Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager

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

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose

This document provides installation, configuration, initial administration, and basic maintenance checklists and procedures for deploying IP Office 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 information on Geographic Redundancy. • Added information about HTTP and HTTPS protocol configuration. • Windows XP references have been removed. Windows XP is no longer supported. • Moved Resources out of Introduction to an independent chapter called Resources. • Updated references to release numbers and to other documents. • Updated the Adding IP Office to System Manager section and explained the impact of IP Office security settings.
Release 10.1, Issue 1	May 2017	• Additional System Manager information has been added.
Release 11.0, Issue 2	June 2019	Updated the document for System Manager Release 8.1 changes.
Release 11.1	March 2020	Updated the procedures for System template, System configuration and Security configuration supporting different browsers and IP Office versions.
Release 11.1.FP1	January 2021	Added new phone Avaya J189 IP Phone.

Related links

Geographic Redundancy configuration on page 180

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.

For more information on how to add Centralized users to an IP Office enterprise branch, see *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*

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).

Integration of IP Office with CS 1000 is provided in a separate document. See *Deploying Avaya IP Office™ as a Distributed Enterprise Branch in a Communication Server 1000 Environment with Avaya Aura® Session Manager*.

Related links

New in this release on page 13
Topology on page 13
Components on page 17

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.

Related links

IP Office as an enterprise branch overview on page 12

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.

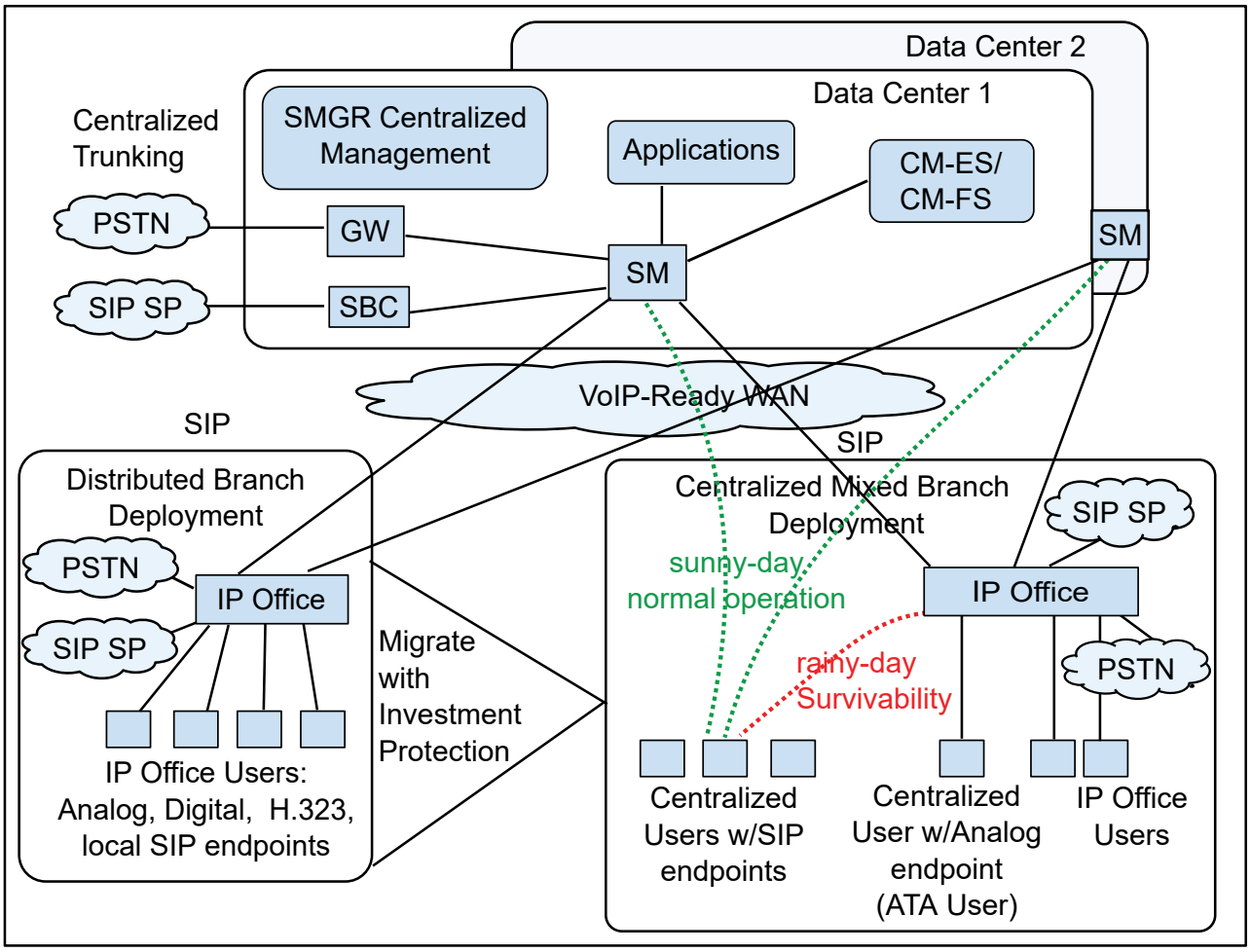


Figure 1: Topology of solution architecture

Related links

IP Office as an enterprise branch overview on page 12
Centralized management on page 15

Centralized management

The primary method for configuring and managing the branches in an IP Office system that is deployed with one of the branch deployment options, is centrally using Avaya Aura® System Manager. Avaya Aura® System Manager is a central management system that delivers a set of shared management services and a common console for different components of the Avaya Aura® solution. System Manager provides a single access interface to administer multiple branch locations and multiple IP Office users and Centralized users. System Manager also starts IP Office Manager in the appropriate mode where you can remotely administer individual IP Office systems.

As an alternative to System Manager, you can use IP Office Manager that is directly connected to the IP Office to configure a branch locally when you need to administer an isolated branch or System Manager is not available. Using IP Office Manager, you are also able to add and manage

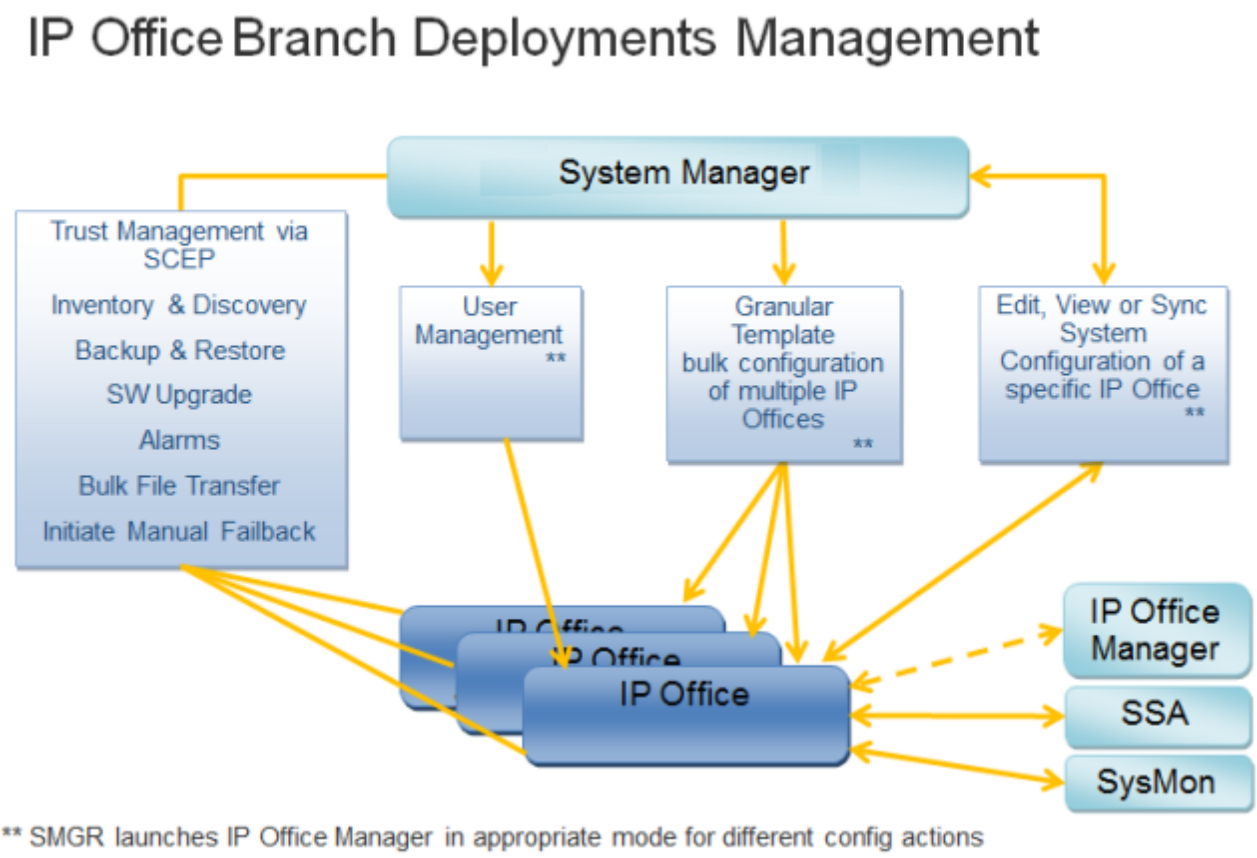
users in the branch. IP Office Manager is an application for viewing and editing an IP Office system's configuration. It is included in the IP Office administration software suite. IP Office Manager is an off-line editor. It receives a copy of the system's current configuration settings. After changes are made to that copy and the file is saved, IP Office Manager automatically sends the file back to the system for those changes to become active.

Most of the tasks in this document to configure and manage the IP Office system are provided using Avaya Aura® System Manager. You are able to perform IP Office configuration directly from IP Office Manager as well. You can manage Voicemail Pro, UCM and Application Server using Avaya Aura® System Manager.

Avaya Aura® System Manager

Using Avaya Aura® System Manager, you are able to:

- Upgrade IP Office systems.
- Add IP Office devices from the network to System Manager.
- Create IP Office endpoint templates that are used to create IP Office users and Centralized users. These templates can be edited, duplicated, or deleted.
- Create IP Office system configuration templates that can be applied to selected IP Office systems. These templates are used for initial device provisioning. These templates can be edited, duplicated, or deleted.
- Upload and convert audio files to System Manager to be used in the IP Office System Configuration Auto Attendant feature.
- Manage IP Office system configurations. From System Manager, you are able to start IP Office Manager to view or edit a system configuration. With this feature, you make changes directly to the IP Office device. You are able to apply the changes immediately or schedule the changes to run at a specified time.
- Manage IP Office security configuration. From System Manager, you are able to start IP Office Manager to view or edit a system security configuration. With this feature, you make changes directly to the IP Office device.
- Create user templates. These templates can be edited or deleted. Templates can be created for Centralized users or IP Office users.
- Perform an IP Office backup with the option of storing the backup output in System Manager or creating a local backup where the system stores the backup output on the local storage attached to the IP Office device.
- Perform an IP Office restore. This feature allows you to restore:
  - a saved IP Office system configuration onto an IP Office from System Manager.
  - a backup of an IP Office system configuration onto an IP Office from the device SD card.
  - users from System Manager to the IP Office.
  - a saved IP Office system configuration and user from System Manager onto an IP Office.
- View events and alarms regarding various operations that occur on the IP Office.



Note: SCEP is Simple Certificate Enrollment Protocol

Related links

Topology on page 13

Components

The IP Office system deployed as an enterprise branch is comprised of the following hardware components.

- **IP500v2 control unit** — The IP500v2 control unit stores the system configuration and performs the routing and switching for telephone calls and data traffic. It includes 4 slots for optional base cards to support trunk and phone extension ports. The slots are numbered 1 to 4 from left to right. They can be used in any order; however, if the capacity for a particular type of card is exceeded, the card in the right-most slot will be disabled.

  Note:

  IP Office in an enterprise branch deployment is supported only on the IP500v2 control unit.

- **System SD card** — The System SD card is a uniquely numbered dongle and has a serial number that must be used as the Host ID in the PLDS license file if the IP Office is operating with an individual license file and not with WebLM licensing. The System SD card also provides Embedded Voicemail support and storage for system software files. The card fits into a slot in the rear of the control unit.
- UCM and Application Server platforms.
- **Base cards** — The control unit has slots for up to 4 base cards. The base cards are used to add analog extension ports, digital extension ports, and voice compression channels. Each base card includes an integral front panel with ports for cable connections. The following base cards are supported:
  - **Digital station base card** — This card provides 8 digital station (DS) ports for the connection of Avaya digital phones other than IP phones. The card can be fitted with a trunk daughter card which uses the base card ports for trunk connection. A maximum of 3 digital station base cards are allowed per control unit.
  - **Analog phone base card** — This card is available in two variants, supporting either 2 or 8 analog phone ports. The card can be fitted with a trunk daughter card which uses the base card ports for trunk connection. A maximum of 4 analog phone base cards are allowed per control unit. The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors. If fitted with an analog trunk daughter card, during power failure phone port 8 is connected to analog trunk port 12.
  - **VCM base card** — This card is available in variants supporting either 32 or 64 Voice Compression Channels (VCM) for use with VoIP calls. A maximum of 2 VCM base cards are allowed per control unit. The card can be fitted with a trunk daughter card which uses the base card ports for trunk connection.
  - **4–port expansion base card** — This card adds an additional 4 expansion ports for external expansion modules. The card is supplied with four 2m yellow interconnect cables. This card does not accept any trunk daughter cards. A maximum of 1 4–port expansion base card is allowed per control unit (right-hand slot 4 only).
  - **BRI combination card** — This card provides 6 digital station ports (1-6), 2 analog extension ports (7-8) and 2 BRI trunk ports (9-10, 4 channels). The card also includes 10 VCM channels. This card has a pre-installed BRI trunk daughter card. A maximum of 2 BRI combination cards of any type are allowed per control unit.
  - **ATM combination card** — This card provides 6 digital station ports (1-6), 2 analog extension ports (7-8) and 4 analog trunk ports (9-12). The card also includes 10 VCM channels. This card has a pre-installed analog trunk daughter card. A maximum of 2 ATM combination cards of any type are allowed per control unit. The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors. If fitted with an analog trunk daughter card, during power failure phone port 8 is connected to analog trunk port 12.
  - **TCM 8 card** — This card provides 8 digital station ports (1-8).

- **Trunk daughter cards** — Most base cards can be fitted with a trunk daughter card to support the connection of trunks to the base card. The following trunk daughter cards are supported:
  - **Analog trunk card** — This card allows the base card to support 4 analog loop-start trunks. The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors. If fitted with an analog trunk daughter card, during power failure phone port 8 is connected to analog trunk port 12. A maximum of 4 analog trunk cards are allowed per control unit.
  - **BRI trunk card** — This card allows the base card to support up to 4 BRI trunk connections, each trunk providing 2B+D digital channels. The card is available in 2 port (4 channels) and 4 port (8 channels) variants. A maximum of 4 BRI trunk cards are allowed per control unit. For S-Bus connection, the card can be switched from To trunk mode to So mode. This mode requires additional terminating resistors and an ISDN crossover cable connection.
  - **PRI trunk card** — This card allows the base card to support up to 2 PRI trunk connections. The card is available in single and dual port variants. The card can be configured for E1 PRI, T1 robbed bit, T1 PRI or E1R2 PRI trunks. A maximum of 4 PRI trunk cards are allowed per control unit. The IP Office system supports 8 unlicensed B-channels on each IP500 PRI-U port fitted. Additional B-channels, up to the capacity of ports installed and PRI mode selected require Universal PRI (Additional Channels) licenses added to the configuration. These additional channels consume the licenses based on which additional channels are configured as in-service from port 9 of slot 1 upwards. D-channels are not affected by licensing.
- **Combination cards** — Combination cards are pre-paired base and trunk daughter cards. They provide 6 digital station ports, 2 analog phone ports, 10 VCM channels and either 4 analog trunk ports or 4 BRI channels (2 ports). The trunk daughter card cannot be removed or replaced with another type of trunk daughter card.
- **External expansion modules** — External expansion modules are used to add additional analog and digital ports. If the control unit is fitted with a 4–port expansion base card, then up to 12 external expansion modules are supported. The following external expansion modules are supported:
  - **Analog trunk module** — This module rovides an additional 16 analog ports for connection of analog trunks. It supports both loop-start and ground-start trunks.
  - **BRI So8 module** — This module provides 8 ETSI BRI-So ports for the connection of ISDN devices. This module is not intended to support BRI trunks.
  - **Digital station module** — This module provides, depending on variant, an additional 16 or 30 DS ports for supported Avaya digital phones.
  - **Phone module** — This module provides, depending on variant, an additional 16 or 30 phone ports for analog phones.
- **Power supplies** — The control unit has an internal power supply unit. Each external expansion module is supplied with an external power supply unit. Additional power supply units may also be required for IP phones and some phone add-ons.

- **Power cords** — Depending on the locale, different power cords need to be ordered for each control unit, external expansion module, and any phones or devices using external power supply units.
- **Mounting kits** — The control unit can be used free-standing, with external expansion modules stacked above it. With optional rack mounting kits, the control unit and external expansion modules can also be rack mounted. Alternatively, with an optional wall mounting kit the control unit can be wall mounted. However, the control unit cannot support any external expansion modules when wall mounted.
- **Surge protectors and barrier boxes** — Where the installation includes extensions in other buildings, additional protective equipment is required. This equipment may also be required in areas where the lightning risk is high.
- **Phones** — IP Office systems support a variety of Avaya digital and IP phones plus analog phones.
- **Application DVDs** — The IP Office applications can be ordered on a number of DVDs. In addition they can be downloaded from the IP Office section of the Avaya support web site (http://support.avaya.com). TheIP Office administration software applications are provided on the application DVDs.

For more information about the system components, see *Deploying Avaya IP Office™ Platform IP500/IP500 V2*.

Related links

IP Office as an enterprise branch overview on page 12
Supported telephones on page 20
IP Office branch interoperability on page 22

Supported telephones

IP Office deployed in an Avaya Aura® branch environment supports all IP Office phones. IP Office phones are used by IP Office users. These users were earlier referred to as Distributed, Local, or Native users. For more information about IP Office phones, see *Deploying Avaya IP Office™ Platform IP500/IP500 V2*.

In addition to the IP Office phones, the following Centralized phones are supported in branches deployed as Centralized or Mixed enterprise branches:

- 9620 SIP
- 9630 SIP
- 9640 SIP
- 9650 SIP
- 9601 SIP
- 9608 SIP

- 9611G SIP
- 9621G SIP
- 9641G SIP
- 1120E
- 1140E
- 1220
- 1230
- Avaya B179
- Avaya J159 IP Phone
- Avaya J169 IP Phone
- Avaya J179 IP Phone
- Avaya J129 IP Phone
- Avaya J139 IP Phone
- Avaya J189 IP Phone
- Avaya Workplace Client for Windows

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.

The following endpoints are supported as IP Office or Centralized users:

- Avaya H175 Video Collaboration Station
- The 1100 and 1200 series phones
- B179 series phones
- J100 series for J129, J139, J159, J169/179, J189 phones (Supported only as Standard SIP phone)

For information about centralized phones and adding Centralized users to an enterprise branch, see *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*.

Video endpoints in an IP Office branch can be connected over the WAN to the central Avaya Aura® infrastructure where they are used by Avaya Aura® users. In this deployment, the endpoint are physically located in a branch where Centralized users use Centralized phones. However, the endpoints are not considered as Centralized endpoints because they do not failover to IP Office in the Rainy day like Centralized phones.

For more information about Radvision video endpoints in an enterprise branch deployment, see *Avaya IP Office™ Platform in a Branch Environment Reference Configuration*.

For information about installing Radvision video endpoints in an enterprise branch deployment, see *Avaya Aura® Communication Manager and Avaya Scopia® Interoperability Day 90 Solution Quick Setup*.

Related links

Components on page 17

IP Office branch interoperability

The IP Office in the branch can interoperate with other applications and services. For more information about IP Office branch interoperability, see https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml?name=IP+Office+Platform.

Centralized SIP users in the branch connect directly to Avaya Aura® Session Manager in sunny-day and have full access to all central applications and services that the Avaya Aura® solution provides to SIP users. IP Office users in the branch cannot access all the features provided through the Avaya Aura® solution. Users in a stand-alone IP Office branch deployment do not have access to any of the centralized applications and services.

Differences in service for IP Office users and Centralized users

IP Office users and Centralized users cannot access all of the services offered through the products listed above. The following table describes the services available to the different users.

Products	Description
Avaya Aura® Session Manager	Used by Centralized users and IP Office users, but plays an enhanced role for Centralized users. For Centralized users, Session Manager is the main interface that handles user registration and call routing.
Avaya Aura® Conferencing	Avaya Aura® Conferencing services can be accessed by IP Office users and Centralized users, but certain services are not available to IP Office users. IP Office users can dial in to an Avaya Aura® Conferencing bridge and be participants in an Avaya Aura® ad-hoc conference. However, IP Office users cannot start ad-hoc Avaya Aura® conferences or perform conference control functions.
Avaya Aura® Call Center Elite	IP Office users cannot have agent roles. Only Centralized users can perform agent roles within the branch. In the Sunny day, the Centralized user is registered to Session Manager and has full agent access. In the Rainy day, the Centralized user in the branch is unavailable and no longer accessible to the Avaya Call Center. The Centralized user's phone registers to the IP Office in the Rainy day and obtains access to the survivable telephony features supported by IP Office. When the Sunny day returns, the Centralized user will reregister to Session Manager and again be available to the Avaya Call Center.

