue monitoring the available controllers. It does this at regular intervals set by the REGISTERWAIT parameter. The default value is 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 parameter. The default value is 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. The legacy setting SIPREGPROXYPOLICY in the phone settings file has no effect. It is always overridden by Session Manager PPM and set to the simultaneous value.
- 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. When 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:
  - The phone does not receive a response to an INVITE sent to the active controller within a set time. The time is set by the FAST_RESPONSE_TIMEOUT parameter. The default value is 60 seconds.

- The phone receives a TCP keep-alive failure or another socket error.
- The phone prompted by an administrator.
- The phone receives an INVITE from a controller other than its active controller.

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*.

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*.
- *SIP Software for Avaya 1200 Series IP Deskphones–Administration*.

Factory settings:

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

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

About this task

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

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.

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 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`.

   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 50

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`	
`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`	

Table continues…

Text in the configuration file	Information specific to Session Manager and IP Office deployments

`[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.
`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

Table continues…

Text in the configuration file	Information specific to Session Manager and IP Office deployments
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	
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 this 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 cleared 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.

B179 phones deployed as Centralized users in IP Office Branch deployments

Configuring B179 phone

About this task

IP Office deployed as a Branch supports B179 R2.4 phones as Centralized users. The configuration of the Centralized B179 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 B179 phone does not support manual failback. Therefore, when a deployment includes a B179 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 B179 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 B179 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**.

Adding Avaya Communicator for Windows as a Centralized user in the IP Office Branch environment

Files and certificates for Avaya Workplace Client for Windows

Avaya Workplace Client for Windows must verify the identity certificate on Session Manager and IP Office to establish a TLS connection with Session Manager and IP Office.

To verify identity certificates, Avaya Workplace Client for Windows must trust the Certificate Authority (CA) identity certificates signed by the System Manager CA. You might need to install either one or two CA certificates with Avaya Workplace Client for Windows.

To maximize security, Session Manager can use an identity certificate signed by the same System Manager CA. Otherwise, Session Manager can use a demo identity certificate signed by the SIP Product CA.

Obtaining the System Manager CA root certificate

About this task

Use this procedure to download the System Manager CA root certificate for Avaya Workplace Client for Windows.

Procedure

1. On the System Manager web console, in the Services area, click **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. In the CA Functions area, click **Basic Functions**.
4. Click **Download pem file**, and save the file to a location on your computer.
5. Change the file extension name from `.pem` to `.crt`.

Obtaining the Session Manager CA certificate signed by a third-party CA

About this task

If Session Manager uses an identity certificate that is signed by a third-party CA, then you must download that root CA certificate. If Session Manager uses the demo identity certificate, then you must download the SIP Product CA certificate.

Procedure

1. On the System Manager web console, in the Services area, click **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Select a Session Manager instance from the **Elements** list.
4. In **More Actions**, select **Configure Trusted Certificates**.
5. On the Trusted Certificates screen, select an Avaya SIP Product CA certificate from the list.
6. To export the Security_Module_SIP certificate, click **Export**.
7. Ensure that the following fields are updated during the certificate creation:
   a. **CN** = SIP Product Certificate Authority.
   b. **OU** = SIP Product Certificate Authority.
   c. **O** = Avaya Inc.
   d. **C** = US.
8. Save the certificate to a location on your computer.
9. Change the file extension name from `.pem` to `.crt`.

10. Do one of the following:
    - Upload the System Manager CA certificate and the SIP Product CA certificate to a website and send the link to Avaya Workplace Client for Windows users.
    - Compress the CA certificate files and send through email as an attachment.

Installing the CA certificates

About this task

Use this procedure to install the CA certificates using the Windows Certificate Installation Wizard. Repeat this procedure for every certificate file.

Before you begin

Store the desired `.crt` files on your computer.

Procedure

1. Double-click the `.crt` file.
2. In the Certificate window, click **Install Certificate** > **Next**.
3. In the Certificate Import Wizard window, select **Place all certificates in the following store**.
4. To select the Certificate store, click **Browse**.
5. In the Select Certificate Store window, select the certificate store that you want to use, and then click **OK**.
6. Follow the instructions to complete the installation.

Setting up Avaya Workplace Client for Windows

Before you begin

- Configure IP Office as part of a Branch solution.
- Install Microsoft .NET Framework 4 on your computer.
- Store the `Avaya-Communicator-2.1.2.75.msi` file on your computer.
- Install all the relevant certificates for enabling PPM.
- Ensure that your system supports TLS and SRTP.

Procedure

1. Double-click the `Avaya-Communicator-2.1.2.75.msi` file, and follow the instructions to complete the installation.
2. Open Avaya Workplace Client for Windows.
3. In the Settings window, do the following:
    a. In **Server Address**, type the Primary Session Manager IP address.

b. In **Domain**, type your domain name.

The PPM message fetches all other controller lists.

4. Click **OK**.

User profile configuration on System Manager

When you deploy Avaya Workplace Client for Windows as a Centralized SIP user, you must configure a Session Manager Profile, a Communication Manager Endpoint Profile, and an IP Office Endpoint Profile on System Manager.

Configuring a voice mail number

About this task

You must configure the voice mail server number of Avaya Aura® Messaging or Modular Messaging in the Communication Manager Endpoint Profile. PPM messages share the configured voice mail numbers with Avaya Workplace Client for Windows. The same voice mail number is used by Avaya Workplace Client for Windows in the Sunny day and Rainy day mode.

When Centralized Avaya Workplace Client for Windows users call their provisioned voice mail number, for example, 70019019 in the Rainy day, IP Office sends the caller information to Avaya Aura® Messaging or Modular Messaging. Caller information is sent through DTMF digits over PSTN.

Voice mail number configuration for the Communication Manager Endpoint Profile is the same when:

- An existing Avaya Workplace Client for Windows client on Avaya Aura® is migrated to IP Office Branch.
- A new Avaya Workplace Client for Windows client is introduced into IP Office Branch.

Procedure

1. Log in to the System Manager console.
2. On the User Profile screen, click **Communication Manager Endpoint Profile**.
3. In **Voice Mail Number**, type `70019019`.

   The system configures the Avaya Modular Messaging pilot number as 70019019 and enables the voice mail number for Avaya Workplace Client for Windows.
4. On the System Manager console, select the IP Office device.
5. Click **Edit** to edit the system configuration for the device.

   IP Office Manager starts on your computer.
6. Add a new Short Code and configure the fields as follows:
   a. In **Code**, type `70019019`
   b. In **Feature**, select **Voicemail Collect**
   c. In **Telephone Number**, type `"?"U`

Next steps

Configure the IP Office voice mail to use Avaya Aura® Messaging or Modular Messaging. For more information about voice mail configuration, see *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

Part 4: User administration

Chapter 6: User administration

This section 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, an 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. 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 on page 64
Adding ATA users to System Manager on page 68
Editing the IP Office Endpoint Profile for a user on page 71
Viewing Session Manager registered users on page 73

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, in the **Users** area, 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 **Last Name**, enter the last name of user.

      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 first name of user.
   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. For more information, see the Deleting users from System Manager when IP Office is unreachable section.

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

User administration on page 63

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

User administration on page 63

Editing the IP Office Endpoint Profile for a user

About this task

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

Note:

If you are editing an existing B5800 Branch Gateway R6.2 user with the Avaya Aura® System Manager R6.3.2, ensure that the **Local Number Length** field is configured correctly in IP Office Manager. If it is not, you cannot modify the extension. An error message will appear indicating the extension length is invalid. For more information on how to configure the **Local Number Length** field in IP Office Manager, see *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 the **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 other parameters for this user, click the **Endpoint Editor** button.

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

    Note:

    IP Office Manager starts if the user profile is created on IP Office 9.0 and earlier. Otherwise, Web Manager starts as the editor for IP Office 9.1 and later.
11. Update the fields as appropriate.
12. Click **Save**.

    You return to the edit user window in System Manager.
13. Click **Commit**.