Table continues…

Products	Description
Avaya Aura® Presence Services	Centralized users can use Avaya Aura® Presence Services. IP Office users cannot use Avaya Aura® Presence Services. IP Office can only use IP Office Presence, which requires Avaya one-X® Portal to be deployed in each branch on Unified Communications Module or on an external server. No interaction is currently supported between IP Office and Avaya Aura® Presence Services.
Avaya Aura® Messaging	When the connection to the Avaya Aura® network is down, the **Message Waiting Indicator** button does not light up to indicate a new message. When the connection to the Avaya Aura® network is restored, the **Message Waiting Indicator** continues working as expected for Centralized users. However, for IP Office users, the Avaya Aura® Messaging server does not refresh immediately even after the connection to the Avaya Aura® network is restored, the **Message Waiting Indicator** does not light up immediately to indicate a new message.
Lync Integration client plug-in	The IP Office Lync Integration client plug-in is available to IP Office users. It requires Avaya one-X® Portal to be installed in each branch on a Unified Communications Module or an external server. The IP Office Lync Integration client plug-in cannot be used by Centralized users. Centralized users in the Sunny day can use Lync Integration, which supports integration with the Avaya SIP phones using Session Manager. This sunny-day support does not involve IP Office. In the Rainy day, when the branch loses connection to the center, the Lync integration of the Centralized users through ACA will not be available.
CS 1000 and Avaya CallPilot®	Only available in a distributed branch deployment connected to CS 1000. With this option, IP Office users can use Avaya CallPilot® as their voice mail system.
Radvision Scopia	Radvision Endpoints are video endpoints for IP Office. Using this option, IP Office devices can join or dail out from a meeting. NAT Firewall traversal is offered to enable outside to/from inside video calls. This enables Internet based endpoints to make calls to video endpoints or meeting rooms in a company network. The Elite MCU series supported with IP Office are Elite 5100 MCU Series and Elite 5200 MCU Series.

Table continues…

Products	Description
Avaya Session Border Controller	This is applicable to Distributed, Mixed, and Centralized branch deployments and includes the following types of calls: • Local SIP trunk - Session Border Controller - IP Office - IP Office user • Local SIP trunk - Session Border Controller - IP Office - Session Manager - Centralized users (in sunny-day) • Local SIP trunk - Session Border Controller - IP Office - Centralized users (in rainy-day) • Local SIP trunk - Session Border Controller - IP Office - Session Manager - users in headquarters or other enterprise sites • Central SIP trunk - Session Border Controller - Session Manager - IP Office - IP Office user • Central SIP trunk - Session Border Controller - Session Manager - Centralized users • IP Office remote worker - Session Border Controller - IP Office - Session Manager - users in headquarters or in other enterprise sites • IP Office remote worker - Session Border Controller - IP Office - Session Manager - Centralized users in a Mixed branch (in sunny-day) • IP Office remote worker - Session Border Controller - IP Office - Centralized users in a Mixed branch (in rainy-day) • IP Office remote worker - Session Border Controller - IP Office - Session Manager - voice mail services on Avaya Aura® Messaging/ Modular Messaging. • Avaya Aura® remote worker - Session Border Controller - Session Manager - IP Office - IP Office user
Avaya BCM	Positions IP Office as a SIP gateway between BCM and Session Manager.
Avaya Experience Portal	IP Office supports basic interoperability with Avaya Experience Portal for SIP calls sent through the Avaya Aura® Session Manager.
Voice Portal	Provides only basic connectivity support with IP Office.
Avaya Aura® Communication Manager	IP Office supports interoperability with Avaya Aura® Communication Manager for SIP calls sent through the Avaya Aura® Session Manager. In addition, Centralized users use the Communication Manager as their telephony server that provides their features and handles all their calls in Sunny day.

Related links

Components on page 17

Chapter 3: Deployment process

Following are the high-level tasks required to deploy an IP Office system as an enterprise branch connected to Avaya Aura® Session Manager.

No.	Task	See
1	Install the IP Office system hardware and software.	*Deploying Avaya IP Office™ Platform IP500/ IP500 V2*
2	Perform planning tasks for the Branch environment.	Planning on page 27
3	Perform initial configuration tasks, such as: • Set up System Manager to start IP Office Manager • Install the shared PLDS license file on the System Manager WebLM server • Generate a certificate on System Manager • Run the Initial Configuration Utility • Configure the SCEP and security settings for the IP Office system • Add the IP Office systems to System Manager • Administer an SM Line for each branch	Initial setup and connectivity on page 35
4	Configure Session Manager to support calls to and from the IP Office systems.	Avaya Aura Session Manager Configuration on page 172
5	Configure the voicemail system that the IP Office system will use.	Voicemail configuration on page 128
6	Add IP Office users to System Manager. **Note:** After you complete this step, you have deployed a Distributed enterprise branch.	User administration on page 190

Table continues…

No.	Task	See
7	Add Centralized users to System Manager. **Note:** When you add Centralized users to System Manager, you are deploying a Mixed or Centralized enterprise branch. A Mixed enterprise branch has both IP Office users and Centralized users located in the same branch. A Centralized enterprise branch has only Centralized users located in the branch.	See “Adding Centralized users” in *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*
8	Optionally, add a standalone SAL gateway for remote service.	Optional standalone Secure Access Link Gateway configuration for remote service on page 185
9	Deploy IP Office as a Distributed enterprise branch in a Communication Server 1000 (CS 1000) environment. **Note:** For CS 1000 environments, further configuration is required in addition to tasks 1 – 5 listed above. Task 6 above does not apply to this configuration because Centralized users are not supported in IP Office and CS 1000 deployments.	See “CS 1000 and IP Office Distributed deployment” in *Deploying IP Office as a Distributed Enterprise Branch in a Communication Server 1000 Environment with Avaya Aura Session Manager*

Chapter 4: Planning

Before you begin the configuration required to deploy the IP Office system as an enterprise branch, you should already have determined the deployment issues listed in the table below.

#	Task	Description	Notes	✔
1	List the dial plan options.	Consider the dial plan you are configuring for the system and each branch.	IP Office supports dial plans comprising of branch prefix and local number length.	
2	Download the licenses required for the installation.	The licenses required for the installation.	A WebLM license is required by each IP Office branch in order to use the WebLM server licensing model.	
3	Select the Branch PSTN call route.	Consider the route for outgoing PSTN calls.		
4	Select the voicemail solution that you are going to deploy.	The supported voicemail solutions are: • Embedded Voicemail • Voicemail Pro • Avaya Aura® Messaging • Modular Messaging		
5	Select the network for VoIP	Use this option to route voice traffic across internal and external data links.		

Related links

Prerequisites on page 28

Network assessment for VoIP requirements on page 28

Planning considerations on page 29

Prerequisites

Depending upon the deployment, the following applications and servers must be installed and configured before the IP Office is installed.

- If you are going to connect the IP Office to an enterprise over the WAN, Avaya Aura® Session Manager must be installed and configured at the headquarters location.
- If you are going to centrally manage the IP Office systems, Avaya Aura® System Manager must be installed and configured at the headquarters location.
- If you are going to use centralized licensing by WebLM, an Avaya Aura® System Manager WebLM server or a standalone WebLM server must be installed and configured. The WebLM server can be located at the headquarters location or anywhere in the network as long as the IP Office systems can access it on the network.
- If you are going to deploy IP Office systems with the Centralized enterprise branch deployment option, Avaya Aura® Communication Manager Feature Server or Avaya Aura® Communication Manager Evolution Server must be installed and configured as a feature server or evolution server at the headquarters location.

  Important:

  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” in *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*.
- To report alarms and receive remote support, a stand-alone Secure Access Link (SAL) Gateway, R2.0 or later must be deployed.

  Note:

  System Platform's virtual SAL gateway is not supported.

Related links

Planning on page 27

Network assessment for VoIP requirements

IP Office is a converged telephony system, that is, it combines aspects of traditional PABX telephone systems and IP data and telephony systems. This works at various levels.

- Individual phone users can control the operation of their phone through applications running on their computer.

- Data traffic can be routed from the LAN interface to a telephony trunk interface, for example a dial-up ISP connection.
- Voice traffic can be routed across internal and external data links. This option is referred to as voice over IP (VoIP).

The VoIP mode of operation can include IP trunks between customer systems and/or SIP telephones for users. In either case, you must consider the following factor:

- A network assessment is a mandatory requirement for all systems using VoIP. For support issues with VoIP, Avaya may request access to the network assessment results and may refuse support if those are not available or satisfactory.

A network assessment includes a determination of the following:

- A network audit to review existing equipment and evaluate its capabilities, including its ability to meet both current and planned voice and data needs.
- A determination of network objectives, including the dominant traffic type, choice of technologies, and setting voice quality objectives.
- The assessment should leave you confident that the implemented network will have the capacity for the foreseen data and voice traffic, and can support SIP, DHCP, TFTP and jitter buffers in SIP applications.
- An outline of the expected network assessment targets is:

Test	Minimum Assessment Target
Latency	Less than 150ms
Packet Loss	Less than 3%
Duration	Monitor statistics once every minute for a full week

Related links

Planning on page 27

Planning considerations

The following sections describe considerations and decisions you must make before deploying IP Office™ Platform as an Enterprise Branch.

Related links

Planning on page 27
Dial plan considerations on page 30
Voicemail considerations on page 33
Branch PSTN call routing considerations on page 34

Dial plan considerations

A uniform dial plan greatly simplifies configuration, management and phone calls within the network branch sites. For example, if each branch has similar roles such as reception, manager and warehouse, using the same extension number for each role and a unique prefix for each branch allows calls between sites with little need for directory lookups. It also means a standard configuration can be used at branches which simplifies installation, user training and maintenance.

IP Office supports dial plans comprised of the branch prefix and local number length for IP Office users and enterprise-wide extensions for Centralized users.

Branch prefix and local number length for IP Office users

Dial plans comprised of the branch prefix and local number length for IP Office users should not exceed 15 digits. The **Branch Prefix** field and the **Local Number Length** field appear in IP Office Manager under **System** > **Telephony** > **SM** tab.

The branch prefix enables IP Office users to have short extension numbers within the local branch but appear to the rest of the enterprise to have unique full enterprise-wide numbers in enterprise canonical format. If a number is configured in the **Branch Prefix** field, it causes automatic conversion of the IP Office users' extension numbers in calls to and from the SM Line. The branch prefix is added as a prefix to the IP Office user's extension number when it appears as the calling number in calls sent to the SM Line. Similarly, it is added to the extension number when it appears in Diversion-Header or History-Info in calls sent over the SM Line to centralized voicemail.

In calls received from the SM Line, if the called number starts with the branch prefix, the prefix is removed and the IP Office will try to target the remaining number locally, to a non-centralized extension or hunt group. If there is no match, IP Office will target it to any matching system short code. If the called number does not start with the branch prefix, the whole number is checked for a match against system short codes.

Centralized users (SIP or ATA) can call local IP Office users in the same branch by dialing the full enterprise number composed of the branch prefix plus local extension number, and IP Office will remove the branch prefix and target the local extension. This may be needed if short-form dialing is not set up on the centralized Avaya Aura® Communication Manager for Sunny day and the Centralized users are accustomed to dialing the full number.

IP Office users cannot call other local IP Office users in the same branch by dialing the full enterprise number composed of the branch prefix plus local extension number.

Note:

This could be enabled in Sunny day if there is a short code in the IP Office configuration that matches the branch prefix and routes it to the SM Line. But it cannot be enabled in Rainy day. Users should not be instructed to dial differently in Sunny day and Rainy day. Therefore, enabling IP Office users to be able to call other local IP Office users in the same branch by dialing the full enterprise number should not be enabled for Sunny day.

When a call is made by any source on the IP Office system and short code matching targets the SM Line, if the target (the dialed number) starts with the branch prefix, the branch prefix is removed and the call is targeted locally. This does not apply if the target is the extension number of a Centralized user or Centralized group configured on the IP Office. In this case, the call is handled as specified below and in Sunny day it will be sent to Session Manager.

The branch prefix is expected to be used in Distributed enterprise branch deployments and it is expected to be left blank in Centralized enterprise branch deployments. In Mixed enterprise branch deployments, the branch prefix can be left blank or used. If left blank, the IP Office users' extension numbers will have to be the full enterprise number. If used, the IP Office users' extension numbers will be shorter than the Centralized users' extension numbers.

The **Local Number Length** field sets the default length for extension numbers. If an extension number of a different length is configured, a warning appears. The **Local Number Length** field can be left blank. In Mixed enterprise branch deployments, if the **Branch Prefix** field is not blank, and the Centralized users and IP Office users have extension numbers of different lengths, then it is recommended to leave the **Local Number Length** field blank.

Enterprise-wide extensions for Centralized users

The extension number configured on IP Office for the Centralized user is the user's enterprise-wide number. This is the same number that is configured for that user on Session Manager, which is the number that the centralized phone uses when registering to Session Manager in Sunny day and when registering to IP Office in Rainy day.

Centralized users' extension numbers can be up to 13 digits in length. IP Office users' extensions can be up to 9 digits in length.

Note:

Although IP Office deployed as a Centralized branch supports extension numbers up to 15 digits, the 13-digit length is determined by the maximum extension number length allowed for provisioning Centralized users in Communication Manager.

The IP Office **Branch Prefix** field, which causes number modifications for IP Office users' extension numbers, does not impact Centralized users' extension numbers when they appear as calling number or as called number.

Centralized users may have extension numbers that are not related to the local IP Office branch prefix or numbers that begin with the same digits as the IP Office branch prefix. If Centralized users have extension numbers that begin with the same digits as the IP Office branch prefix, the Centralized users' extension numbers look like the IP Office users' extension numbers to the rest of the enterprise. This enables users to keep their numbers when migrating from a Distributed enterprise branch to a Centralized enterprise branch.

Targeting/routing to Centralized users

Calls to centralized users, which can arrive from different sources, are sent to the SM Line in Sunny day and are targeted to the Centralized user's extension locally in Rainy day. Both Sunny day and Rainy day call handling are done automatically by matching the called number to the Centralized user's extension number.

IP Office can manage calls to Centralized users that are dialed to the Centralized user's full extension number, or calls that are dialed using short-form dialing. To support short-form dialing, the global parameter Short Form Dialing Length must be configured. The **Short Form Dialing Length** field appears in IP Office Manager under **System > Telephony** tab **> SM** tab. Configuration of this feature allows IP Office to treat the last *N* digits (where *N* is the number configured for the Short Form Dialing Length) as an alias to that user's extension number.

Short-form dialing from Centralized phones

The Sunny day conversion from the dialed short-form number (for example, 1111) to the enterprise canonical extension number (for example, 5381111) is done by the Communication Manager

Feature Server (CM-FS) or Communication Manager Evolution Server (Communication Manager-ES) based on the caller's location. When a Centralized user makes a call in Sunny day, the call goes directly from the Centralized phone to Session Manager, and IP Office is not involved at this stage. Session Manager first sends the call to the Communication Manager-FS or Communication Manager-ES responsible for calling the Centralized user for origination-side features. That Communication Manager performs the called-number conversion from the dialed short-form to the enterprise canonical number, and sends the call back to Session Manager with the called number modified to the enterprise-canonical number. Session Manager then sequences the call to other applications, if any, and then routes the call based on the enterprise-canonical number. This conversion in Communication Manager is based on Communication Manager configuration of a per-branch location via ip-network-map and ip-network-region forms, as well as Communication Manager per-location AAR analysis to identify the short-form dialed number and per-location route pattern which modifies the called number before sending to Session Manager.

For Rainy day calls made from one Centralized user to another Centralized user, the IP Office Short Form Dialing Length has to be set.

Related links

Planning considerations on page 29
Dial plan example on page 32

Dial plan example

To describe a dial plan example, we have created Acme Travel, a travel agency with a growing number of branches. Each branch follows the same pattern, with extensions for a branch manager and a small team of travel consultants in a sales group.

Given the nature of the business, branch users need to make national and international calls. The company has taken advantage of a bulk call contracts from it headquarters site so wants such calls routed via the headquarters site wherever possible. In addition, the branch staff want to keep their branch phone numbers.

For our examples we have used the following dial plan for each branch site:

- **3-digit branch prefixes beginning with 8** — A 3-digit branch prefix in the range 800 to 899. This allows us up to 100 branches yet keeps call routing simple. Any dialing at a branch that begins with an 8 can be assumed to be a call to a branch number and can be routed to the Avaya Aura® Session Manager for routing to the correct branch.
- **3-digit extension numbers beginning with 2** — 3-digit extension numbers for all extensions and hunt groups starting from 200. This is the default numbering used by IP Office.

SIP extensions may have very different numbering. However, even here, adopting elements of the uniform dial plan will simplify management and usage. For the SIP extension in our examples we have used a dial plan that has 6-digit extension numbers of which the first 3 digits are equal to the branch prefix. This allows users that migrate from a Distributed enterprise branch to a Centralized enterprise branch to keep their same numbers. The numbers for the SIP extensions can also be different and don't necessarily have to share common first digits.

- 3-digit branch numbers beginning with 8, ie. 800 to 899.
- 3-digit IP Office user extension numbers beginning with 2, ie. 200 to 299.

- 6-digit Centralized user extension numbers of which the first 3 digits are equal to the branch prefix e.g. 811250.
- Dial 9 prefix for outgoing PSTN calls.
- National and international calls allowed but routed via the headquarters site's PSTN trunks.
- Where a national call matches a branch location, it should be routed to the PSTN via that branch.
- Local calls allowed from each branch using its own PSTN trunks.
- Modular Messaging at the headquarters site provides voicemail services to all employees.
- The LAN on each branch has a unique IP address, 192.168.42.1, 192.168.44.1 and so on.
- National calls are made via the branch's PSTN trunks when the branch data connection to the headquarters site is not available or at maximum capacity.
- Modular Messaging fallback via PSTN.

This example assumes that all the branches were initially set up with the default North American locale. For IP Office that means that a dial 9 prefix is used for external calls. For calls in other locales or between branches in different locales, the example will need to be adjusted to ensure that the resulting number received at the remote branch will be routed to an external PSTN trunk and is suitable for external dialing.

Related links

Dial plan considerations on page 30

Voicemail considerations

The IP Office system uses its Embedded Voicemail by default. However, a number of other voicemail options are supported.

- **Embedded Voicemail** — Embedded Voicemail uses the system SD card in the IP Office system control unit for storage of prompts and messages. Embedded Voicemail supports mailboxes for all local extension numbers, announcements to waiting callers, and auto attendants (up to 40) for external calls. Its capacity is limited to 15 hours of recorded messages, prompts and announcements.
- **Voicemail Pro** — Voicemail Pro runs on a server computer connected to IP Office and provides a wide range of features. Voicemail Pro is the only option that supports manual call recording for IP Office users and automatic call recording for the IP Office system.
- **Avaya Aura Messaging** — The IP Office system can be configured to use Avaya Aura® Messaging as its voicemail server when Session Manager is used as the core SIP router. When Avaya Aura® Messaging is used as the central voicemail system, at each branch you have the option to still use the local Embedded Voicemail or Voicemail Pro for auto attendant operation and for announcements to waiting calls.
- **Modular Messaging** — The IP Office system can be configured to use Modular Messaging as its voicemail server when Session Manager is used as the core SIP router. When Modular Messaging is used as the central voicemail system, at each branch you have the option to

use Embedded Voicemail to provide auto-attendant operation and announcements for waiting calls or Voicemail Pro for customized call flow actions created for the mailbox.

The Park and Page feature is supported when the system voicemail type is configured as Embedded Voicemail or Voicemail Pro. Park and Page is also supported on systems where Avaya Aura® Messaging or Modular Messaging is configured as the central voicemail system and the local Embedded Voicemail provides auto attendant operation, or Voicemail Pro provides customized call flow actions created for the mailbox.

The Park and Page feature allows a call to be parked while a page is made to a hunt group or extension.

Related links

Planning considerations on page 29
Voicemail options on page 128

Branch PSTN call routing considerations

Each IP Office system can support its own external PSTN trunks. When deployed in an Avaya Aura® network, you have considerable flexibility over where outgoing PSTN calls should emerge from the network and similarly where incoming calls should be routed.

For examples of some of the options available, see Branch PSTN call routing examples on page 204. The examples demonstrate the following options:

- Centralized call control on page 204 — External calls at a branch site can be rerouted to be dialed out at another site. This can be done for reasons of call cost and call control. For example, the central site may have a bulk call tariff for national and international calls that would benefit all branches.
- Branch PSTN Override on page 207 — Having configured the branch to send outgoing external calls to the Avaya Aura® Session Manager for onward routing, there may be cases where a specific number should still be routed via the branches own PSTN trunks.
- PSTN Fallback on page 209 — The IP Office can be configured to allow some calls that would normally use the SM Line to be routed via the PSTN when the SM Line is not available.

The various methods used in the these examples can be combined to match the customer's needs. However the main aim should be as follows:

- To keep the branch configuration as generic as possible, i.e. to use the same PSTN call control in all branch configurations. This simplifies maintenance of multiple branches.
- To centralize as much of the PSTN call control in the Avaya Aura® Session Manager as possible. Again this simplifies maintenance and control.

Related links

Planning considerations on page 29

Chapter 5: Initial setup and connectivity

This chapter provides the initial setup tasks required to deploy an IP Office system as an enterprise branch. This chapter is for new IP Office installations. To migrate an existing IP Office or B5800 Branch Gateway to IP Office, see *Migrating an IP Office or B5800 Branch Gateway to an IP Office Enterprise Branch*.

Initial setup and connectivity checklist

Use this checklist to set up and connect an IP Office system in a Distributed or Centralized enterprise branch deployment.

Number	Description	Section	✔
1	Confirm that the version of Avaya Aura® System Manager is the latest and supports this release of IP Office. For more information, see https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml?name=IP+Office+Platform.		
2	Download IP Office Manager onto the System Manager server.	Manually transferring the IPOAdminLite.exe file to the System Manager server on page 38	
3	Install the shared PLDS license file on the System Manager WebLM server.	Installing the shared PLDS license file on the System Manager WebLM server on page 46 **Note:** If you are using individual license files, and not centralized licensing by WebLM, see Support for individual license files on page 47.	
	Note: Steps 1 through 3 only need to be performed one time. They do not need to be performed for each new IP Office.		

Table continues…

Number	Description	Section	✔
4	Prepare Avaya Aura® System Manager to issue an identity certificate for the IP Office system.	Preparing System Manager to issue an identity certificate for IP Office on page 56	
5	Run the Initial Configuration Utility (ICU). The ICU provides configuration and security settings that minimize initial installation activities and maximize security.	Running the Initial Configuration Utility on page 61 **Note:** When you run the ICU, the Simple Certificate Enrollment Protocol (SCEP) and security settings are automatically configured for the IP Office system and a security certificate is automatically installed on the IP Office. If you do not run the ICU, you must manually configure the SCEP and security settings on the IP Office. This is not the preferred method, but can be used as an alternative. For more information, see Manually configuring the IP Office for SCEP on page 64.	
6	Add each IP Office to System Manager.	Discovering IP Offices on page 66 In this task, you add the branch to System Manager by identifying the subnet IP address in which the branch is located. This task must be performed for each IP Office that you want to manage from System Manager. As an alternative, you can also use one of the following methods to add the IP Office systems to System Manager: • Bulk importing of devices on page 67. This method requires that you first add each IP Office to an xml file. The xml file is then used to import the devices to System Manager. • Adding IP Office to System Manager on page 69. In this task, you manually add each branch to System Manager by identifying the IP address of the IP Office. This task must be performed for each IP Office that you want to manage from System Manager.	
7	Confirm that WebLM licensing for the branch is enabled.	Enabling WebLM licensing for the branch on page 71	
8	Create a system template. (Optional)	Creating a system template on page 72	
9	Upload an auto attendant audio file. (Optional)	Uploading an auto attendant audio file on page 84	

Table continues…

Number	Description	Section	✔
10	Apply the system template to one or more branches. (Optional)	Applying the system template on page 79	
11	Create an endpoint template.	Creating an endpoint template on page 80 **Note:** You must create an IP Office endpoint template. You cannot add a user in System Manager unless an endpoint template has been created.	
12	Configure IP Office to request required licenses from WebLM.	Configuring IP Office to request required licenses from WebLM on page 46	
13	Disable unused trunks.	Disabling unused trunks on page 86	
14	Set a trunk clock quality setting.	Setting a trunk clock quality setting on page 88	
15	Set trunk prefixes.	Setting the trunk prefixes on page 88	
16	Enable SIP trunk support.	Enabling SIP trunk support on page 91	
17	Set the branch prefix and local number length for the extension numbering.	Setting the branch prefix and other fields in the Session Manager System Telephony tab on page 92	
18	Configure system-wide security for the SM Line(s) and Centralized phones	Configuring media security on page 104	
19	Change the default codec selection.	Changing the default codec selection on page 95	
20	Add an SM Line.	Adding an SM Line on page 96 This procedure includes the steps to configure TLS transport for the SM Line.	
21	Add a second SM Line for redundancy.	SM Line redundancy on page 105	
22	Set up outgoing call routing.	• Setting up outgoing call routing on page 108 • For information on routing back to the branch for fallback alternate routes, see Branch PSTN call routing examples on page 204.	
23	Configure the type of voicemail system the branch will use.	Voicemail options on page 128	
24	Enable branch SIP extension support.	Enabling branch SIP extension support on page 110	

System Manager configuration for IP Office

To manage IP Office from System Manager, you must download the IP Office Manager `IPOAdminLite.exe` file onto the System Manager server. You can use the Software Management tool in System Manager to download the `IPOAdminLite.exe` file from PLDS onto the System Manager server.

If you cannot download the `IPOAdminLite.exe` file from PLDS using the System Manager Software Management tool, you can manually transfer the `IPOAdminLite.exe` file to the System Manager server. For more information, see Manually transferring the IPOAdminLite.exe file to the System Manager server on page 38.

When you view or edit an IP Office system template, system configuration, or security configuration from System Manager, System Manager starts IP Office Manager in the appropriate mode on your computer. System Manager automatically prompts you to install IP Office Manager if IP Office Manager is not yet installed on your computer. For more information, see Installing IP Office Manager from the System Manager server to your computer on page 42.

If you have installed IP Office Manager from the IP Office Administrator Applications DVD, ensure that you have the same version of IP Office Manager that is downloaded onto System Manager. If the versions are different, you must do one of the following:

- Upgrade the version of IP Office Manager on the administration computer.
- Update the version of IP Office Manager in System Manager.

Manually transferring the IPOAdminLite.exe file to the System Manager server

About this task

In addition to Manager, the Admin suite, IPOAdminLite, is also available for users to configure Manager applications.

Unlike the Admin suite, IPOAdminLite does not have all the bin files and firmware. It is purely the Manager application for configuring systems.

The following are the limitations of IPOAdminLite as compared to the full Admin suite.

- Help files: Only the English language The `Manager.chm` help file is present in the `IPOAdminLite.exe` installation, and other language variants are not present. Also mode specific chm help files for Partner, quick, norstar mode are not present in the `IPOAdminLite.exe`.
- Phone file: Phone bin files are not present in the `IPOAdminLite.exe` installation. Also, other phone-related xml and settings.txt files are not present with the `IPOAdminLite.exe` installation.
- Memory cards folder : Memory cards folder is missing in the `IPOAdminLite.exe` installation because of which your will not be able to upgrade system files or Web Manager files using IPOAdminLite Manager. Also, the user will not be able to recreat SD card with the `IPOAdminLite.exe` installation.

Procedure

1. Download the `AdminLite-xxx.exe` file, where *xxx* is the version string.

   For example, you can download `AdminLite-<release>(38).exe` from http://plds.avaya.com.

2. Transfer the `AdminLite-xxx.exe` file to the System Manager server to the directory `/opt/Avaya/ABG/<version>/tools`, where <*version*> refers to the System Manager version.

   For example, you might transfer to `/opt/Avaya/ABG/6.3.8/tools`.

   Use any SCP or SFTP protocol to connect to the server and transfer the file. You might use any client to perform this step.

3. Change this file into an executable file by using the command `chmod +x <file name>`.

4. Create a soft link using the name `ManagerSFX.exe` for the uploaded file, as follows:

   a. Go to `$ABG_HOME/tools` by entering `cd $ABG_HOME/tools`.

   b. Use the command `ln -sf <target> <linkname>` to create the soft link.

   For example, if the file name uploaded to `$ABG_HOME/tools` is `IPOAdminLite.exe`, then enter `ln -sf IPOAdminLite.exe ManagerSFX.exe`.

   Tip:

   Use `ls -l ManagerSFX.exe` to verify that the sym link exists.

5. Using any Linux editor, update the parameter abg_b5800_mgr_version in the `/opt/Avaya/ABG/<version>/tools/ManagerSFXVersion.properties` file with the version of IP Office Manager you downloaded from PLDS.

   Important:

   You must update the parameter abg_b5800_mgr_version each time you download a new version of IP Office Manager from PLDS and transfer to System Manager. If you fail to do so, then when you try to start IP Office Manager from System Manager, the start fails and the system displays an error message prompting you to update the parameter.

   The following is an example of the content in the `ManagerSFX.exe` file:

```
[root@smgr tools]# cat ManagerSFXVersion.properties
#The following property should be updated correctly with every version change of
ManagerSFX.exe
# Example
# abg_b5800_mgr_version= 8.1 (4138
# 8.1 (4138) is the version of Avaya B5800 Branch Gateway Manager (ManagerSFX.exe
installer)

#abg_b5800_mgr_version=6.2(38)
abg_b5800_mgr_version=9.0.0.829
```

6. On the administration computer that is used to start IP Office Manager Lite, set the environment variable to match the version of the `IPOAdminLite-xxx.exe` file.

7. Perform the following if the computer is running on Windows:
   a. Click **Start** and then right-click **Computer**.
   b. Click **Properties**.
   c. In the left navigation pane, click **Advanced system settings**.
   d. In the System Properties dialog box, click **Environment Variables**.
   e. In the Environment Variable dialog box, in the **User variables for <*name*>** area, select **IPOFFICEADMIN_VER**.

      Note:

      This variable is applicable if you have added IP Office as a device. You must select **AVAYAB5800_VER** as the variable if you have not added any IP Office devices.

   f. Click **Edit**.
   g. In the Edit User Variables dialog box, in the **Variable value** field, change the value to match the version of IPOAdminLite, for example, `9.0`.
   h. Click **OK**.
   i. Click **OK** for each subsequent dialog box, and then click **Apply**.
8. Install IP Office Manager Lite on the administration computer.

Setting up the environment variable in Windows to match the version of AdminLite

About this task

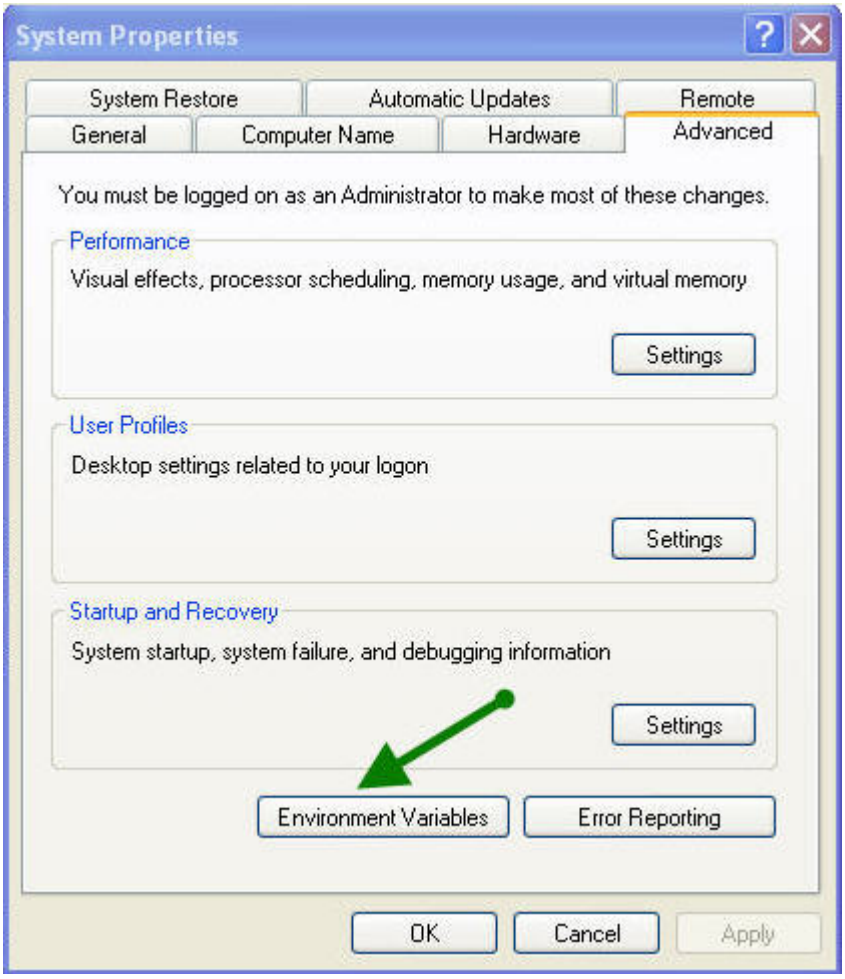
Follow this procedure to set the environment variable of your system to match with the version of AdminLite you install.

Procedure

1. Click **Start**.
2. Right click **Computer**.
3. Click **Properties**.
4. In the left navigation pane, click **Advanced system settings**.
5. In the System Properties dialog box, click **Environment Variables**.
6. In the Environment Variable dialog box, in the **User variables forandmp; lt;n ame>** area, select **IPOFFICEADMIN_VER**. The variable **IPOFFICEADMIN_VER** is applicable if you have added IP Office 9.0 as a device.

   You must select **AVAYAB5800_VER** as the variable if you have not added any IP Office device.

7. Click **Edit**.



8. In the Edit User Variables dialog box, in the **Variable value** field, change the value to match the version of AdminLite.

   Set the value to `9.1`.

9. Click **OK**.
10. Click **OK** for each dialog box.
11. Click **Apply**.

Installing IP Office Manager from the System Manager server to your computer

About this task

Use this procedure to install IP Office Manager from the System Manager server to a computer. When you perform this task, the next time you attempt to view or edit an IP Office device from System Manager on this computer, IP Office Manager starts automatically.

Before you begin

Download the `IPOAdminLite.exe` file onto the System Manager server.

Procedure

1. From 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**.
5. At the prompt **Do you want to download IP Office Manager from the server now?**, click **Yes**.
6. In the **File Download** dialog box, click **Save**.
7. Save the file to an appropriate directory, for example, **C:\Program Files\Avaya\IP Office**.
8. After the download completes, in the **Download complete** dialog box, click **Run**.
9. In the **Internet Explorer - Security Warning** dialog box where you are prompted **Are you sure you want to run this software?** click **Run**.
10. In the **WinZip Self–Extractor** dialog box where you are prompted **Do you want to install IP Office Manager?** click **Setup**.
11. In the **IP Office Manager Lite – InstallShield Wizard** dialog box, do the following:
    a. In the **Welcome** dialog box, click **Next**.
    b. In the **Customer Information** dialog box, click **Next**.
    c. In the **Destination Folder** dialog box, click **Next**.
    d. In the **Custom Setup** dialog box, click **Next**.
    e. Click **Install**.
    f. In the **InstallShield Wizard Completed** dialog box, click **Finish**.
12. Restart your computer.
13. To verify your computer is configured correctly, click **My Computer** > **System Properties** > **Advanced tab** > **Environment Variables**.

Licensing

IP Office deployed as an enterprise branch supports centralized licensing with WebLM. In this licensing model, a single license file is generated in the Avaya Product Licensing and Delivery System (PLDS) for multiple branches. Individual nodal PLDS license files for each branch are also supported. The remote PLDS license on WebLM is the recommended method for IP Office deployed as an enterprise branch.

Note:

A WebLM license is required by each IP Office branch in order to use the WebLM server licensing model. This license is available in PLDS.

Branch System and SM Trunk Channels are added to the IP Office reserve license configuration for WebLM in IP Office Manager.

WebLM license management

IP Office deployed as an enterprise branch supports WebLM licensing in which a single license file is generated in PLDS for multiple branches. This license file contains the host ID of the WebLM server and is managed by the WebLM server. Each IP Office communicates with the WebLM server to request the required license entitlements. IP Office deployed as an enterprise branch uses the Avaya Aura® System Manager WebLM server.

Two configuration models are supported:

- WebLM standard licensing model — in this model, one WebLM server is used. This model is used for enterprises where the System Manager WebLM server is able to manage all IP Office licenses required for the enterprise.
- WebLM enterprise licensing model — in this model, multiple WebLM servers are used. This model is used for enterprises where the licenses required for all branches in the enterprise exceed the System Manager WebLM server capacity. One WebLM server acts as a master WebLM server and hosts the license file from PLDS. The other WebLM servers(s) act as a local WebLM server and host allocation license files from the master WebLM server. Each IP Office must be configured with the IP address of one of the WebLM servers.

For information about WebLM server capacities, see *Avaya IP Office™ Platform in a Branch Environment Reference Configuration*.

Note:

The correct expiration time of licenses for an IP Office that uses a local WebLM server is provided on the corresponding master WebLM server. The local WebLM server shows the licenses as having an expiration time of 30 days or less. However, periodically the license expiration time on the local WebLM server is automatically refreshed and extended when the master WebLM server pushes a refreshed Allocation License File to the local WebLM.

For more information about WebLM licensing, see *Administering Avaya WebLM (standalone)* and *Avaya WebLM Administration Guide*.

Separate PLDS license for each branch

A separate PLDS license file can be generated in PLDS and installed on each branch. This licensing method does not require a WebLM server. The WebLM licensing method is the

recommended method for enterprise branch deployments. However, the separate PLDS licensing method is supported for branches that cannot be connected through an enterprise WAN to a central WebLM server or for upgrading installed B5800 Branch Gateway systems to IP Office.

About the System SD card

The System SD card provides a 10-digit serial number that is used to generate licenses. For ADI licenses, the 10-digit serial number is used to generate the ADI licenses. For the separate PLDS licensing method, a 12-digit serial number is required. For the 12–digit serial number, the digits **11** are pre-pended to the 10-digit serial number printed on the System SD card. In the IP Office Manager application, this number appears in the **PLDS Host ID** field on the System page when you select **System > System**.

Note:

The PLDS Host ID is not relevant to a PLDS WebLM license file because that file is not specific to an individual IP Office system. The PLDS WebLM license file uses the WebLM server's ID (MAC address) as the file Host ID.

About the PLDS Host ID

The IP Office PLDS Host ID is used as the Host ID in PLDS license files when generating an individual PLDS license file for the IP Office. The PLDS Host ID is displayed as part of the IP Office configuration, as well as in SSA. It is a 12-digit number comprised of the digits **11** following by the 10-digit Feature Key serial number printed on the System SD card.

For IP Office systems that are upgrading and using the individual PLDS licenses, the serial number format on the System SD card will be different than what appears for the PLDS Host ID configured for the system. The pre-pended digits **11** do not appear on these System SD cards.

B5800 Branch Gateway systems upgrading to IP Office can continue to use the same System SD card. For these SD cards, the 12-digit serial number printed on the System SD card already includes the additional two digits **11** and will be identical to the IP Host ID displayed in the IP Office configuration.

If the IP Office is using a System SD card from a B5800 Branch Gateway system that has been upgraded to IP Office, then the serial number printed on the SD card will be 12-digits long starting with the digits **11**. These first two digits are ignored in the 10-digit serial number that is displayed in Manager and that is used by ADI licenses.

License modes

The IP Office system can be in one of two license modes — License mode or WebLM mode. Within each license mode, the system can be in one of three states as described below. The license mode is displayed in IP Office Manager when you select **License > License** tab.

License mode

The IP Office system is in License mode when individual licenses are provided for each system and WebLM licensing has not been configured. In License mode, the IP Office system can be in one of three states:

- **License normal** — No license errors are present. Over configuration of licensed features is allowed. There is no 30-day grace period or virtual licenses.

- **License server error** — WebLM has been configured but the server is not available. This state is only possible during the transition period from License mode to WebLM mode. Over configuration of licensed features is allowed. There is no 30-day grace period or virtual licenses.
- **License configuration error** — WebLM has been configured and the server is available, but there are not enough licenses available to license all of the configured features. This state is only possible during the transition period from License mode to WebLM mode. Only individual licenses and the licenses that were able to be obtained from the server are valid. Over configuration of licensed features is allowed. There is no 30-day grace period or virtual licenses.

WebLM mode

The IP Office system is in WebLM mode when the WebLM server has been configured for WebLM licensing. In WebLM mode, the IP Office system can be in one of these states:

- **License normal** — No license errors are present. WebLM has been configured, the server is available, and there are enough licenses available to license all of the configured features. Over configuration of licensed features is not allowed. There is no 30-day grace period or virtual licenses. From this mode, the system can only transition to WebLM error mode.
- **WebLM error** — WebLM has been configured but either the server is not available or licenses for previously configured features are no longer available from the server. Over configuration of licensed features is not allowed. There is a 30-day grace period and virtual licenses for all configured features. This provides time for the required licenses to be acquired.
- **WebLM restricted** — The 30-day grace period for the WebLM error state has expired and the underlying issues causing the error state have not been resolved. Over configuration of licensed features is not allowed. Only configuration changes that reduce the licensing errors are permitted. The configuration change can incrementally reduce the licensing errors and does not need to eliminate all licensing errors. For example, if several different licenses are showing alarms, you can resolve them one at a time. You can resolve one alarm and confirm it is resolved and then continue resolving the remaining alarms in the same way. The system will remain in WebLM restricted mode until all the alarms are resolved. All virtual licenses for the previously configured features during the 30-day grace period are deleted and those features are no longer available.

About returning to License mode from WebLM mode

When the WebLM licensing feature for a branch is disabled (**License > Remote Server** tab, then click **Enable Remote Server** check box to deselect), the IP Office system reverts back to License mode where individual licenses are provided for each branch. The following occurs when a branch reverts back to License mode:

- All WebLM licenses are removed and the features they license will not work.
- Over configuration of licensed features is allowed.
- The 30-day grace period is reset.
- The only path back to WebLM mode is license normal mode where the server is available and there are enough licenses available to license all configured features.