Related links

User administration on page 63

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 63

Part 5: Miscellaneous

Chapter 7: Resources

Documentation

For a complete list of IP Office documents, see *Avaya IP Office™ Platform Start Here First* at support.avaya.com.

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

Training

Avaya training and credentials are designed to ensure our Business Partners have the capabilities and skills to successfully sell, implement, and support Avaya solutions and exceed customer expectations. The following credentials are available:

- Avaya Certified Sales Specialist (APSS)
- Avaya Implementation Professional Specialist (AIPS)

- Avaya Certified Support Specialist (ACSS)

Credential maps are available on the Avaya Learning website at http://avaya-learning.com/.

The following courses are also available on the Avaya Learning website. After logging in to the website, enter the course code or the course title in the **Search** field.

Course code	Course title
2S00012W	APSS – Small and MidMarket Communications – IP Office™ Platform and Select Overview
4601W	Avaya IP Office™ Platform — Components
4602W	Avaya IP Office™ Platform — Editions
2S00015O	Small and Midmarket Communications — IP Office — Endpoints
10S00005E	Knowledge Access: Avaya IP Office™ Platform Implementation
5S00004E	Knowledge Access: Avaya IP Office™ Platform Support

Included in all Knowledge Collection Access offers above is a separate area called IP Office Supplemental Knowledge. This floor in the Virtual Campus contains self-directed learning objects, which cover IP Office delta information. This material can be consumed by technicians experienced in IP Office.

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.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.

- Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

Note:

Videos are not available for all products.

Additional IP Office resources

You can find information at the following additional resource websites.

Avaya

https://www.avaya.com is the official Avaya website. The front page also provides access to individual Avaya websites for different countries.

Avaya Sales & Partner Portal

https://sales.avaya.com is the official website for all Avaya Business Partners. The site requires registration for a user name and password. Once accessed, the portal can be customized for specific products and information types that you wish to see and be notified about by email.

Avaya IP Office Knowledge Base

https://ipofficekb.avaya.com provides access to an online, regularly updated version of the IP Office Knowledge Base.

Avaya maintenance, lifecycle and warranty information

Avaya support services complement standard Avaya maintenance, lifecycle and warranty policies that are posted on https://support.avaya.com. For more information, send email to support@avaya.com.

International Avaya User Group

https://www.iaug.org is the official discussion forum for Avaya product users.

Support

Go to the Avaya Support website at https://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.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Accessing Avaya DevConnect Application Notes

The Avaya DevConnect program conducts testing with service providers to establish compatibility with Avaya products.

Procedure

1. Go to http://www.devconnectprogram.com/site/global/compliance_testing/application_notes/index.gsp.
2. Sign in or register.
3. Click a timeframe to search within.

   A list of all the application notes for that timeframe appears.
4. In the **Search** field, type `IP Office` and press **Enter**.

   A list of relevant Application Notes appear.

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.

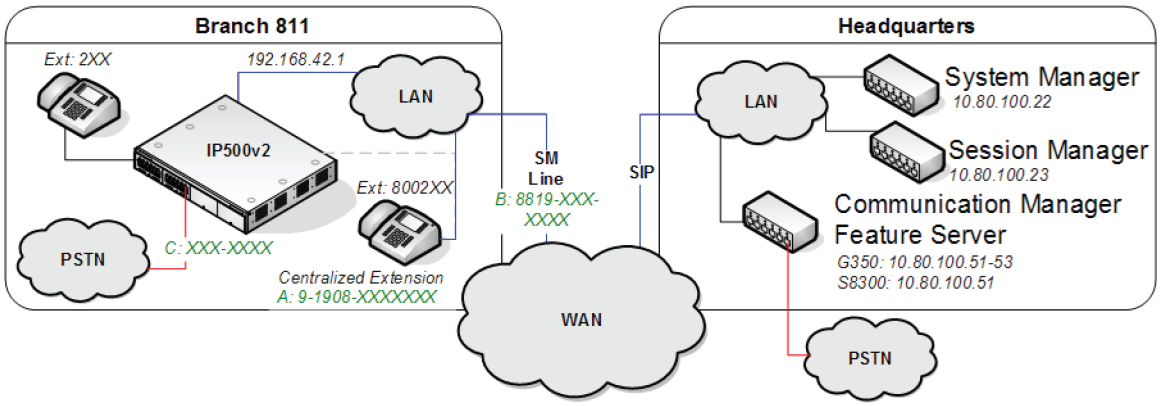

Figure 2: Communication Manager configuration example

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 required 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 79.