Mode	State	WebLM configured	Over configuration* allowed	Virtual license and grace period
License	Normal	No	Yes	No
	Server error	Yes	Yes	No
	Configuration error	Yes	Yes	No
WebLM	Normal	Yes	No	No
	Error	Yes	No	Yes
	Restricted	Yes	No	No

* The phrase *over configuration* refers to accepting configuration of features that require a license to activate regardless of the availability of the license. When the system is in WebLM Normal or WebLM Error mode, it expects to obtain the license from the server and will reject the configuration of features if the license is not available. When the system is in WebLM Restricted mode, only configuration changes that reduce the licensing errors are permitted. The configuration change can incrementally reduce the licensing errors and does not need to eliminate all licensing errors.

Installing the shared PLDS license file on the System Manager WebLM server

Before you begin

A shared IP Office license file has been activated with the Host ID of the WebLM server. See Activating license entitlements on page 51.

About this task

IP Office uses the Avaya Product Licensing and Delivery System (PLDS) and integration with Web License Manager (WebLM) for license management. If you are using centralized licensing by WebLM, use this task to install the license file on the WebLM server.

Procedure

1. On the System Manager console, under **Services**, click **Licenses**.
2. In the left navigation pane, click **Install License**.
3. Click the **Browse** button and navigate to the appropriate license file.
4. Click the **Install** button.

Configuring IP Office to request required licenses from WebLM

About this task

If you are using centralized WebLM licensing, use this procedure to configure IP Office to request reserved licenses from the remote WebLM server. Most of the reserved licenses that are listed are

not required in a branch deployment. You must identify which licenses are required, and then configure them.

For example, a branch system reserved license with the quantity set to “1” is required. SM Trunks are also typically required with the quantity reflecting the maximum number of simultaneous calls allowed on the SM Line. This must have a minimum value of 1 to allow correct operation.

For more information about general IP Office license requirements, see *Avaya IP Office™ Platform Solution Description*. The steps you must perform to apply licenses in IP Office Manager are described in *Administering Avaya IP Office™ Platform with Manager*.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **License**.
3. Click the **Remote Server** tab.
4. In the **Reserved Licenses** section, use the up and down arrows to select the number of licenses for each license as appropriate.

   Note:

   One of the two local voicemail fields – **Embedded Voicemail Ports** and **Voicemail Pro Ports** – are enabled depending on which local voicemail system is configured.

Support for individual license files

Centralized licensing by WebLM where a shared PLDS license file is installed on the WebLM server is the recommended method for installing license files on IP Office systems that are centrally managed by System Manager. However, IP Office also supports the following licensing methods where individual license files are installed on the IP Office systems:

- Embedded File Management — see Using Embedded File Management to install a PLDS license file on page 47.
- IP Office Manager license file upload — see Using Manager to deliver license files to the branches on page 48.

Using Embedded File Management to install a PLDS license file

Before you begin

License files have been activated. See Activating license entitlements on page 51.

About this task

Use this procedure to install an individual PLDS license on an IP Office that is centrally managed by System Manager.

If the IP Office is centrally managed by System Manager, you must first disable the System Manager administration feature for the branch. After you upload the license file, you must then

enable the System Manager administration feature for the branch. See Disabling the System Manager administration feature for the branch from System Manager on page 149.

Note:

To install an individual PLDS license on an IP Office system that is centrally managed by System Manager, you must rename the PLDS license file to **PLDStemp.xml**. The IP Office system will validate the **PLDStemp.xml** file, and if the validation succeeds, IP Office will automatically rename the file to **PLDSkeys.xml** and save it (overriding the previous valid license file, if any was installed).

Procedure

1. Start Manager.
2. Select **File > Advanced > Embedded File Management**.
3. In the Select IP Office window, click the check box next to the IP Office system.
4. Click **OK**.
5. In the IP Office Embedded File Management dialog box, enter the **Service User Name** and **Service User Password**.
6. Click **OK**.
7. In the Folders pane on the left, select **System SD > System > Primary**.
8. Select **File > Upload file**.
9. Select the **PLDStemp.xml** file and click **Open**.
10. Click **OK**.

    The Upload System Files window appears and shows the upload progress.
11. When the upload is complete, click **Close**.
12. From the Primary folder, perform a refresh.

    The error mode will change to License Normal Mode. The PLDStemp.xml filename is automatically renamed to PLDSkeys.xml.

    Note:

    If the PLDS file is not accepted by IP Office, the IP Office will remain in License Error Mode and the PLDStemp.xml file is not renamed.

Using Manager to deliver license files to the branches

Before you begin

License files have been activated with the Host ID (that is, the Feature Key Serial Number) printed on the IP Office System SD card. See Activating license entitlements on page 51.

About this task

You can use Manager to distribute activated license files to IP Office sites. This procedure explains how to distribute the license files to a single branch at a time.

If the IP Office is centrally managed by System Manager, you must first disable the System Manager administration feature for the branch. After you download the license file, you must then enable the System Manager administration feature for the branch. See Disabling the System Manager administration feature for the branch from System Manager on page 149.

Procedure

1. Start Manager and connect to the IP Office system.
2. In the left navigation pane, select **License**.
3. Right-click **License** and select **Send license file to Avaya Branch Gateway**.
4. In the Upload Files window, select the PLDS license xml file.

   Manager copies the license file to the IP Office SD card where it is validated and stored for persistent use.
5. Select **File > Close Configuration**.
6. To view the license, select **File > Open Configuration**.

WebLM licensing when upgrading IP Office branches to a new release

The WebLM server cannot automatically distinguish between IP Office servers based on their release and provide licenses from two different license files.

In IP Office Branch deployments, when some branches are upgraded and other branches are still running an older release, you cannot add a new license file to the WebLM server just for the upgraded branches and keep licensing the existing branches from an older license file on that WebLM server.

Before starting an upgrade, you must upgrade the licenses for all customers. You might incur a one-time expense from this process. You must generate one new shared license file, instead of the existing shared license file, and install it on WebLM. Then you can start upgrading the IP Office devices. During the transition period, both new and existing IP Office servers request licenses from WebLM and receive licenses from the new shared license file. The license quantities in the shared WebLM license file must be sufficient for all the branches. The existing IP Office servers accept the new licenses. The new shared WebLM license file must include the WebLM Model licenses needed by new and existing IP Office servers.

Alternatively, you can set up a second WebLM server using a standalone virtual WebLM server, and have an older license file installed on one WebLM server and a new license file installed on the second WebLM server. You must change the configuration of each IP Office that is upgraded to use the second WebLM server as the Licensing Remote Server. During the transition, the existing IP Office requests licenses from the first WebLM server and the new IP Office requests licenses from the second WebLM server. Each of the license files on the two WebLM servers must have sufficient license quantities for all new and existing IP Office systems. As you upgrade additional IP Office servers, you must upgrade more licenses in PLDS, re-generate the two license files, and install them on the respective WebLM servers.

Managing license files with PLDS

PLDS overview

Avaya Product Licensing and Delivery System (PLDS) provides customers, Avaya Partners, distributors, and Avaya Associates with tools for managing license entitlements and electronic delivery of software and related license files.

Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads.

Installation software packages for Avaya products are available as OVA and ISO files on PLDS. Users can download the OVA files or the ISO images to a computer, and choose to either burn a DVD for installation or transfer the file to the target server for installation.

You can check PLDS to determine if a later service pack or software release is available. If updates do exist, see the appropriate upgrade procedures, contact Avaya, or contact the Avaya Partner Service representative.

When you place an order for a PLDS-licensed software product, the license entitlements on the order are automatically created in PLDS. When the license entitlements are created, PLDS sends you an email notification. The email notification includes a license activation code (LAC). Using LAC, you can find and activate the newly purchased license entitlements in PLDS. You can then download the license file.

Important:

You must provide the WebLM host ID to activate the license file in PLDS. You can view the WebLM host ID in the WebLM Server Properties page.

Examples of license management tasks that you can perform in PLDS include:

- Adding more license entitlements to an existing activation
- Upgrading a license file to a new major release
- Moving license entitlement activations between license files
- Regenerating a license file with an new host ID

Registering for PLDS

Procedure

1. Go to the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

   The PLDS website redirects you to the Avaya single sign-on (SSO) webpage.
2. Log in to SSO with your SSO ID and password.
3. On the PLDS registration page, register as:
   - An Avaya Partner: Enter the Partner Link ID. To know your Partner Link ID, send an email to prmadmin@avaya.com.

- A customer: Enter one of the following:
  - Company Sold-To
  - Ship-To number
  - License authorization code (LAC)

4. Click **Submit**.

   Avaya sends the PLDS access confirmation within one business day.

About license activation

What is license activation?

License activation is a process of activating license entitlements by specifying a license host and host ID of the WebLM server. The process includes generating the license file.

When license entitlements are activated, PLDS generates activation records that contain the activation information and the license or key.

Types of license activation

Types of activation include:

- Regular activation: where license entitlements are activated to generate activation records.
- Upgrade activation, which involves activating license entitlements that are:
  - Marked as upgradeable. When you activate these license entitlements, you can generate the license or key for the current or an old version.
  - Purchased to upgrade other existing license entitlements. When users activate these license entitlements, they select the license entitlements to upgrade.

Activating license entitlements

Before you begin

Obtain the Host ID of WebLM if you are activating license entitlements on a new license host.

About this task

Use License Activation Code (LAC) to activate one or more license entitlements from the available licenses. After successful activation of the license entitlements, PLDS creates an Activation Record and sends an Activation Notification email message to the customer who is registered with the entitlements. The Activation Record and Activation Notification provide details on the number of activated licenses and the License Host. The license file can be accessed on the License/Keys tab of the Activation Record in PLDS and is also an attachment to the Activation Notification email message.

You must install the license file on WebLM to use the licenses.

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. In the **LAC(s)** field of the Quick Activation section, enter the LAC that you received in an email message.

Note:

If you do not have an email message with your LAC, see “Searching for entitlements” and make a note of the appropriate LAC from the LAC column.

Note:

The Quick Activation automatically activates all license entitlements on LAC. However, you can remove line items or specify the number of licenses to activate from the available licenses.

4. Enter the License Host information.

   You can create a new license host or use an existing license host.
5. Click **Next** to validate the registration detail.
6. Enter the License Host Information.
   - The Host ID of the WebLM server. The Host ID is obtained from the Server Properties page of the WebLM server where the license file is installed.
   - If you are using Centralized Licensing, enter the Centralized Licensing ID of the WebLM server where the license file is installed. Obtain the Centralized Licensing ID from the Server Properties page of the System Manager WebLM server.
7. Type the number of licenses that you want to activate.
8. Review the Avaya License Agreement and accept the agreement.
9. Perform the following steps to send an activation notification email message:
   a. In the **E-mail to** field, enter the email addresses of the additional activation notification recipients.
   b. Enter the comments or special instructions in the **Comments** field.
   c. Click **Finish**.
10. Click **View Activation Record**.
    - The **Overview** tab displays a summary of the license activation information.
    - The **Ownership** tab displays the registration information.
    - The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application.

Searching for license entitlements

About this task

Use this functionality to search for an entitlement by using any one or all of the following search criteria:

- Company name
- Group name
- Group ID

- License activation code

In addition to these search criteria, PLDS also provides other additional advanced search criteria for searching license entitlements.

Note:

Avaya associate or Avaya Partners can only search license entitlements by company name.

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. Click **Assets** > **View Entitlements**.

   The system displays Search Entitlements page.
4. To search license entitlements by company name, type the company name in the **%Company: field**. To see a complete list of companies before you search for their corresponding entitlements, do the following:
   a. Click the **magnifying glass** icon.
   b. Type the name or several characters of the name and a wildcard (%) character.
   c. Click **Search Companies**.
   d. Select the company name from the list.

   Tip:

   You can use a wildcard (%) character if you do not know the exact name of the company you are searching for. For example, if you enter `Av%`, the system searches for all the company names starting with the letter Av. You can enter a wildcard character at any position in the search criteria.
5. To search license entitlements by group name, enter the appropriate information in the **%Group name:** or **%Group ID:** fields.

   Group Names or IDs are specific to Functional Locations and Sold-To's that define the actual location of equipment and software.

   Tip:

   You can use a wildcard character if you do not know the exact name of the group you are searching for. For example, if you enter `Gr%`, the system searches for all the groups starting with the characters Gr. You can enter a wildcard character at any position in the search criteria.
6. To search license entitlements by LAC, enter the specific LAC in the **%LAC:** field.

   Tip:

   If you do not know the exact LAC that you want to search, use a wildcard character. For example, if you type `AS0%`, the system searches for all LACs starting with AS0. You can enter a wildcard character at any position in the search criteria.

You will receive LACs in an e-mail if you have provided the email address in the sales order. If you do not have this code, search by using one of the other search criteria.

7. To search license entitlements by application, *product* or license status, select the appropriate application, product, and/or status from the field.
8. Click **Search Entitlements**.

Result

All corresponding entitlement records appear at the bottom of the page.

Moving activated license entitlements

Before you begin

Host ID or License Host name of the move from/to License Host.

About this task

Use this functionality to move activated license entitlements from one License Host to another. You can chose to move all or a specified quantity of license entitlements.

Note:

If you move a specified number of activated license entitlements from one host to another by using the Rehost/Move transaction in PLDS, two new license files are generated:

- One license file reduces the number of license entitlements on the License Host from which you are moving license entitlements.
- One license file increases the number of license entitlements on the License Host to which you are moving license entitlements.

Install each of these license files on the appropriate server.

If you move all activated license entitlements, only one license file is generated. Install this new license file on the License Host to which you are moving license entitlements. Remove the license file from the License Host from which you are moving all license entitlements.

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. Click **Activation** > **Rehost/Move** from the Home page.
4. Click **View Activation Record information** to find and select licenses to rehost or move.

   You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.

   Note:

   If you are an Avaya associate or Avaya Partner, enter the search criteria and click **Search Activation Records**.
5. Select **Rehost/Move** for the License Host from which you are moving license entitlements.

6. In the **Search License Hosts** field, enter the License Host to which you are moving license entitlements.

   Alternatively, you can click **Add a License Host** to select an existing License Host.

7. Validate the Registration Detail, and click **Next**.
8. Enter the License Host Information.
   - The Host ID of the WebLM server. The Host ID is obtained from the Server Properties page of the WebLM server where the license file is installed.
   - If you are using Centralized Licensing, enter the Centralized Licensing ID of the WebLM server where the license file is installed. Obtain the Centralized Licensing ID from the Server Properties page of the System Manager WebLM server.
9. Enter the number of Licenses to move in the **QTY column** field and click **Next**.
10. Accept the Avaya Legal Agreement.

    You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.

11. Perform the following steps to send an activation notification email message:
    a. In the **E-mail to** field, enter the email addresses of the additional activation notification recipients.
    b. Enter the comments or special instructions in the **Comments** field.
    c. Click **Finish**.
12. Click **View Activation Record**.

    From the **License/Key** tab, you can view and download the license file. Install each license file on the WebLM server associated with the License Host.
    - The **Overview** tab displays a summary of the license activation information.
    - The **Ownership** tab displays the registration information.
    - The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application.

Regenerate License files

Use this functionality to regenerate the license file on a selected License Host. During the regeneration process, you can only modify host ID information.

Regenerating a license file

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. Click **Activation** > **Regeneration** from the Home page.
4. Search License Activations to Regenerate.

You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.

5. Click **Regenerate** from the appropriate record.
6. Validate the Registration Detail, and click **Next**.
7. Validate the items that will regenerate and click **Next**.
8. Accept the Avaya Legal Agreement.

   You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.
9. Perform the following steps to send an activation notification email message:
   a. In the **E-mail to** field, enter the email addresses of the additional activation notification recipients.
   b. Enter the comments or special instructions in the **Comments** field.
   c. Click **Finish**.
10. Click **View Activation Record**.

    From the **License/Key** tab, you can view and download the license file. Install each license file on the WebLM server associated with the License Host.

    - The **Overview** tab displays a summary of the license activation information.
    - The **Ownership** tab displays the registration information.
    - The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application.

Installing certificates

Preparing System Manager to issue an identity certificate for IP Office

About this task

Use this procedure to add an IP Office End Entity to System Manager. This procedure adds the IP Office to the System Manager trust domain and is required to establish a trust relationship between the IP Office and System Manager.

Procedure

1. On the System Manager console, in the **Services** area, click **Security**.
2. On the **Security** page, in the left navigation pane, click **Certificates > Authority**.

3. In the left navigation pane, click **Add End Entity**.
4. On the **Add End Entity** page, do the following:
   a. In the **End Entity Profile** drop-down box, select **INBOUND_OUTBOUND_TLS**.
   b. In the **Username** field, enter the name of the IP Office system.

      You can use the system name that you used when running the ICU.
   c. In the **Password** field, enter a certificate password.

      Note:

      - The password must be a minimum of eight characters and contain any two of the following:
        - Uppercase letters.
        - Lowercase letters.
        - Numbers.
        - Special characters, such as `#` or `*`.
      - Do not repeat the same letter, number, or character more than twice.
      - The password cannot be `Administrator`, `securitypwd`, or `password`.
      - This password is used as the Simple Certificate Enrollment Protocol (SCEP) password. You must enter this password again when you run the ICU.
   d. In the **Confirm Password** field, enter the password again.
   e. In the **CN, Common Name** field, enter the appropriate name.

      This name must be the same as the name of the IP Office system that you entered in the step 4.b on page 57. You must enter this name again when you run the ICU.

      Note:

      The certificate name cannot contain spaces.
   f. In the **Certificate Profile** drop-down box, accept the default setting, **ID_CLIENT_SERVER**.
   g. In the **CA** drop-down menu, accept the default setting, **tmdefaultca**.

      For more information on System Manager CA behavior with cryptographic algorithms, see System Manager certificate algorithm on page 58.
   h. In the **Token** drop-down box, accept the default setting, **User Generated**.
   i. Click **Add End Entity**.

      The page refreshes and a message appears at the top of the page stating the End Entity was added successfully.
5. Click **List/Edit End Entities**.
6. In the **Or with status** drop-down menu, click **All**.

7. Click the **List** button.
8. Confirm the IP Office End Entity that you added is listed.

   Note:

   New appears in the **Status** column, indicating that System Manager has prepared the certificate for exchange with an end entity.
9. Run the ICU.

   Note:

   If you are not going to run the ICU, you must manually configure the IP Office for an identity certificate. For more information, see Configuring the SCEP and security settings for IP Office on page 59.

Related links

Running the Initial Configuration Utility on page 61

System Manager certificate algorithm

In Release 6.3.8 and later, there is a change in the System Manager Certificate Authority (CA) behavior with regards to cryptographic algorithms used for hashing while signing Identity (ID) certificates. IP Office also has a change in behavior while generating new identity certificates. In the CA settings, under **Home** > **Services** > **Configurations** > **Settings** > **SMGR** > **Trust Management**, the preference settings for the signing algorithm is `1` by default. This means **tmdefaultca** uses **SHA-256** while signing ID certificates have a key length of `1024`. Therefore, when the System Manager upgrades, the **tmdefaultca** operates with the new behavior. The recommended release with IP Office is System Manager 6.3.11.

The IP Office device also generates new certificates with **SHA-256** and `2048` as the defaults for cryptographic hashing and key lengths, respectively. However, an IP Office upgraded from a prior release retains its identity certificate from prior releases. Therefore, the certificate will have **SHA-1/1024** as the hashing algorithm and key length. Deleting the certificate preserves the choice for **SHA-1/1024**. If the security settings are reset, then IP Office chooses **SHA-256/2048** as the hashing algorithm and key length. Therefore, you must match the signing algorithms in the System Manager settings and IP Office.

Setting the received certificate check option in IP Office Manager

About this task

The Received Certificate Check option for the Management interface for IP Office Manager is set to **Secure** or **Medium**. The default setting is **Medium**. The System Manager root CA certificate is always generated using a keysize of `1024`. For a setting that is higher, IP Office requires a minimum key size of `2048`.

Procedure

1. In IP Office Manager, click **System**, and then click the **Certificates** tab.
2. In the Identity Certificate area, click **Regenerate**.

3. In the **Received Certificate Checks** drop-down menu, click the appropriate option.
4. Click **OK**.

Adding certificates

Before you begin

Prepare the end entity in Avaya Aura® System Manager for a request from IP Office.

Note:

You need to ensure that the latest System Manager certificates exist in the Trusted Certificate Store. To ensure that the SCEP process runs and updates the Trusted Certificate Store with the correct System Manager Root CA certificate, do the following:

Procedure

1. Open security settings in IP Office Manager.
2. From **System**, click **Certificates**.
3. Delete the Avaya Aura® System Manager root CA from **Trusted Certificate Store**.
4. Enter the DNS and IP address entries as: `DNS: Enter the FQDN of IP Office, DNS: Enter the IP address of IP Office, IP: Enter the IP address of IP office`
5. Click **Delete**.
6. Click **OK** and then save the security settings.

Result

IP Office contacts Avaya Aura® System Manager to sign the identity certificate and stores the root CA in the trusted store.

Configuring the SCEP and security settings for IP Office

When you deploy IP Office with System Manager, IP Office must have an identity certificate that System Manager can validate.

The trust policy selected for the IP Office uses identity certificates signed by the System Manager Certificate Authority (CA). In this case, you must enable the Simple Certificate Enrollment Protocol (SCEP) on the IP Office. You do not need to enable SCEP on the IP Office if you:

- Select a different trust policy for the IP Office servers to use identity certificates from a third-party CA.
- Install the identity certificate through the IP Office security settings.

You must add the root CA certificate, of the CA that issued the IP Office identity certificate, to the System Manager trusted certificates store.