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. 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 or 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.

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. 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 Configuring SIP trunk groups on page 86.
   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 Configuring SIP trunk groups on page 86.

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 87 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 89.

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 89.

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 87.

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
```

Appendix B: Deleting users from System Manager when IP Office is unreachable

About this task

You can add, delete, or edit users with IP Office endpoint profile in System Manager only when the respective IP Office is reachable. This action in System Manager will update the data automatically and consistently in both System Manager and IP Office. If you cannot reach IP Office permanently and if System Manager has stale user records, then use the procedure below to force deletion of such users from the System Manager database.

Procedure

1. To edit IP Office from **opt** > **Avaya** > **ABG** > **6.3.8** > **tools** > **IP Office properties**, set **force_delete_user** to **true**.
2. Restart the Jboss server.
3. Delete IP Office profile from all users.
4. Using IP Office Manager open IP Office in unrestricted mode and reset the *BranchAdmin* password.
5. Perform the following checks:
   a. All users must be deleted.
   b. All soft extensions must be deleted.
   c. IP Office must have only digital and analog extensions as per the card installed in IP Office.
   d. The digital and analog extension that have default attributes must include the ID and extension.
6. If the analog and digital extensions are not displayed as in default configuration, then reboot IP Office.
7. In case the default configuration is not displayed in IP Office using the above steps 5 or 6, erase the IP Office configuration.
8. Delete the data from the System Manager database.

9. To edit IP Office from **opt** > **Avaya** > **ABG** > **6.3.8** > **tools** > **IP Office properties**, set **force_delete_user** to **false**.
10. Restart the Jboss server.
11. Change the IP Office password in the Inventory to *BranchAdmin* and run the IP Office system configuration and users synchronization.

Related links

Deleting data from System Manager database on page 91

Deleting data from System Manager database

Procedure

1. To log in to System Manager, use putty with the root login.
2. Type following commands:

   ```
   sudo -u postgres psql avmgmt
   ```

3. Execute following queries:

   a. `delete from abg_user_profile where istemplate = 'f' and rtsappsystemid in (select rtsappsystemid from abg_device where devicename = 'GE-SAND-IPO-1');` The device name is the name of the IP Office.

   b. `delete from abg_user_profile where istemplate = 'f' and rtsappsystemid in (select rtsappsystemid from abg_device where devicename = 'GE-SAND-IPO-2');`

   c. `update abg_extension_info set rtsappsysid = 0 where rtsappsysid in (select rtsappsystemid from abg_device where devicename = 'GE-SAND-IPO-1');`

   d. `update abg_extension_info set rtsappsysid = 0 where rtsappsysid in (select rtsappsystemid from abg_device where devicename = 'GE-SAND-IPO-2');`

Next steps

Reprovision all the Centralized SIP and ATA users with the IP Office profile.

Related links

Deleting users from System Manager when IP Office is unreachable on page 90

Appendix C: Removing an IP Office from System Manager

About this task

You can remove an IP Office system from System Manager only after all the users have been deleted from the IP Office system. When you remove a user from an IP Office system, all entity links and elements associated with the user are also deleted.

Procedure

1. Identify the IP Office you want to remove.
2. Log on to System Manager interface.
3. Navigate to **Users** > **User Management** > **Manage Users**.