Note:

The default IP Office self-signed identity certificate must not be used in deployments with System Manager.

The preferred method to configure Simple Certificate Enrollment Protocol (SCEP) and security settings for the IP Office system is to run the Initial Configuration Utility. The Initial Configuration Utility automatically configures the SCEP and security settings for the IP Office system. If you do not run the ICU, as an alternative you can manually configure the SCEP and security settings for the IP Office system.

The IP Office system uses SCEP to acquire its certificate from System Manager. The SCEP request triggers System Manager to generate the identity certificate for the IP Office based on the configuration performed in Preparing System Manager to issue an identity certificate for IP Office on page 56. IP Office then receives its certificate from System Manager through the SCEP exchange, and installs it as its identity certificate. IP Office also receives the System Manager CA root certificate from System Manager though the SCEP exchange, and installs it in its Trusted Certificate Store (with the name **default**). This configuration process occurs automatically when you run the ICU. If you do not run the ICU, you must manually perform this configuration as described in Manually configuring the IP Office for SCEP on page 64. Additional information about configuring the SCEP and security settings for IP Office is available in *Avaya Aura® System Manager Online Help*.

Configuring identity certificates for IP Office Branch

About this task

The identity certificate of IP Office must contain a URI that matches with the phone. If you are using SCEP to sign the identity certificate, then you must prepare the Avaya Aura® Session Manager.

Procedure

1. Open IP Office.
2. In **Manager Security Settings** > **Access the System** , click **Certificates**.
3. In **Subject Alternative Name**, select **URI**.
4. In **SIP**, type the IP address of the IP Office.
5. Press **Delete** and click **OK**.
6. Click **Save**.

Next steps

Register the phone with IP Office.

Running the Initial Configuration Utility

Before you begin

Perform the task Preparing System Manager to issue an identity certificate for IP Office on page 56.

About this task

The IP Office Initial Configuration Utility (ICU) provides default configuration and security settings that minimize initial installation activities and maximize security. The ICU is used for new installations and after an IP Office upgrade to enable System Manager administration of the IP Office. The default settings must be configured before the system can be administered by Avaya Aura® System Manager.

Note:

For new installations, use the ICU before the control unit is connected to the network. The ICU can be used to administer the control unit on site or while the IP Office control unit is being staged off site.

This procedure includes the steps to manually launch the ICU. When a new IP Office is detected, the ICU is launched automatically.

Procedure

1. Start Manager and connect to the IP Office system.
2. Select **File** > **Advanced** > **Initial Configuration**.
3. Click the radio button for **IP Office Standard Mode**.
4. In the **System Name** field, enter the appropriate system name.
5. For the **LAN Interface**, select **LAN1** to connect to the enterprise network.

   Warning:

   You are also able to select LAN2 to connect to the enterprise network. However, LAN2 is primarily intended to connect to the Internet or to public SIP trunks from carriers.

   The LAN2 firewall is normally disabled. If you select LAN2 and choose to enable the firewall, be sure to open the necessary ports for communicating with the enterprise network. For more information, see the following documents:

   - *Avaya IP Office™ Platform in a Branch Environment Reference Configuration*.
   - *Avaya IP Office™ Platform Port Matrix* is available at https://support.avaya.com/security under the **Avaya Product Port Matrix Documents** link.
6. In the **IP Address** field, enter the appropriate IP address.
7. In the **IP Mask** field, enter the appropriate IP mask.
8. In the **Gateway** field, enter the IP address of the router that is deployed in the branch. This field is equivalent to what is often referred to as *default gateway* in many IP host implementations.

IP Office Manager will create an IP route in the IP Office configuration using this gateway IP address with the selected IP Office LAN interface as the destination.

9. In the **DHCP Mode** section, click the radio button for **Disabled**.
10. If you want the IP Office to be managed by System Manager, check the **Under Centralized Management?** check box. Then complete the following fields:
    a. In the **New Administrator Password** field, enter a new administrator password.
    b. In the **New Security Password** field, enter a new security password.

    Note:

    The **New Administrator Password** and **New Security Password** fields appear only when these passwords are set to the default. After you change the default passwords, the next time you run the Initial Configuration Utility, these fields will not appear.

    c. In the **SMGR Address** field, enter the IP address of the System Manager server.
    d. In the **Redundant SMGR Address** field, enter the IP address of the secondary System Manager server.
    e. In the **SNMP Community** field, enter the appropriate SNMP community. This is the SNMP community for System Manager.

    Note:

    This field must be configured correctly in order for the centralized management functionality to work.

    f. In the **SNMP Device ID** field, enter the alarm ID you receive from a registration.
    g. In the **Trap Community** field, enter the appropriate trap community.

    This is the SNMP community for the System Manager server.

    Note:

    This field must be configured correctly in order for the centralized management functionality to work.

    The SNMPv1 trap community string can be set from the System Manager console in **Services** > **Configurations** > **Settings** > **SMGR** > **TrapListener**. The trap community string in System Manager must match the trap community string set on the device so that System Manager receives the device alarms properly.

    h. In the **Device Certificate Name** field, enter the certificate name for the IP Office. This name must match the name entered in the **CN, Common Name** field when you added the IP Office End Entity to System Manager.

    Note:

    The device certificate name cannot contain spaces.

i. In the **Certificate Enrollment (SCEP) Password** field, enter the certificate password. This password must match the password entered in the **Password** field when you added the IP Office End Entity to System Manager.

Note:

You must repeat steps 10.h on page 62 and 10.i on page 63 to enable SCEP when the trust policy uses IP Office identity certificates signed by the System Manager Certificate Authority (CA). For more information about SCEP configuration, see Configuring the SCEP and security settings for IP Office on page 59

11. Click **Save**.

The IP Office reboots.

Result

When the IP Office is administered by System Manager, the following is automatically configured:

- SNMP enabled
- SNMP trap destination 1 set as the Primary System Manager address and SNMP trap destination 2 set as the Secondary Redundant System Manager address. IP Office sends alarms as SNMP traps to both System Manager servers.
- All SNMP traps active
- WebLM client active
- WebLM service address from System Manager IP address
- Removes all default extension users, leaving “NoUser” and “RemoteManager”

Additional features configured by the Initial Configuration Utility

After you run the Initial Configuration Utility, the following features are also configured:

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

Manually configuring the IP Office for SCEP

Before you begin

Perform the task Preparing System Manager to issue an identity certificate for IP Office on page 56.

About this task

This task provides an alternate method to configure the SCEP and security settings for an IP Office. Perform this task only if you did not run the Initial Configuration Utility. When you run the Initial Configuration Utility, the SCEP and security settings for the IP Office are automatically configured. For more information, see Configuring the SCEP and security settings for IP Office on page 59.

Procedure

1. Start Manager and connect to the IP Office system.
2. Select **File** > **Advanced** > **Security Settings**.
3. In the **Select IP Office** window, click the check box for the appropriate system.
4. Click **OK**.
5. In the **Security Service User Login** window, enter a user name and password of an account that has security configuration access to the IP Office system.

   The defaults are **security** and **securitypwd**.
6. In the **Security Settings** pane, click **System**.
7. Click the **Certificates** tab.

   The certificate settings are set to the default values. The **Issued to** field shows the default certificate that resides on the IP Office. The default value is the MAC address of the IP Office system.
8. In the **Identity Certificate** section, click **Delete** to delete the default certificate.
9. In the **Warning** dialog box, click **OK**.
10. In the **Default Certificate Name** box, enter the appropriate name. This is the same name you used when you created the certificate for the End Entity in System Manager. See Preparing System Manager to issue an identity certificate for IP Office on page 56 for more information.
11. In the **Received Certificate Checks (Management Interfaces)** drop-down box, accept the default setting, **None**.
12. In the **Received Certificate Checks (Telephony Endpoints)** drop-down box, accept the default setting, **None**.
13. In the **SCEP Settings** section, do the following:
    a. Click the **Active** check box to select that option.
    b. In the **Request Interval (Seconds)** field, accept the default setting, **120**.

c. In the **SCEP Server IP/Name** field, enter the IP address of the System Manager server. Include `https://` at the beginning of the IP address, for example `https://123.4.567.89`.

d. In the **SCEP Server Port** field, accept the default setting, **443**.

e. In the **SCEP URI** field, accept the default setting.

f. In the **SCEP Password** field, enter the appropriate password. This is the same password you used when you created the certificate for the End Entity in System Manager. See Preparing System Manager to issue an identity certificate for IP Office on page 56 for more information.

g. Click **OK**.

14. Click **File > Save** to save the security configuration.
15. From the System Manager console, do the following:
    a. Go to the **List End Entities** page. (See Steps 1 to 2 in Preparing System Manager to issue an identity certificate for IP Office on page 56.
    b. In the left navigation pane, click **List End Entities**.
    c. Click the **Reload** button to reload the End Entity.

       After the page refreshes, the status of the End Entity changes from **New** to **Generated**. This indicates the End Entity certificate exchange has occurred.
16. In Manager, return to the **Certificates** tab. See Steps 1 to 7 above.
17. In the **Received Certificate Checks (Management Interfaces)** drop-down box, select **Medium**.

    This ensures the IP Office will enforce the use of certificates.
18. Click **OK**.
19. Click **File > Save** to save the security configuration.

About adding IP Offices to System Manager

There are three different methods available that can be used to add IP Offices to System Manager. See one of the following topics:

- Discovering IP Offices on page 66. This method requires you to identify the subnet IP address in which each branch is located. This method does not automatically discover all IP Offices in a network.
- Bulk importing of devices on page 67. This method requires you to manually add each IP Office to an xml file that is then used for bulk import to System Manager.
- Adding the IP Offices to System Manager on page 69. This method requires you to manually add each branch to System Manager by identifying the IP address of the IP Office.

After the IP Office systems are added to System Manager, perform a synchronization. See Synchronizing IP Office with System Manager on page 151.

Discovering IP Offices

About this task

Use this task to discover the IP Offices in the network and add them to System Manager. This task requires that you identify the subnet IP address in which the branch is located. There is always one IP Office per branch and each branch is in a different subnet. This procedure must be performed for each branch.

Before you begin

Enable SNMP on the IP Office to be updated. See Enabling SNMP and polling support on page 67.

Procedure

1. From the System Manager console, under **Services**, click **Inventory**.
2. On the Inventory page, select **Manage Elements > Discovery**.
3. On the Subnet Configurations page, click **New**.
4. On the New SNMP Access Profile page, in the **Type** drop-down box, select **V1**.
5. In the **Description** field, enter a description to help identify this SNMP access configuration.
6. Set the **Read Community** field as configured on the device.
7. Set the **Write Community** field as configured on the device.
8. Accept the default settings in the **Timeout (ms)** and **Retries** fields.
9. Click **Commit**.
10. On the Discovery Profiles page, click **New**.
11. On the Create Discovery profile page, in the `DiscoveryProfileName` field, enter a name to identity the new discovery profile.
12. From **Subnet Configurations**, select the appropriate subnet.
13. From **Element Type Access Profiles**, select **IP Office** or **IP Office UCM or IP Office Application Server**.
14. From **Profile List**, select the appropriate SNMP profile.
15. Click **Commit**.
16. To schedule a discovery, select the appropriate Discovery Profile and choose one of the following options: .
    - Click **Discover Now** to run the discovery job now.
    - Click **Schedule Discovery** to run the discovery job at a scheduled date and time.

17. Repeat steps 10 to 16 for each branch that is to be managed from System Manager

Result

When the job is completed, the IP Office device(s) appear on the Collected Inventory page (**Services > Inventory > Collected Inventory**) and on the IP Office page (**Services > Software Management > Manage Software > IP Office**).

Enabling SNMP and polling support

About this task

In order for the IP Office control unit to be discovered and polled by an SNMP manager, its SNMP agent must be enabled and placed in the same read community as the SNMP manager.

Procedure

1. Start Manager and connect to the IP Office system.
2. In the left navigation pane, click **System**.
3. Click the **System Events** tab.
4. Select **SNMP Enabled**.
5. In the **SNMP Port** field, enter the UDP port number used by the SNMP agent to listen for and respond to SNMP traffic.

   The default is 161.
6. In the **Community (Read-only)** field, enter the community to which the device belongs for read access.

   This community name must match that used by the SNMP manager application when sending requests to the device. The community public is frequently used to establish communication and then changed (at both the SNMP agent and manager ends) for security.
7. Click **OK**.
8. Select **File > Save Configuration** to send the configuration back to the IP Office and then select **reboot**.

   After the reboot, the SNMP manager will be able to discover the control unit. The discovery includes the control unit type and the current level of core software.

Bulk importing of devices

Before you begin

Each IP Office device has been added to an xml file. For information about the xml file containing the devices, see About the xml file containing the devices on page 68.

About this task

Use this task to import the IP Office devices from an xml file to System Manager.

Procedure

1. From the System Manager console, under **Services**, select **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **More Actions > Import**.
4. On the Import Elements page, in the **Select File** field, enter the complete path of the xml file. Or, click **Browse** to locate the xml file.
5. Select one of the following error configuration options:
   - **Abort on first error**
   - **Continue processing other records**
6. Select one of the following import options:
   - To skip a matching record that already exists in the system during an import operation, click **Skip**.
   - To replace all data for an application, click **Replace**.
   - To merge application data so that you simultaneously perform an add and update operation of the application data, click **Merge**.
   - To delete the application data from the database that match the records in the xml file, click **Delete**.
7. Select one of the following schedule job options:
   - Click **Run immediately** to run the job now.
   - Click **Schedule later** and then select the date and time to run the job at a scheduled date and time.
8. Click **Import**.

XML file containing the IP Office devices

To use the bulk import method to add IP Office systems to System Manager, you must first manually add each IP Office device to an XML file.

The following sample shows the contents of an XML file for one IP Office device.

```
<?xml version=”1.0” ?>
<RTSElements xmlns="http://www.avaya.com/rts"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<ApplicationSystems>
<ApplicationSystem name="IPOffice_2" isTrusted="false">
<Host ipaddress="192.168.42.2"></Host>
<ApplicationSystemType name="IP Office Branch"
version="0"></ApplicationSystemType>
      <Attributes>
               <Attribute name="Is IPOffice for Linux"
value="false"></Attribute>
               <Attribute name="Service Login"
value="BranchAdmin"></Attribute>
               <Attribute name="Service Password"
value="BranchAdmin"></Attribute>
               <Attribute name="Device version"
```

```
value="<release>"></Attribute></Attributes>
</ApplicationSystem>
</ApplicationSystems>
</RTSElements>
```

The fields for each IP Office device that you add to the XML file will be the same except for the following two fields. These fields contain unique information for each device:

- **<ApplicationSystem name="***IPOffice device***"isTrusted="false">** where *IPOffice device* is a unique name for this system.
- **<Host ipaddress="***IP address***"></Host>** where *IP address* is a unique IP address for this system.

Adding IP Office to System Manager

About this task

Use this procedure to manually add each IP Office system to System Manager.

Procedure

1. On the System Manager console, in the **Services** area, click **Inventory**.
2. On the Inventory page, click **Manage Elements**.
3. On the Manage Elements page, click **New**.
4. In the **New Elements** area, in **Type**, click **IP Office**.
5. On the Add IP Office page, do the following:
   a. In **Name**, type a name for this IP Office.
   b. In **Description**, type a description to identify the IP Office.
   c. In **Node**, type the IP address of the IP Office.
   d. In the **Device Type** drop-down menu, click **IP Office**.
   e. In the **Device Version** drop-down menu, accept the default release number.

      The **Device Type** and **Device Version** fields display **Select** by default. You must select an item from the drop-down list.

   f. In **Service Login**, type the appropriate login.

      The default login is `BranchAdmin`.

      In the earlier version of IP Office R9.1, the default login for IP Office is `SMGRB5800Admin`. When you upgrade IP Office, you can use this default login name, `SMGRB5800Admin`.

      A new `BranchAdmin` account is created automatically. The configuration of the `BranchAdmin` account is the same as the `SMGRB5800Admin` account.

If you add a new IP Office R9.1 or later to System Manager by running the Initial Configuration Utility (ICU) on IP Office, the `BranchAdmin` account becomes available.

g. In **Service Password**, type the appropriate password.

The default service password is the same as the Service Login.

h. In **Confirm Service Password**, type the password again.

6. Click the **SNMP** tab.
7. For the SNMP Version, click **V1**.
8. In **Read Community**, type the community to which the device belongs for read access.
9. In **Write Community**, type the community to which the device belongs for write access.
10. In **Retries**, select the appropriate number.
11. In **Timeout (ms)**, select the appropriate number.
12. Click **Commit**.
13. Repeat steps 3 on page 69 to 12 on page 70 for each branch that you plan to manage from System Manager

Add IP Office field descriptions

General

Name	Description
Name	The name of the IP Office device. The name must only contain lowercase and uppercase alphabets, numbers from 0 to 9, commas, hyphens, and underscores.
Description	The description of the IP Office device.
Node	The IP address can be in the IPv4 or IPv6 format. The host name or the IP address of the IP Office device.
Device Type	The type of the IP Office device. The options are IP Office and B5800.
Device Version	The version of the IP Office device.
Service Login	The login name to access the IP Office device. The default is BranchAdmin.
Service Password	The password to access the IP Office device.
Confirm Service Password	The service password that you retype for confirmation.

For IP Office releases earlier than 9.1, the default service login for IP Office is SMGRB5800Admin. After you upgrade IP Office from Release 9.0 to 9.1 or later, you can use the same login name, SMGRB5800Admin. The account remains active.

However, the system creates a new account, BranchAdmin. The configuration of the BranchAdmin account is the same as the SMGRB5800Admin account. The new account also becomes active.

In IP Office Release 9.1 or later, if you reset the security setting, the system deletes the SMGRB5800Admin account and adds the BranchAdmin account that remains disabled. You must activate the account by accessing the IP Office security setting offline.

Also, if you add the new IP Office Release 9.1 or later in System Manager by running Initial Configuration Utility (ICU) on IP Office, the default account, BranchAdmin, will be available. The account becomes active.

SNMP

Name	Description
Version	The SNMP protocol type. The options are None and V1.
Read Community	The read community of the device.
Write Community	The write community of the device.
Retries	The number of times that an application polls a device without receiving a response before timing out.
Timeout (ms)	The number of milliseconds that an application polls a device without receiving a response before timing out.

Button	Description
Commit	Adds the IP Office device to the inventory.
Clear	Clears your entries and reset the page.
Cancel	Cancels the add operation, and returns to the previous page.

Impact of IP Office security settings on the BranchAdmin account

In IP Office R9.1 and later, if you reset the security settings, the `SMGRB5800Admin` account is deleted and the `BranchAdmin` account is disabled. You must activate the account by accessing IP Office security settings offline.

Enabling WebLM licensing for the branch

About this task

If you are going to use WebLM licensing, you must enable the WebLM licensing feature for the branch. See Licensing on page 43 for more information.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **License**.
3. Click the **Remote Server** tab.
4. Click the check box for **Enable Remote Server** to select this option.

5. In the **Domain Name (URL)** field, enter the IP address or fully qualified domain name of the System Manager WebLM server or other WebLM server that is being used.
6. In the **URN** field, enter the name of the WebLM server. The default is **WebLM/LicenseServer**.
7. In the **Port Number** field, use the up and down arrows to select the port number of the WebLM server. The default is **52233**.
8. Click **File > Save Configuration**.

Template Management

Creating a system template

About this task

Use this task to create a system template and distribute it to multiple IP Office systems using different browsers for IP Office 11.0 and above versions.

Procedure

1. From the System Manager console, under **Services**, select **Templates**.
2. On the **Templates** page, in the left navigation pane, click **IP Office System Configuration**.
3. On the **IP Office System Configuration Templates** page, under **Supported IP Office Types**, click the check box for **IP Office**.

Browser	Procedure
Mozilla Firefox (all supported versions)	a. In IP Office Manager, go to **Tools** > **System Template** > **New System Template** **Create Template** page opens. b. Type the **Output File Name** and select the appropriate release version from **Select Version** drop-down list and click **OK**. c. When finished, select **File** > **Save Template** > **Exit**. d. In SMGR, under **Upload System Configuration Template File** click **Choose File**. e. Click **Upload**. f. Click **Commit**.

Browser	Procedure
Internet Explorer 11.x	a. Under **Templates List**, click **New**. b. In the **Name** field, enter a name for this template. c. In the **System Type** drop-down box, select **IP Office**. d. In the **Version** drop-down box, select the appropriate release. e. To add more details to this system template, click **Details**. IP Office Manager is launches. f. Complete the fields as appropriate. g. When finished, select **File** > **Save Template** > **Exit**.

4. Apply the system template to the IP Office systems. See Applying the system template on page 79.

Viewing an IP Office system template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **IP Office System Configuration**.
3. On the **IP Office System Configuration Templates** page, do the following:
   a. Under **Supported IP Office Types**, click the check box for the IP Office systems you want to modify.
   b. Click **Show List**.

   Templates List lists all the templates.

Browser	Procedure
Mozilla Firefox (all supported versions)	a. Under **Templates List**, click the check box for the template you want to modify. b. Click **Download**. c. Open IP Office Manager. • Go to **File** > **Open File** • Browse to select the downloaded **.cfg** file. and click **Open**. In the IP Office Manager window, in the right pane, you can view the system configuration template details. All the fields are read-only. • Click **File** > **Exit** to exit IP Office Manager.

Browser	Procedure
Internet Explorer 11.x	a. Under **Templates List**, click the check box for the template you want to modify. b. Click **View**. IP Office Manager launches. • In the IP Office Manager window, in the right pane, you can view the system configuration template details. All the fields are read-only. • Click **File** > **Exit** to exit IP Office Manager.

Modifying a system template

About this task

The system template provides the capability to modify the system configuration on a granular level. This is referred to as a partial system template. An existing system template can be modified and pushed to specific devices to merge the updated and/or new configuration information without overriding the existing configuration in other areas. Not all fields in the system template can be updated in this way. This feature is available for specific blocks of fields. See Editable system template fields on page 76 for the block of fields that can be modified.

Typical ways that a partial system template can be used are to:

- Provision a new auto attendant only on multiple IP Office systems
- Modify the greeting file name for an auto attendant on multiple IP Office systems
- Delete an auto attendant which is not being used on multiple IP Office systems

Use this task to modify a system template using different browsers for IP Office 11.0 and above versions.

Procedure

1. From the System Manager console, under **Services**, select **Templates**.
2. On the **Templates** page, in the left navigation pane, click **IP Office System Configuration**.
3. On the **IP Office System Configuration Templates** page, do the following:
   a. Under **Supported IP Office Types**, click the check box for the IP Office systems you want to modify.
   b. Click **Show List**.

   Templates List lists all the templates.

Browser	Procedure
Mozilla Firefox (all supported versions).	a. Under **Templates List**, click the check box for the template you want to modify. b. Click **Download**. c. Open IP Office Manager and go to **Tools** > **System Template** > **Edit System Template** **Edit Template** page opens. a. Click **Browse** to select the downloaded template. b. Type the same file that matches with browsed file name without extension (.cfg) in **Output File Name** and click **OK**. c. In the left pane, click the check box for the node you want to modify. d. On the details pane, click the check box for the current active tab. The fields in the active tab become editable. e. Modify the fields as appropriate. The tab turns red to indicate changes have been made to the fields in that tab. **Note:** When in partial edit mode, if you clear the main check box in the upper left-had corner of the screen, all changes you have made to the template will get cleared. You must click that check box again to return to partial edit mode. f. When finished, select **File** > **Save Template** > **Exit**. d. In SMGR, under **Upload System Configuration Template File** click **Choose File**. e. Click **Upload**. If the template file name matches the existing template file name, SMGR replaces the existing template with uploaded modified template. f. Click **Commit**.

Browser	Procedure
Internet Explorer 11.x	a. Under **Templates List**, click the check box for the template you want to modify. b. Click **Edit**. IP Office Manager is launched. c. To edit the system template on a granular level, do the following: a. Click the main check box in the upper left-hand corner of the screen. All screens become read-only and you are in partial edit mode. b. In the left pane, click the check box for the node you want to modify. c. On the details pane, click the check box for the current active tab. The fields in the active tab become editable. d. Modify the fields as appropriate. The tab turns red to indicate changes have been made to the fields in that tab. **Note:** When in partial edit mode, if you uncheck the main check box in the upper left-had corner of the screen, all changes you have made to the template will get cleared. You must click that check box again to return to partial edit mode. e. Click **OK**. d. When finished, select **File > Save Template and Exit**.

4. Apply the modified system template to the IP Office systems. See Applying the system template on page 79.

Editable system template fields

Node Level	Group/Sub Group
System	LAN1/LAN Settings
	LAN1/VoIP
	LAN1/SIP Registrar
	LAN1/Network Topology
	LAN2/LAN Settings
	LAN2/VoIP
	LAN2/Network Topology
	LAN2/SIP Registrar
	Directory Services
	Telephony/Telephony

Table continues…

Node Level	Group/Sub Group
	Telephony/Park & page
	Telephony/ Tones & Music
	Telephony/ Ringtones
	Telephony/ SM
	Telephony/ Call Log
	Telephony/ TUI
	System Events/Configuration
	DNS/ Newtwork Services
	VoiceMail
	CDR/SMDR
	SMTP
	Codecs
	Twinning
	CCR
Hunt Group	Hunt Group
	Queuing
	Overflow
	FallBack
	VoiceMail
	Voice Recording
	Announcements
	SIP
Analog Line	Line Settings
	Analog Options
Dect Line	Dect Line
SIP Dect Line	SIP Dect Base
	VOIP
SIP Line	SIP Line
	Transport
	SIP URI
	T38 Fax
	SIP Credentials
	VOIP
H323 Line	VoIP Line
	Short Codes

Table continues…

Node Level	Group/Sub Group
	VOIP Settings
SM Line	Session Manager
	VOIP
	T38 Fax
License	Remote Server
ARS	ARS
Directory	Directory
IP Routes	IP Route
Account Code	Account Code
	Voice Recording
Auto Attendants	Auto Attendant
	AA Actions
Firewall Profile	Standard
	Custom List
	Static NAT (IP Address List)
Time Profile	Time Profile
ICR	Standard
	Voice Recording
	Destinations
Short Code	Short Code
RAS	RAS PPP
Tunnel	Tunnel L2TP PPP
Location	Location
Services	Service
	Session
	NAPT
	FALLBack
	Bandwidth
	IP
	Auto Connect
	Quota
WAN Port	WAN Port

Table continues…

Node Level	Group/Sub Group
	Frame Relay
	DLCIs
	Advanced

Deleting an IP Office system template

Procedure

1. From the System Manager console, under **Services**, select **Templates**.
2. On the **Templates** page, in the left navigation pane, click **IP Office System Configuration**.
3. On the **IP Office System Configuration Templates** page, do the following:
   a. Under **Supported IP Office Types**, click the check box for the IP Office systems you want to modify.
   b. Click **Show List**.

   Templates List lists all the templates.
4. Select the system template you want to delete from the IP Office System Configuration list.
5. Click **Delete**.

   The system displays the system template instance you selected for deletion.
6. Do one of the following:
   - Click **Delete** to delete the template.
   - Click **Cancel** to cancel the delete operation.

Applying the system template

Procedure

1. From the System Manager console, under **Services**, select **Templates**.
2. On the **Templates** page, in the left navigation pane, click **IP Office System Configuration**.
3. Under **Supported IP Office Types**, click the check box for **IP Office**.
4. Click **Show List**.

   All templates appear in the **Templates List**.
5. Select the template you want to apply, and then click **Apply**.
6. On the **Apply IP Office System Configuration** page, select the IP Office(s) to which you want to apply the template.

7. Do one of the following:
   - Click **Now** to run the job now.
   - Click **Schedule** to run the job at a scheduled date and time.

Creating an endpoint template

About this task

Use this task to create endpoint templates that can be used for user administration.

Procedure

1. From the System Manager console, under **Services**, select **Templates**.
2. On the **Templates** page, in the left navigation pane, click **IP Office Endpoint**.
3. On the **IP Office Endpoint Templates** page, do the following:
   a. Under **Supported IP Office Types**, click the check box for **IP Office**.
   b. Under **Templates List**, click **New**.
4. In the **Name** field, enter a name for this endpoint.
5. In the **System Type** drop-down box, select **IP Office**.
6. In the **Set Type** drop-down box, do one of the following:
   - Select **ANALOG** to create a template for Analog Terminal Adapters (ATAs). This template can be applied when adding ATA users to System Manager. An ATA user is a user configured as a Centralized user whose associated extension is an analog extension.

     Note:

     Standard analog phones or analog fax devices are supported for use by ATA users.
   - Select **SIP** to create a template for SIP Phones. This template can be applied with adding Centralized SIP users to System Manager.
7. In the **Version** drop-down box, select the appropriate version.
8. To configure more details for this endpoint, click the **Details** button.

   The IP Office Web Manager is launched.
9. On the Request Authentication page, click the **OK** button.

   Note:

   You do not need to provide a certificate on this page. This page will always appear when you launch IP Office Manager.
10. Complete the appropriate fields.

    The fields you can edit in the user template are those that are applicable to multiple users. Fields that are non-editable are not applicable to multiple users.

Note:

Specific user configuration is available with the Endpoint Editor. See Adding IP Office users to System Manager on page 69 for more information.

11. When finished, select **File > Save Template and Exit**.

    The template is saved in System Manager and listed in the Template List table.

Managing the IP Office Endpoint template

Adding an IP Office endpoint template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **IP Office Endpoint**.
3. Click **New**.
4. Enter the required information in the **Name**, **System Type**, **Set Type**, and **Version** fields.
5. Click **Details**.

   The system launches the IP Office Manager application.
6. On the IP Office Manager window, in the right pane, specify the required details, such as voice mail, telephony, and button programming in the respective tabs.
7. Click **File** > **Save Template and Exit** to save the template configuration and exit the IP Office application.

   The system directs you to the landing page of **IP Office Endpoint**.

   You can view the newly created template in the list of templates under IP Office endpoint templates.

   When you upgrade System Manager, Default Centralized ATA Template, Default Centralized SIP Template are now available to create centralized users.

Viewing an IP Office endpoint template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **IP Office Endpoint**.
3. Select a type of system from the list of IP Office supported templates.
4. Click **Show List**.
5. Under **IP Office Endpoint Templates**, select the template you want to view from the list of templates.
6. Click **View**.

This action launches the IP Office Manager application.

7. On the IP Office Manager window, click the tabs on the right pane to view the template details.
8. Click **File** > **Exit** to exit the IP Office Manager application.

   The system displays the **IP Office Endpoint** landing page.

Editing an IP Office endpoint template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **IP Office Endpoint**.
3. Select a type of system from the list of IP Office supported templates.
4. Click **Show List**.
5. From the list of **IP Office Endpoint Templates**, select the template you want to edit.
6. Click **Edit**.

   This system launches the IP Office application.
7. On the IP Office Manager window, in the right pane, edit the required details.
8. Click **File** > **Save Template and Exit** to save the modifications to the template and exit the IP Office Manager application.

   The system displays the IP Office Endpoint landing page.

Duplicating an IP Office endpoint template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **IP Office Endpoint**.
3. Select a system type from the list of IP Office supported templates.
4. Click **Show List**.
5. From the list of IP Office endpoint templates, select the template you want to duplicate.
6. Click **Duplicate**.
7. Type a template name in the **New Template Name** field.
8. Click **Commit**.

   If you want to make changes to the new endpoint template, click **Details**.

Deleting an IP Office endpoint template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.

2. In the navigation pane, click **IP Office Endpoint**.
3. Select a type of system from the list of IP Office supported templates.
4. Click **Show List**.
5. From the **IP Office Endpoint Templates** list, select the template you want to delete.
6. Click **Delete**.

   The system displays the template instance you selected for deletion.
7. Perform one of the following:
   - Click **Delete** to delete the template.
   - Click **Cancel** to cancel the delete operation and return to the **IP Office Endpoint** landing page.

Upgrading IP Office endpoint templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **IP Office Endpoint**.
3. Select the IP Office device type.
4. Click **Show List**.
5. Select the template you want to upgrade.
6. Click **Upgrade**.
7. In the **Supported IP Office Versions** field, enter the target version for upgrade.
8. In **Template Name**, type the name of the template.

   Template name must be a unique name.
9. Click **Upgrade**.

   System Manager upgrades the selected template, and the IP Office Manager starts with the upgraded template. The original template you selected is retained.
10. After the IP Office Manager starts, the new, upgraded template, save and exit.

    The system displays the upgraded template in the IP Office Endpoint List page.

IP Office endpoint template field descriptions

Name	Description
Name	The name of the IP Office endpoint template.

Table continues…

Name	Description
System Type	The type of system associated with the IP Office device. The valid options are: • **IP Office**: for IP Office core unit • **B5800**: for B5800 core unit
Version	The version of the IP Office endpoint template.
Set Type	The set type associated with the IP Office endpoint template. This is a drop-down field listing the following set types: • **ANALOG** • **SIP** • **IPDECT** • **DIGITAL** • **H323** • **SIP DECT** Only IP Office devices support the **SIP DECT** set type.
Last Modified Time	The date and time when you last modified the template.

Button	Description
Details	Click to open the IP Office application to add or edit the template details.

Uploading an auto attendant audio file

About this task

You are able to upload and convert audio files to System Manager that can be used in the IP Office system configuration auto attendant feature. Once uploaded, from IP Office Manager you are able to select the audio files from the Auto Attendant page. For more information about the field options in System Manager, see *Avaya Aura® System Manager Online Help*.

Note:

If you are using a system template, you can add the audio file to the template to push the audio file down to multiple IP Office systems.

Procedure

1. From the System Manager console, under **Services**, select **Templates**.
2. On the **Templates** page, click **IP Office System Configuration**.
3. On the **IP Office System Configuration Templates** page, under **Templates List**, select **More Options > Manage Audio**.

4. On the **Manage Audio** page, click the **Browse** button to locate the .WAV file you want to upload.
5. Click the **Upload** button.

   The voice file is uploaded to System Manager in the .C11 format that is required for Embedded Voicemail on IP Office systems. The file is automatically converted from the .WAV format to the .C11 format.
6. When finished, click the **Done** button.

Converting a .WAV audio file to a .C11 audio file

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **IP Office System Configuration**.
3. Click **More Options** > **Manage Audio**.
4. On the Manage Audio page, select the .WAV audio file from the **List of Audio Files** that you want to convert to .C11 format.
5. On the Convert Audio page, the system lists the file you selected for conversion.
6. If you want to change the recording label of the .WAV file, edit the label text in the corresponding text box under the **Recording Label** column.
7. Click **Commit** to confirm the convert action.

   The system displays the newly converted audio file under the corresponding audio name column in the **List of Audio Files** table.

Deleting an audio file

About this task

Use the **Delete** button to delete audio files from the list of audio files. You can choose to either delete the .WAV audio format, or the .C11 audio file format, or delete both the audio file formats in a single step.

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **IP Office System Configuration**.
3. Click **More Options** > **Manage Audio**.
4. On the Manage Audio page, select the audio file you want to delete from the list of audio files.
5. Click **Delete**.

6. On the Delete Audio File Confirmation page, you can view the audio files you selected in Step 4 for deletion. From the **Select the type of deletion** field perform one of the following:
   - Select the type of audio file extension you want to delete.
   - Select **Both** if you want to delete both the file extension types.

   Sample scenario: Suppose you have ABC.wav and ABC.c11 audio files in the **List of Audio Files**. If you want to delete only the ABC.wav audio file, then select **Wave** from **Select the type of deletion**. If you want to delete both the audio files in a single step, then select **Both** from the **Select the type of deletion** field.
7. Click **Delete**.
8. Click **Done** to return to the IP Office System Configuration landing page.

Disabling unused trunks

About this task

Each IP Office trunk card provides a fixed number of trunk ports with digital trunk ports supporting a fixed number of digital channels. By default the IP Office configuration will have settings for all the possible trunks and channels.

In cases where the number of trunks or trunk channels in use is lower than the number supported by the trunk card, the unused trunks and channel must be disabled.

Important:

Failure to do this will cause problems with outgoing calls. For example, on a system with an ATM4 trunk card fitted but only two analog trunks actually connected, failure to disable the other two trunks within the IP Office configuration will cause 50% of outgoing call attempts to fail.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **Line**.
3. For each line, set those lines or channels that are not connected or not being used as **Out of Service**.

   The location of the relevant setting varies for each trunk type.
4. For **Analog Trunks**, set the **Trunk Type** to **Out of Service**.
5. For **BRI, E1 PRI, S0 and QSIG Trunks**, set the channels quantities to match the actual subscribed channels.

6. For **T1, T1 PRI and E1R2 Trunks**, select the Channels tab. Then do the following:

   Select those channels that are not used and click **Edit**.

   - For T1 set the **Type** to **Out of Service**
   - For T1 PRI set the **Admin** field to **Out of Service**.
   - For E1R2 trunks set the **Line Signalling Type** to **Out of Service**.

7. Click **File > Save Configuration**.

Digital trunk clock source

About this task

Digital trunks require the telephone system at each end of the trunk to share a clock signal to ensure synchronization of call signalling. The IP Office can obtain and use the clock signal from any of its digital trunks. Typically the clock signal provided by a digital trunk from the central office exchange is used as this will be the most accurate and reliable clock source.

To do this, the **Clock Quality** setting on each line in the IP Office configuration is set to one of the following:

- **Network**

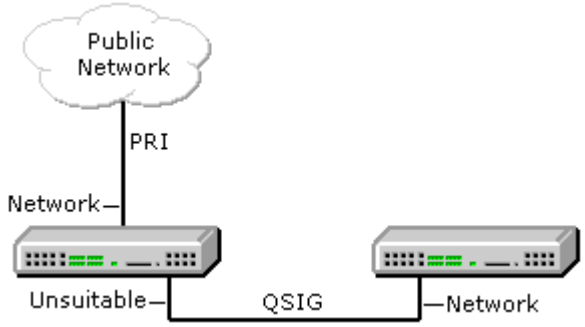
  If available, the clock signal from this trunk should be used as the IP Office clock source for call synchronization. If several trunk sources are set as Network, the IP Office will default to using one as detailed below.
- **Fallback**

  If available, the clock signal from this trunk can be used as the clock source if none of the trunks set as Network are providing a clock source.
- **Unsuitable**

  The clock source from this trunk will never be used as the IP Office clock source.

If no clock source is available the IP Office can use its own internal clock if necessary.

In the example below the first IP Office is set to use the public network trunk as its clock source and ignoring the possible clock source from the QSIG trunk. The other IP Office system is using the clock signal received from the first IP Officeon its QSIG trunk as its clock source. Thus both systems are using the same clock source and that clock source is the public network exchange.



When multiple trunks with the same setting are providing clock signals, trunks are used in the order of slots 1 to 4 and then by port on each slot.

The current clock source being used by an IP Office system is shown on the Resources page within the IP Office System Status Application.

Setting a trunk clock quality setting

About this task

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **Line**.
3. For each digital line, do the following:
   a. Select the line.
   b. On the **Line** tab, select whether that trunk should provide the clock source for the network or whether the trunk is unsuitable.

   Note:

   For E1R2 trunks the **Clock Quality** setting is on the **Advanced** tab
4. Ensure that only one trunk is set to **Network**. This should preferably be a direct digital trunk to the central office exchange.
5. Set one other trunk to **Fallback** in case the selected network trunk connection is lost.

   Note:

   If possible this should be a trunk from a different provider since that reduces the chances of both sources failing at the same time.
6. Ensure that all other digital trunks are set as **Unsuitable**.
7. Click **File > Save Configuration**.

Setting the trunk prefixes

About this task

Where a prefix has been implemented for outgoing calls, that same prefix needs to be added to trunk settings. The prefix is then used as follows:

- On incoming calls the prefix is added to any incoming ICLID received with the call. That allows the ICLID to be used by IP Office phones and applications to make return calls.
- On outgoing calls, the short codes used to route the call to a trunk must remove the dialing prefix.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **Line**.
3. For each line enter the prefix. The location of the relevant setting varies for each trunk type.
   - For analog trunks, select the **Line Settings** tab and enter the prefix in the **Prefix** field.
   - For T1 and T1 PRI trunks, select the **PRI 24 Line** tab and enter the prefix in the **Prefix** field.
   - For BRI, E1 PRI, and QSIG trunks, select the **PRI Line** tab and enter the appropriate prefix in the following fields:
     - Prefix
     - National Prefix
     - International Prefix
4. Click **File > Save Configuration**.

SIP trunk prefixes

The prefix fields Prefix, National Prefix, Country Code and International Prefix are available with the SIP line settings. These fields are used in the following order:

1. If an incoming number (called or calling) starts with the + symbol, the + is replaced with the International Prefix.
2. If the Country Code has been set and an incoming number begins with that Country Code or with the International Prefix and Country Code, they are replaced with the National Prefix.
3. If the Country Code has been set and the incoming number does not start with the National Prefix or International Prefix, the International Prefix is added.
4. If the incoming number does not begin with either the National Prefix or International Prefix, then the Line Prefix is added.

For example, if the SIP line is configured with the following prefixes, the numbers are processed as described in the table below.

- Line Prefix: 9
- National Prefix: 90
- International Prefix: 900
- Country Code: 44

Number Received	Processing	Resulting Number
+441707362200	Following rule 1 above, the + is replaced with the International Prefix (900), resulting in 900441707362200. The number now matches the International Prefix (900) and Country Code (44). Following rule 2 above they are replaced with the National Prefix (90).	901707362200
00441707362200	Following rule 2 above the International Prefix (900) and the Country Code (44) are replaced with the National Prefix (90).	90107362200
441707362200	Following rule 2 above, the Country Code (44) is replaced with the National Prefix (90).	901707362200
6494770557	Following rule 3 above the International Prefix (900) is added.	9006494770557

Configuring the time server

Procedure

1. In IP Office Manager, click the **System** tab.
2. Set the **Time Setting Config Source** value to **SNTP**.
3. In the **Time Settings** area, in **Time Server Address**, set the address of the time server that is used by the enterprise.

   This server is the same time server that Avaya Aura® components in the enterprise are configured to use as their NTP server.

Administration of the IP Office connection to Session Manager

This section provides the procedures required to configure an SM Line between each branch site and the headquarters site. SM Trunk Channel licenses are required to make and receive calls through the SM Line. For more information, see Configuring IP Office to request required licenses from WebLM on page 46.

Also provided in this section is information about how the IP Office uses a configured SM Line to handle incoming and outgoing calls to and from the branch and how a second SM Line can be configured for SM Line redundancy.