4. Select the Users you want to delete and click **Delete**.
5. Select **More Actions** > **Show Deleted Users**.

   All the users you have deleted are displayed.
6. Select the Users and click **Delete**.

   The selected Users are deleted permanently from the IP Office system.
7. Select **Services** > **Inventory** > **Manage Elements**.
8. Select the IP Office system you want to remove.
9. Click **Delete**.

   The Delete IP Office screen lists the selected IP Office to be deleted.
10. Click **Delete**.

    The selected IP Office is removed from System Manager.

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 computer, 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

Numerics

1100 and 1200 phones
    centralized users 46
9600 series 33

A

adding a NoUser Source Number to enable SIP firmware download 39
Adding ATA users to System Manager 68
Adding centralized users to System Manager 64
additional parameters 37
Administering users
    ATA users 63
    Centralized SIP users 63
    IP Office users 63
application notes 78
ATA users 23
Avaya Communicator for Windows 57
Avaya H175 Video Collaboration Station 33
Avaya support website 77

B

B179 phone advanced settings 57
branch deployment options 14

C

CALLFWDADDR 37
CALLFWDDELAY 37
CALLFWDSTAT 37
CA root certificate 58
centralized IP Office branch 33
centralized users 17
certificates 42, 57
CM features
    ATA users 23
    communication manager features 23
configuration 60
Configuring
    1100 Series 47
    1200 Series 47
    Voice Mail Number 60
configuring B179 phone 56
configuring failback
    IP Office Manager 21

D

deleting data from system manager database 91
deleting users from system manager when IP Office is unreachable 90
DevConnect 78
DIALPLAN 37
direct media setting on Communication Manager 15
DISCOVER_AVAYA_ENVIRONMENT 38
document changes history 9
document conventions 9
downloading the System Manager CA root certificate 29

E

editing
    IP Office Endpoint 71
    user 71
ENABLE_PPM_SOURCED_SIPPROXYSRVR 38
ENABLE_REMOVE_PSTN_ACCESS_PREFIX 38
enabling the DHCP server on the IP Office 28
external DHCP servers 29

F

failback policy 19
files 57
files and certificates 39
    9600 series phones, J100 series phone 39
    Avaya H175 Video Collaboration Station 40
Files and certificates required for the file server 29
file server content
    examples 51
    samples 51
File server for settings and firmware 28
firmware
    Centralized phones 38

G

global failback policy
    System Manager 21

I

initiate failback
    IP Office 20
InSite Knowledge Base 78
installing 49
    CA certificates 59
IP Office failback field descriptions 20

L

loading files

loading files *(continued)*
IP Office system 30
System Manager File Transfer 30

M

mandatory 57
MEDIAENCRYPTION 36
MSGNUM 38

N

new in this release 13

O

obtaining 58
CA certificate 58
optional 57
overview
enterprise branch 11
IP Office 11

P

parameters 34
PSTN_VM_NUM 38

R

rebooting the phones by power cycling the phones 44
rebooting the phones from System Manager 43
reboots
Centralized 9600 phone 43
RECOVERYREGISTERWAIT 38
related documentation 75
remove IP Office from System Manager 92
resource websites 77

S

Sample configuration files
1100 and 1200 Series SIP telephones 50
Session Manager 58
Setting files
Centralized phones 38
settings
9600 series 33
Avaya H175 Video Collaboration Station 33
settings file
J100 series phone 41
settings files
9600 series phones 41
Settings files 41
setting up
Avaya Communicator for Windows 59
SIMULTANEOUS_REGISTRATIONS 34
SIP_CONTROLLER_LIST 35
SIP controller monitoring 19
Centralized 9600 series phones 45
SIPDOMAIN 35
starting
manual failback 22
SUBSCRIBE_LIST_NON_AVAYA 36
support 77
supported telephones 15
survivability operation 18
System Manager 58

T

third-party CA 58
TLSSRVRID 36
topology 11
training 75
TRUSTCERTS 36

U

upgrade file
Avaya H175 Video Collaboration Station 41
J100 series phone 41
upgrade files
9600 series phones 40
user profile configuration
System Manager 60
using
SIP Product CA root certificate 43
Using a central file server for SIP phone files 30

V

videos 76
Viewing Session Manager registered users 73