- See Enabling SIP trunk support on page 91. Use this procedure to configure the IP Office LAN interface which will be used for the SM Line connection to the Avaya Aura® Session Manager.
- See Setting the branch prefix and local number length for extension numbering on page 92. Use this procedure to set the prefix number for the IP Office and the required extension length.
- See Configuring system-wide security for the SM Line and Centralized phones on page 104. Use this procedure to apply system-wide security settings to the SM Line(s) and Centralized phones.
- See Changing the default codec selection on page 95. Use this procedure to set the preferred order for codec negotiation. This can be done as a system default and also for each individual SIP and SM Line.
- See Adding an SM Line on page 96. Use this procedure to create an SM Line for calls to the Avaya Aura® Session Manager.
- See Setting up outgoing call routing on page 108. Use this procedure to create short codes for routing calls to the SM Line when the required destination or resource is on another branch of the Avaya Aura® network.
- See How the IP Office uses a configured SM Line on page 106. Read this topic to understand how the SM Line is used once it is configured and in operation.
- See SM Line redundancy on page 105. Read this topic to understand how in an Avaya Aura® network that includes multiple SM Lines for redundancy, the IP Office can be configured with a secondary SM Line. If for any reason the IP Office system's primary SM Line goes out of service, the system will automatically attempt to use the secondary SM Line.

Enabling SIP trunk support

About this task

Before adding any SIP trunks, including SM Lines, the IP Office system must be configured for SIP trunk operation. The system has 2 LAN interfaces, LAN1 and LAN2 (the physical ports are labeled LAN and WAN respectively). It is recommended that LAN1 be used for the data connection to the Avaya Aura® network for the SM Line operation.

Important:

The configuration changes in the following procedure will require the IP Office system to be rebooted.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.

2. In the left navigation pane, click **System**.
3. Click the **LAN1** tab.
4. Confirm that the IP address and IP Mask fields are set correctly for the site.
5. Click the **VoIP** tab.
6. Select the **SIP Trunks Enable** option. This is required for Avaya Aura® Session Manager trunk support.

   Note:

   The **SIP Registrar Enable** setting and settings in the **SIP Registrar** tab relate to SIP extension support and therefore do not affect SM Lines. The settings in the **Network Topology** tab relate to external SIP trunks. Those settings are not used by the SM Lines, which use a connection across the customer WAN that does not go through Network Address Translation (NAT).
7. Click **OK**.
8. Select **File > Save Configuration**.

Setting the branch prefix and other fields in the Session Manager System Telephony tab

About this task

Each IP Office in the network must have a unique branch number. That number is added as a prefix to the caller's extension number for calls routed from IP Office user extensions to the Avaya Aura® Session Manager. This means that IP Office user extensions are defined on the IP Office without the branch prefix, so that when the branch prefix is added, the number is the correct length and format expected by Avaya Aura® Session Manager.

The prefix is also used in the Avaya Aura® Session Manager configuration to create unique dial patterns for routing calls to the appropriate IP Office.

You have the option to leave the **Branch Prefix** field blank. If you do not configure the branch prefix, the IP Office user extensions must be defined with the full enterprise number. You are also able to leave the **Local Number Length** field blank.

By default IP Office systems use 3-digit extension numbering starting from 200. The existing allocated numbers can be changed in bulk using the **Tools > Extension Renumber** option. This will add or remove a set value from all existing extension numbers in the configuration.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **System**.
3. Click the **Telephony** tab.
4. Click the **SM** tab.

5. Set the fields as appropriate. For more information, see SM tab field descriptions on page 93.
6. Click **OK**.
7. Click **File > Save Configuration**.

SM tab field descriptions

Name	Range or Default	Description
Short Form Dialing Length	Default = 0 (feature is disabled) Range = 0 to 14	This number specifies the short-form dialing length for all Centralized users and Groups. This feature does not apply to IP Office users. Configuration of this field allows IP Office to treat the last *N* digits (where *N* is the number entered in this field) of each Centralized user's extension number as an alias to that user's extension number. For example, if a Centralized user's extension number is 5381111 and the Short Form Dialing Length is 4, the system will match calls to 1111 with this extension. When 1111 is dialed by another user on the system, entered from the auto-attendant, or comes from the ICR, then in Sunny day that call will be sent to Session Manager with the number converted to 5381111 and in Rainy day it will target the extension 5381111 locally.
Branch Prefix	Range = 0 to 999999999	This number is used to identify the IP Office system within the Avaya Aura® network. The branch prefix of each IP Office system must be unique and must not overlap. For example 85, 861 and 862 are okay, but 86 and 861 overlap. On calls routed via an SM Line, the branch prefix is added to the caller's extension number. You have the option to leave the **Branch Prefix** field blank. If you do not configure the branch prefix, the IP Office user extensions must be defined with the full enterprise number.

Table continues…

Name	Range or Default	Description
Local Number Length	Range = Blank (Off) or 3 to 9 for IP Office user extensions	This field sets the default length for extension numbers for extensions, users, and hunt groups added to the IP Office configuration. Entry of an extension number of a different length will cause an error warning by Manager. The number of digits entered in the **Branch Prefix** field plus the number entered in the **Local Number Length** field must not exceed 15 digits. You have the option to leave the **Local Number Length** field blank.
Proactive Monitoring	Default = 60 seconds, Range = 60 to 100000 seconds	The IP Office sends regular SIP OPTIONS messages to the SM Line in order to check the status of the line. This setting controls the frequency of the messages when the SM Line is currently in service.
Monitoring Retries	Default = 1 Range = 0 to 5	This field sets the number of times the IP Office system attempts to send a SIP OPTIONS request to Session Manager before the SM Line is marked out-of-service.
Reactive Monitoring	Default = 60 seconds, Range = 10 to 3600 seconds	The IP Office sends regular SIP OPTION messages to the SM Line in order to check the status of the line. This setting controls the frequency of the messages when the SM Line is currently out-of-service.
Failback Policy	Default = Auto	This field allows the administrator to choose between an automatic or manual failback policy on the IP Office. In deployments with Centralized phones, this field must be set consistently with the failback policy of the phones which is configured via the Session Manager global settings in System Manager. Choices are: • **Auto** — IP Office automatically brings the SM Line to “In Service” status as soon as it detects via the **Reactive Monitoring** setting that the Session Manager is reachable. • **Manual** — when an SM Line is in the “Out of Service” state, the IP Office does not bring it back to “In Service” status based on automatic detection. IP Office keeps the SM Line in the “Out of Service” state until the administrator manually initiates the IP Office failback from System Manager.

Changing the default codec selection

About this task

By default, all IP Office IP trunks and extensions use automatic codec negotiation. The default negotiation order depends on the type of SD card used.

- With an IPO MU_LAW SD card, the default negotiation order is:
  - G711.MU_LAW
  - G711 A_LAW
  - G729a
  - G723.1
- With an IPO A_LAW SD card, the default negotiation order is:
  - G711.A_LAW
  - G711.MU_LAW
  - G729a
  - G723.1

For more information about codecs, see *Avaya IP Office™ Platform in a Branch Environment Reference Configuration*.

Note:

The specific setting for individual branch trunks and extensions can be set to override the system setting if necessary.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **System**.
3. Click the **Codecs** tab.
4. In the **Available Codecs** section, check the appropriate codecs and move them to the **Selected** section.

   The order of the codecs listed in the **Selected** section indicates the preferred codec order for trunks and extensions that are using automatic codec negotiation. See Automatic codec preference settings on page 96 for more information.
5. Click **OK**.
6. Select **File > Save Configuration**.

Automatic codec preference settings

Setting	Selected Preference	2nd Preference	3rd Preference	4th Preference
G.729	G729(a) 8K CS-ACELP	G711 U-Law 64K	G711 A-Law 64K	G723.1 6K3 MP-MLQ
G.723	G723.1 6K3 MP-MLQ	G729(a) 8K CS-ACELP	G711 U-Law 64K	G711 A-Law 64K
G.711 U-Law	G711 U-Law 64K	G711 A-Law 64K	G729(a) 8K CS-ACELP	G723.1 6K3 MP-MLQ
G.711 A-Law	G711 A-Law 64K	G711 U-Law 64K	G729(a) 8K CS-ACELP	G723.1 6K3 MP-MLQ

Adding an SM Line

About this task

Use this procedure to add an SM Line to the IP Office system configuration. If multiple Avaya Aura®Session Managers are available at the headquarters site, an additional SM Line can be added for SM Line redundancy. The two SM Lines are prioritized based on the line number. The lower line number is considered the primary SM Line. Based on the priority of the SM Lines designated by the line number, the active line to which the IP Office sends all calls will always be the highest priority SM Line in service. See the IP Office Manager online help and SM Line redundancy on page 105 for more information.

Important:

The configuration changes in the following procedure will require the IP Office system to be rebooted.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, right-click **Line**.
3. Select **New > SM Line**.
4. Configure the line settings as appropriate. See Session Manager tab field descriptions on page 97 for more information.
5. Click **OK**.
6. Click the **VoIP** tab.
7. Confirm the **Re-Invite Supported** check box is selected (selected by default).
8. Confirm the **Allow Direct Media Path** check box is selected. This option is selected by default when **Re-Invite Supported** is selected.

9. Configure the remaining fields as appropriate. See VoIP tab field descriptions on page 100 for more information.
10. Click **OK**.
11. Select **File > Save Configuration**.

Session Manager tab field descriptions

Name	Range or Default	Description
Line Number		This value is automatically assigned by IP Office and should be unique for each line added to the configuration.
In Service	Default = Enabled	This option can be used to administratively disable the SM Line. It does not reflect the dynamic state of the line. If an SM Line is administratively disabled, it is not equivalent to being in the dynamic out of service state.
SM Domain Name	Default = Blank	This name should match a SIP domain defined in the Session Manager system's SIP Domains table. Unless there are reasons to do otherwise, all the IP Office systems in the Avaya Aura® network can share the same domain. **Note:** See Viewing the SIP domains on page 174 for a list of SIP domains defined in Session Manager.
SM Address	Default = 0000	Enter the IP address of the Session Manager that the line should use in the Avaya Aura® network. The same Session Manager should be used for the matching Entity Link entry in the Avaya Aura® configuration.
Outgoing Group ID	Default = 98888	This value is not changeable. However note the value as it is used in IP Office short codes used to route calls to the Session Manager.

Table continues…

Name	Range or Default	Description
Prefix	Default = Blank	This prefix will be added to any source number received with incoming calls.
Max Calls	Default = 10	This value sets the number of simultaneous calls allowed between IP Office and Session Manager using this connection. Each call uses one of the available licenses that are shared by all SIP trunks configured in the system.
URI Type	Default = SIP	When SIP or SIPS is selected in the drop-down box, the SIP URI format is used (for example, name@example.com). This affects the From field of outgoing calls. The To field for outgoing calls will always use the format specified by the short codes used for outgoing call routing. Recommendation: When SIP Secured URI is required, the URI Type should be set to SIPS. SIPS can be used only when Layer 4 Protocol is set to TLS.
Media Connection Preservation	Default for new installations and upgrades = Enabled. Choices are: • System • Enabled • Disabled	This feature allows you to choose the media connection preservation capability of established calls for instances when the call signaling over the SM Line is lost due to network failures. When set to **Enabled**, users are able to continue talking even though call features, such as transfer, can no longer be applied on the call due to the loss of the SIP dialog. When set to **System**, the system-wide setting defined in System > Telephony > Telephony tab is used.
Layer 4 Protocol	Default = TLS	This can be set to TLS or TCP. Set to TLS to choose SIPS as the URI Type when SIP Secured URI is required.

Table continues…

Name	Range or Default	Description
Send Port	Default = 5061	When Layer 4 Protocol is set to TLS, the default setting is 5061. When Layer 4 Protocol is set to TCP, the default setting is 5060.
Listen Port	Default = 5061	When Layer 4 Protocol is set to TLS, the default setting is 5061. When Layer 4 Protocol is set to TCP, the default setting is 5060.
Session Timer (seconds)	Default = 1200 seconds Value can be changed in 30-second intervals. **Note:** To avoid extra SIP messages, this value should be *double* the value configured in the **Preferred Minimum Session Refresh Interval (sec)** field in the **add trunkgroup** administration screen for the Communication Manager that the IP Office communicates with via the SM Line.	This value sets the Session expiry time. At the half-way point of the expiry time, a session refresh message is sent. This value can also be changed to **On Demand**. When set to **On Demand**, IP Office does not initiate the session timer and only supports it if it is initiated by the other end. **Note:** Communication Manager R6.2 SP1 and later supports SIP session refresh via UPDATE. This is compatible with the session timer enhancement on the IP Office, which makes IP Office initiate session refreshes. However, if the Communication Manager that the IP Office communicates with via the SM Line is an earlier release, then this field should be set to **On Demand** and not to a numeric value.

VoIP tab field descriptions

Name	Range or Default	Description
Codec Selection	Default = System Default	This field defines the codec or codecs offered during call setup. When System Default is selected, the codec list shown matches the codecs set in the system-wide Default Codec Selection (System > Codecs).
Fax Transport Support	Default = None	This option is only selectable if the option **Re-Invite Supported** is also selected. If enabled, the IP Office is able to support the sending and receiving of faxes via the SM Line using the T38 protocol. The settings for T38 are set on the T38 Fax tab.
Location	Default = Cloud	This field is not relevant to IP Office enterprise branch deployments.
Call Initiation Timeout(s)	Default = 4 seconds	This option sets how long the system would wait for a response to its attempt to initiate a call over the SM Line.
DTMF Support	Default = RFC2833	This setting is used to select the method by which DTMF key presses are signaled to the remote end. The supported options are **In Band**, **RFC2833** or **Info**.
VoIP Silence Suppression	Default = Off	When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods.

Table continues…

Name	Range or Default	Description
Allow Direct Media Path	Default = On	This setting controls whether connected calls must remain routed via IP Office or can be routed alternately if possible within the network structure. • If enabled, connected calls can take routes other than through IP Office. This removes the need for a voice compression channel. • If disabled or not supported at one end of the call, the call is routed through IP Office. However RTP relay support allows calls between devices using the same audio codec to not require a voice compression channel.
Re-Invite Supported	Default = On	When enabled, **Re-Invite** can be used during a session to change the characteristics of the session, for example when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk.

Table continues…

Name	Range or Default	Description
Codec Lockdown	Default = Off	Supports RFC 3264 Section 10.2 when **Re-Invite Supported** and **Codec Lockdown** are enabled. In response to a SIP offer with a list of codecs supported, some SIP user agents supply a SDP answer that also lists multiple codecs. This means that the user agent may switch to any of those codecs during the session without further negotiation. The system does not support multiple concurrent codecs for a session, so loss of speech path will occur if the codec is changed during the session. If codec lockdown is enabled, when the system receives an SDP answer with more than one codec from the list of offered codecs, it sends an extra re-INVITE using just a single codec from the list and resubmits a new SDP offer with just the single chosen codec.
Force direct media with phones	Default = Off	This setting is enabled when **Allow Direct Media Path** and **Re-Invite Supported** check boxes are checked. This feature allows digit presses on the extension to be detected and the call changed to an indirect media call so the RFC2833 DTMF can be sent. The call remains as a direct media call for 15 seconds after the last digit before reverting back to being an indirect media call.

Table continues…

Name	Range or Default	Description
Media Security	Default = Same as System	Secure RTP (SRTP) can be used between IP devices to add additional security. These settings control whether SRTP is used for the SM Line. Choices are: • **Same as System** — Calls on the SM Line use the Media Security settings configured at the System level on the IP Office. • **Disable** — Media security is not required. All media sessions (audio, video, and data) will be enforced to use RTP only. • **Best Effort** — Attempt to use secure media first and if unsuccessful, fall back to non-secure media. • **Enforce** — Media security is required. All media sessions (audio, video, and data) will be enforced to use SRTP only.
Media Security Options		This section appears when **Media Security** is set to **Best Effort** or **Enforce**. The following options appear in this section: • Encryptions • Authentication • Replay Protection SRTP Window Size • Crypto Suites
Encryptions	Default = RTP	This setting allows selection of which parts of a media session should be protected using encryption. The default is to encrypt just the RTP stream (the speech).

Table continues…

Name	Range or Default	Description
Authentication	Default = RTP and RTCP	This setting allows selection of which parts of a media session should be protected using authentication. The default is to authenticate both the RTP stream (the speech) and the RTCP stream (call control signals).
Replay Protection SRTP Window Size	Default = 64	Displays the options for the SRTP window size. Currently not adjustable.
Crypto Suites	Default = SRTP_AES_CM_128_SHA1_80	AES_CM_128_SHA1_80 is enabled by default. SRTP_AES_CM_128_SHA1_32 is supported but not enabled by default.

Configuring media security

About this task

In IP Office, the system-wide security settings apply to the SM Lines, SIP extensions of Centralized users, and the trunks and extensions of IP Office users. The system-level settings can be overridden for individual trunks or extensions in special cases. It is recommended to use the *Same as System* configuration for the trunks and extensions. The SM Lines and the extensions of all Centralized users must have a consistent media security configuration.

Note:

For more information about Centralized users and Centralized phones, see *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **System**.
3. Click the **VoIP Security** tab.

   The following fields are relative to setting the system-wide security:

   - Media Security
   - Media Security Options
   - Encryptions
   - Authentication
   - Replay Protection SRTP Window Size

- Crypto Suites

4. Set the fields as appropriate. See VoIP tab field descriptions on page 100 for more information.

   Note:

   In IP Office R9.0, SRTP was supported only for traffic across the SM Line or with Centralized users. If an IP Office, on which SRTP is enabled, is upgraded, the existing IP Office R9.0 SRTP configuration is copied automatically to the individual configuration of each SM Line and Centralized SIP extension. This keeps the existing behavior unchanged during upgrades. Therefore, to take advantage of the broader support for SRTP, you should enable SRTP at the IP Office system-level configuration. You should also set the configuration of the SM Lines and individual Centralized SIP extensions to *Same as System*, which is the default setting for new installations.

5. Click **OK**.
6. Select **File** > **Save Configuration**.

SM Line redundancy

In an Avaya Aura® network that includes multiple SM Lines for redundancy, the IP Office can be configured with a secondary SM Line. If for any reason the IP Office system's primary SM Line goes out of service, the system will automatically attempt to use the secondary SM Line. Prioritization of the SM Lines is determined by the line number configured for a particular SM Line. For example, if the first SM Line is configured with line number 17 and the second SM Line is configured with line number 18, then line number 17 has the higher priority and is considered the primary SM Line. If for some reason you want to designate the secondary SM Line as the primary line, you must change one or both of the line numbers associated with the SM Lines so that the secondary SM Line number is lower than that of the primary line.

The redundancy operation of the SM lines is based on line prioritization. The active line to which IP Office sends all calls is always the highest priority SM Line in service. If the primary SM Line is in service, it is the active line for sending calls. If the connection to the primary SM Line is lost, causing IP Office to switch to the secondary SM Line, when the primary line comes back up, IP Office will switch back to the primary line.

The secondary SM Line is configured in the same way as the primary SM Line. The only difference required is to set the **SM Address** field to the address of the alternate Avaya Aura®Session Manager from the one being used by the primary SM Line.

Note:

Depending on how the IP Office failback policy is configured, failback from the secondary Session Manager to the primary Session Manager may need to be performed manually when the primary Session Manager comes back into service. For more information, see “About the failback policy” in *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*.

If all available channels of the current SM Line are in use, the IP Office will not overflow calls to the other SM Line. However, if PSTN trunk fallback has been configured, the other SM Line will be used. See PSTN trunk fallback on page 209 for more information.

How the IP Office uses a configured SM Line

Once configured and in operation, the SM Line is used as follows.

Outgoing calls from a branch

In a Distributed enterprise branch, if the outgoing call begins with the branch's own prefix, the prefix is removed and the call is targeted locally to the matching native user or hunt group extension number. If there is no matching extension number, the call is targeted to any matching system short code.

Incoming calls to a branch

Incoming calls on an SM Line are treated as being internal calls and do not go through the IP Office system's Incoming Call Route settings.

- If the destination of the incoming call on the SM Line starts with the system's branch prefix, the prefix is removed. The call is then targeted to the matching IP Office user or hunt group extension number. If there is no matching extension number, the call is targeted to any matching system short code.
- If the destination of the incoming call on the SM Line does not start with the system's branch prefix, the whole number is checked for a match against system short codes.

Line status detection

The IP Office system sends regular OPTION 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 OPTION 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 OPTION 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.

Different ways to set up outgoing call routing

You are able to use IP Office short codes to configure outgoing call routing to enterprise extension numbers in other sites within the enterprise network. The short codes are used to route the calls to the SM Line. The Avaya Aura® Session Manager then performs the routing to determine where the

call should go. The best way to configure the short codes for outgoing call routing for a deployment depends on the enterprise numbering, dial plan, and call routing requirements.

Ideally the number of system short codes should be kept to a minimum and the same short codes used on all branches in order to ease maintenance. This is where using a uniform dial plan for all branches helps, as explained in Dial plan considerations on page 30. A uniform dial plan allows the same single short code to be used at all branches.

Examples

The following examples show different approaches for configuring outgoing call routing.

- **Configuration based on common first digit** — If the enterprise numbers start with a common first digit, then a short code can be configured based on that common first digit. For example, `8XXXXXX | Dial | 8N | 98888`
- **Configuration based on common first digit with different length numbers** — If the enterprise numbers start with a common first digit but are different lengths, then a short code could be based on that common first digit and numbers of different lengths. For example, `8N; | Dial | 8N | 98888` (with Dial Delay Count = 0 and Dial Delay Time = 4 seconds).
- **Configuration based on explicit match for calls to local trunks and sending everything else to the SM Line** — Configure a default short code, for example `? | Dial | . | 50:Main`, that sends the calls to ARS, and then in ARS use a default entry, such as `? | Dial | . | 98888` to send to the SM Line anything that does not match other entries in the ARS. In this example, explicit entries are required in the ARS for calls that must be routed to the PSTN through local trunks.
  - If the end users dial an access digit for outside line to PSTN, then the ARS can contain an entry that will match that access digit and route to the local trunks.
  - Alternatively, the ARS can contain entries that will match the numbers that have to be routed to the local trunks, for example, the local area code.

  Warning:

  The configuration of routing to the SM Line via ARS should not be used when IP Office is deployed within a particular contact center scenario. That scenario is one where IP Office sends calls to Avaya Aura® Experience Portal, which then blind transfers the call to CC-Elite agents, requiring IP Office to copy information known as UUI to a new SIP message. IP Office does not function correctly in this call flow when routing to the SM Line is configured via ARS.

  Hence, in deployments that include this contact center scenario, configure routing to the SM Line directly from short codes. The variation on the example above would be as follows: .
  - Configure the default short code `? | Dial | . | 98888` to send anything that does not match other short codes to the SM Line.
  - Configure explicit short codes to match all calls that must be routed to local trunks and send those calls to ARS.
- **Configuration based on explicit match for calls to the SM Line and sending everything else to local trunks** — Configure explicit short codes to match calls to other sites within the enterprise and send them to the SM Line. Configure a default short code that sends to ARS anything that does not match other short codes. This approach is the opposite of the previous

approach. Which of these two approaches to use depends on the enterprise numbering and dial plan. The enterprise numbering and dial plan will determine which list of explicit match entries is easier to identify and configure.

- **Configuration in ARS to send calls to other enterprise sites via the PSTN when the SM Line is down** — In some cases, ARS with alternate routing can be configured to automatically route calls to other enterprise sites to the PSTN during Rainy day. This configuration is simple if the enterprise extension numbers are the same as their corresponding DID numbers as dialed on the PSTN. In this case alternate routing can send the dialed number as is to the PSTN trunk. In other cases, if the enterprise extension numbers have corresponding DID number but in a different format, it may be possible to adapt the dialed numbers to corresponding PSTN numbers by specifying number manipulation in the alternate route ARS short code.

  To configure routing calls to other enterprise sites via the SM Line with alternate routing via the PSTN:

  - Short codes must send the calls to the main ARS.
  - Within the main ARS, short codes as described above must route the calls to the SM Line.
  - The alternate route in the main ARS must specify another ARS form for PSTN trunk fallback.
  - Within the PSTN trunk fallback ARS, the short codes must route the calls to local PSTN trunks on the IP Office, possibly with some number manipulation.

  Warning:

  The configuration of routing to the SM Line via ARS should not be used when IP Office is deployed within a particular contact center scenario, as described in the previous **Warning** above.

Note:

IP Office also allows for the flexibility of optionally configuring a domain name in the **Telephone Number** field of a short code that routes to the SM Line. In this case, the domain name specified in the short code is used in the SIP message sent to the SM Line, instead of the domain name that is specified in the SM Line configuration. This optional capability is not expected to be used for the regular case of routing to the SM Line.

Setting up outgoing call routing

About this task

Use this task to create a short code for outgoing call routing. For information about the different short codes that can be created to route outgoing calls in different ways, see Different ways to set up outgoing call routing on page 106.

Note the following:

- If using Avaya Aura® Conferencing, the IP Office short code must include routing to Session Manager any call that is made to the Avaya Aura® Conferencing number.

- In a Distributed enterprise branch, when a short code match occurs and the telephone number to be sent to the SM Line begins with the IP Office system's own branch prefix, the prefix is removed and the call is re-targeted locally on the IP Office system.
- For information on routing back to the branch for fallback alternate routes, see Branch PSTN call routing examples on page 204.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **Short Code**.
3. Click the **New** icon and select **Short Code**.
4. Configure the settings as appropriate. See Short Code tab field descriptions on page 109 for more information.
5. Click **OK**.
6. Click **File > Save Configuration**.

Short Code tab field descriptions

Name	Description
Code	Enter the number dialed by users that should be matched to this short code. Use **X** wildcards for any single digit.
Feature	Leave this field set as **Dial**.
Telephone Number	Set this field to match a number that should be passed to the Avaya Aura®Session Manager for routing against its dialing pattern matches. The **N** wildcard can be used to match any wildcards in the **Code**. **Note:** Add `SS` to the entry in this field to have the caller ID passed to the SM Line. For example, if you are entering `8N` in the Telephone Number field, enter `8NSS`.
Line Group Id	Set the **Line Group ID** to match the **Outgoing Group** settings used in the SM lines URI setting.
Local	Features that transfer the caller to Voicemail Pro can indicate the language locale required for prompts. This is subject to the language being supported and installed on the voicemail server. The default is blank.

Table continues…

Name	Description
Force Account Code	When selected, for short codes that result in the dialing of a number, the user is prompted to enter a valid account code before the call is allowed to continue. The default is **Off**.

Defining the media connection preservation system default setting

About this task

This setting defines the media connection preservation setting for SM Lines and SIP trunks whose **Media Connection Preservation** field is set to **System**. This feature allows for preservation of the media connection of established calls for instances when the call signaling over the SM Line is lost due to network failures. When set to **Enabled**, users are able to continue talking even though call features can no longer be applied on the call due to the loss of the SIP dialog.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **System**.
3. Click the **Telephony > Telephony** tab.
4. In the **Media Connection Preservation** drop-down box, select one of the following:
   - **Enabled** — media connection of established calls is preserved if call signaling over the SM Line is lost due to network failures.
   - **Disabled** — media connection of established calls is not preserved if call signaling over the SM Line is lost due to network failures.
5. Click **OK**.

Enabling branch SIP extension support

About this task

Before adding any SIP extensions, the IP Office system must be enabled for SIP extension support. Use this procedure to configure the IP Office to support the addition of SIP extensions.

Important:

The configuration changes in the following procedure will require the IP Office system to be rebooted.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **System**.
3. Click the **LAN1** tab.
4. In the **LAN Settings** tab, make a note of the IP Address and IP Mask details as these will be required during the SIP extension configuration.
5. Click the **VoIP** tab.
6. Ensure the check box for **SIP Registrar Enable** is checked (it is checked by default). This is necessary for support of SIP extensions directly by the branch or when providing survivability support for Avaya Aura® SIP extensions.
7. Configure the remaining fields on the **VoIP** tab as appropriate. See VoIP tab field descriptions on page 111 for more information.
8. Click **OK**.
9. Select **File > Save Configuration**.

VoIP tab field descriptions

Name	Default	Description
H.323 Gatekeeper Enable	Default = On	This setting enables gatekeeper operation.

Table continues…

Name	Default	Description
Auto-create Extn	Default = Off	This feature is disabled for IP Office enterprise branch systems that are configured for System Manager administration or WebLM centralized licensing. For IP Office systems under System Manager administration, all users and extensions for VoIP users are created by System Manager. The feature is disabled to avoid creation of extensions that System Manager is not aware of. For IP Office systems that are administered for WebLM centralized licensing, this feature is disabled because of potential conflict with acquiring the licenses required for new extensions from the WebLM server.
Auto-create User	Default = Off	This feature is disabled for IP Office enterprise branch systems that are configured for System Manager administration or WebLM centralized licensing. For IP Office systems under System Manager administration, all users and extensions for VoIP users are created by System Manager. The feature is disabled to avoid creation of extensions that System Manager is not aware of. For IP Office systems that are administered for WebLM centralized licensing, this feature is disabled because of potential conflict with acquiring the licenses required for new extensions from the WebLM server.

Table continues…

Name	Default	Description
Remote Extn Enable	Default = Off	When **H.323 Gatekeeper Enabled** is selected, this option is available. The system can be configured to support remote H.323 extensions in the case where NAT is used in the connection path. See the IP Office Manager Help page for more information.
SIP Trunks Enable	Default = On	This setting enables support of SIP trunks.
SIP Registrar Enable	Default = On	This setting enables support of SIP extensions.
Auto-create Extn/User	Default = Off	This feature is disabled for IP Office enterprise branch systems that are configured for System Manager administration or WebLM centralized licensing. For IP Office systems under System Manager administration, all users and extensions for VoIP users are created by System Manager. The feature is disabled to avoid creation of extensions that System Manager is not aware of. For IP Office systems that are administered for WebLM centralized licensing, this feature is disabled because of potential conflict with acquiring the licenses required for new extensions from the WebLM server.
SIP Remote Extn Enable	Default = Off	
Domain Name	Default = Blank	This is the local SIP registrar domain name that will be needed by SIP devices in order to register with the IP Office. If this field is left blank, registration is against the LAN IP address. For our examples we have been using a domain, **example.com**.

Table continues…

Name	Default	Description
Layer 4 Protocol	Default = UDP, TCP • UDP, SIP port = 5060 • TCP, SIP port = 5060 • TLS, SIP port = 5061	This is the transport protocol for SIP traffic between the IP Office and SIP extension devices. TLS is disabled by default.
Challenge Expiry Time (sec)	Default = 10	The challenge expiry time is used during SIP extension registration. When a device registers, the SIP Registrar will send a challenge back to the device and waits for an appropriate response. If the response is not received within this timeout the registration is failed.
Port Number Range, Minimum	Default = 49152 Range = 1024 to 65280	This sets the lower limit for the RTP port numbers used by the system. See the IP Office Manager Help for more information about this feature.
Port Number Range, Maximum	Default = 53246 Range = 1278 to 65534	This sets the upper limit for the RTP port numbers used by the system. See the IP Office Manager Help for more information about this feature.
Port Number Range (NAT), Minimum		
Port Number Range (NAT), Maximum		
Enable RTCP Monitoring on Port 5005	Default = On	For 9600 Series H.323 phones, the system can collect VoIP QoS data from the phones. For other phones, including non-IP phones, it can collect QoS data for calls if they use a VCM channel. The QoS data collected by the system is displayed by the System Status application.
Keepalives, Scope	Default = Disabled	

Table continues…

Name	Default	Description
DiffServ Settings		When transporting voice over low speed links, it is possible for normal data packets to prevent or delay voice packets from getting across the link. This can cause unacceptable speech quality. It is therefore important that all traffic routers and switches in a network have some form of Quality of Service (QoS) mechanism. QoS routers are essential to ensure low speech latency and to maintain sufficient audible quality. See the IP Office Manager Help for more information about this feature.
Primary Site Specific Option Number (SSON)	Default = 176 Range = 128 to 254	An SSON is used as part of DHCP to request additional information. See the IP Office Manager Help for more information about this feature.
Secondary Site Specific Option Number (SSON)	Default = 242 Range = 128 to 254	An SSON is used as part of DHCP to request additional information. See the IP Office Manager Help for more information about this feature.
VLAN	Default = Not Present	This option is applied to H.323 phones using the system for DHCP support. If set to **Disabled**, the L2Q value indicated to phones in the DHCP response is 2 (disabled). If set to **Not Present**, no L2Q value is included in the DHCP response.
1100 Voice VLAN Site Specific Option Number (SSON)	Default = Blank	This is the SSON used for responses to 1100/1200 Series phones using the system for DHCP

Table continues…

Name	Default	Description
1100 Voice VLAN IDs	Default = Blank	For 1100/1200 Series phones being supported by DHCP, this option sets the VLAN ID that should be provided if necessary. Multiple IDs (up to 10) can be added, each separated by a + sign.

Managing VMPro system configuration templates

Adding a VMPro System Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro System Configuration Template**.
3. Click **New**.
4. Complete the **Name** and **Version** fields.
5. Click **Details**.

   The system launches the **VMPro** application.
6. In the right pane, complete the system configuration template by filling the required fields, and click **Update**.
7. Click **Save and Exit** to save the template specifications and exit the **VMPro** application.

   The system displays the VMPro System Configuration page where you can view the newly created system configuration template.

Viewing a VMPro System Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro System Configuration Template**.
3. On the VMPro Template page, from the **VMPro** supported templates list, select a **VMPro** system type.
4. Click **Show List**.

5. Select the system configuration template you want to view from the **VMPro** System Configuration list.
6. Click **View**.

   The system launches the **VMPro** application.
7. On the VMPro window, in the right pane, you can view the system configuration template details. All the fields are read-only.

Editing a VMPro System Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro System Configuration Template**.
3. On the VMPro System Configuration Templates page, select a VoicemailPro system type.
4. Click **Show List**.
5. Select the system configuration template you want to edit from the VMPro System Configuration list.
6. Click **Edit**.

   The system launches the VMPro application.
7. To edit the configuration parameters on the Voicemail Pro-System Preferences window, click **Update**.
8. Click **OK**.
9. Click **File** > **Save and Exit** to save the modifications to the system configuration template and exit the VMPro application.

   The system displays the VMPro System Configuration Template page.

Deleting a VMPro System Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro System Configuration Template**.
3. On the VMPro System Configuration Templates page, select a **VMPro** system type.
4. Click **Show List**.
5. Select the system configuration template you want to delete from the VMPro System Configuration Template list.
6. Click **Delete**.

The system displays the system template instance you selected for deletion.

7. Do one of the following:
   - Click **Delete** to delete the template.
   - Click **Cancel** to cancel the delete operation, and return to the VMPro System Configuration Template landing page.

Applying a VMPro System Configuration template on a device

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro System Configuration Templates**.
3. On the VMPro System Configuration Template page, select a Voicemail Pro system type.
4. Click **Show List**.
5. From the VMPro System Configuration Templates List, select the system template you want to apply to a VMPro device.
6. Click **Apply**.

   The system displays the VMPro System Configuration page where you can select a device to apply the template.
7. From the list of VMPro devices, select the VMPro device on which you want to apply the VMPro system configuration template.

   Important:

   When you apply a template on a device, the data of the template that you apply might override the existing system configuration data on the device.
8. Do one of the following:
   - Click **Now** to perform apply the template immediately.
   - Click **Schedule** to apply the template at a specified time in **Scheduler**.
   - Click **Cancel** to cancel this task and return to the VMPro System Configuration Template landing page.

Duplicating a VMPro System Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro System Configuration Template**.
3. On the VMPro System Configuration Templates page, select a VoicemailPro system type.

4. Click **Show List**.
5. From the VMPro System Configuration list, select the system configuration template that you want to duplicate.
6. Click **Duplicate**.

   The system launches the VMPro application.
7. In the **New Template Name** field, type the name of the new template.
8. Click **Commit**.

   The system displays the new template on the VMPro System Configuration Templates page.

VMPro System Configuration Templates field descriptions

Name	Description
Name	The name of the Voicemail Pro template.
Version	The version number of the template.
Last Modified Time	The date and time when the IP Office Voicemail Pro template was last modified.

Button	Description
Details	Displays the IP Office Voicemail Pro application where you can add or edit the template details.

Managing VMPro call flow template

Adding a VMPro Call Flow template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro Call Flow Template**.
3. Click **New**.
4. Complete the **Name** and **Version** fields.
5. Click **Details**.

   The system launches the **VMPro** application.

6. In the right pane, complete the call flow template by filling the required fields, and click **Update**.
7. Click **Save and Exit** to save the template specifications and exit the **VMPro** application.

Result

The system displays the VMPro Call Flow page where you can view the newly created call flow template.

Viewing a VMPro Call Flow template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro Call Flow Template**.
3. On the VMPro Template page, from the **VMPro** supported templates list, select the **VMPro** system type.
4. Click **Show List**.
5. Select the system configuration template you want to view from the **VMPro** call flow list.
6. Click **View**.

Result

The system launches the **VMPro** application. On the VMPro window, in the right pane, you can view the call flow template details. All the fields are read-only.

Editing a VMPro Call Flow template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro Call Flow Template**.
3. On the VMPro Call Flow Templates page, select a VoicemailPro system type.
4. Click **Show List**.
5. Select the call flow template you want to edit from the VMPro Call Flow list.
6. Click **Edit**.

   The system launches the VMPro application.
7. To edit the call flow parameters on the Voicemail Pro-System Preferences window, click **Update**.
8. Click **OK**.

9. Click **File** > **Save and Exit** to save the modifications to the call flow template and exit the VMPro application.

Result

The system displays the VMPro Call Flow Templates page.

Deleting a VMPro Call Flow template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro Call Flow Template**.
3. On the VMPro Call Flow Templates page, select a **VMPro** system type.
4. Click **Show List**.
5. Select the call flow template you want to delete from the VMPro Call Flow Templates list.
6. Click **Delete**.

   The system displays the VMPro call flow template that you selected for deletion.
7. Do one of the following:
   - Click **Delete** to delete the template.
   - Click **Cancel** to cancel the delete operation, and return to the VMPro Call Flow Templates page.

Applying a VMPro Call Flow template on a device

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro Call Flow Templates**.
3. On the VMPro Call Flow Templates page, select the Voicemail Pro system type.
4. Click **Show List**.
5. From the VMPro Call Flow Templates List, select the system template you want to apply to a VMPro device.
6. Click **Apply**.

   The system displays the VMPro Call Flow page where you can select a device to apply the template.
7. From the list of VMPro devices, select the VMPro device on which you want to apply the VMPro call flow template.

Important:

When you apply a template on a device, the data of the template that you apply might override the call flow data on the device.

8. Do one of the following:
   - Click **Now** to apply the template immediately.
   - Click **Schedule** to apply the template at a specified time in **Scheduler**.
   - Click **Cancel** to cancel the task and return to the VMPro Call Flow Templates page.

Duplicating a VMPro Call Flow template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro Call Flow Template**.
3. On the VMPro Call Flow Templates page, select a VoicemailPro system type.
4. Click **Show List**.
5. From the VMPro Call Flow list, select the call flow template that you want to duplicate.
6. Click **Duplicate**.

   The system launches the VMPro application.
7. In the **New Template Name** field, type the name of the new template.
8. Click **Commit**.

Result

The system displays the new template on the VMPro Call Flow Templates page.

VMPro Call Flow Templates field descriptions

Name	Description
Name	The name of the Voicemail Pro template.
Version	The version number of the template.
Last modified time	The last time that the IP Office Voicemail Pro template was modified.

Button	Description
Details	Displays the template details of the IP Office Voicemail Pro application.

Adding Unified Communications Module or Application Server manually

About this task

You can integrate the Unified Communications Module (UCM) or Application Server with System Manager manually through **Inventory**.

Before you begin

The administrator must provide details of the device, such as the IP Address, device type, device version, and SNMP Profile.

Procedure

1. To add a new Application Server, from **Home** > **Services** > **Inventory** > **Manage Elements** > **New Elements**, set the **Type** to **IP Office UCM** or **IP Office Application Server**.
2. Click **Commit**.
3. In the Add Unified Communication Module/ Application Server window, from the **SNMP** tab, type the name of the Application Server in the **Name** field.
4. In the **Description** field, type the description of the Application Server.
5. In the **Node** field, type the node address.
6. From the **Device Type** drop-down field, select one of the following devices:
   - Unified Communications Module
   - **IP Office Application Server**
7. From the **Device Version** drop-down field, select the latest release number.
8. In the **Service Login** field, type **BranchAdmin**.
9. In the **Service Password**, type the password.
10. In the **Confirm Service Password** field, confirm the password.
11. Click **Commit**.

Adding a UCM and Application Server Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **UCM and Application Server Configuration**.
3. On the UCM and Application Server Templates page, in the **Templates List** section, click **New**.
4. Complete the **Name**, **System Type**, and **Version** fields.

5. Click **Details**.

   The system launches the IP Office Manager application.

6. On the Offline Configuration Creation window, click **OK**.
7. In the right pane, complete the system configuration template by filling the required fields, and click **OK**.
8. Click **File** > **Save Template and Exit** to save the template specifications and exit the IP Office Manager application.

   The system directs you to the UCM and Application Server Templates landing page where you can view the newly created system template in the **UCM and Application Server Templates** list.

Viewing a UCM and Application Server Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **UCM and Application Server Configuration**.
3. On the UCM and Application Server Templates page, in the **Supported System Types** section, select one of the following system types:
   - IP Office Application Server
   - Unified Communications Module
4. Click **Show List**.
5. Select the system configuration template you want to view from the **UCM and Application Server Templates** list.
6. Click **View**.

   On the IP Office Manager window, in the right pane, you can view the system configuration template details. All the fields are read-only.

   The system starts the IP Office Manager application.

7. Click **File** > **Exit** to exit IP Office Manager.

   The system displays the UCM and Application Server Templates page where you can select a device to apply the template.

Editing a UCM and Application Server Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation page, click **UCM and Application Server Configuration**.

3. On the UCM and Application Server Templates page, In the **Supported System Types** section, select any one of the following system types:
   - IP Office Application Server
   - Unified Communications Module
4. Click **Show List**.
5. Select the system configuration template you want to edit from the UCM and Application Server Templates list.
6. Click **Edit**.

   The system launches the IP Office Manager application.
7. On the IP Office Manager window, edit the required configuration parameters, and click **OK**.
8. Click **File** > **Save Template and Exit** to save the modifications to the system configuration template and exit the IP Office Manager application.

   The system displays the UCM and Application Server Templates landing page.

Deleting a UCM and Application Server Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **UCM and Application Server Configuration**.
3. On the UCM and Application Server Templates page, In the **Supported System Types** section, select one of the following system types:
   - IP Office Application Server
   - Unified Communications Module
4. Click **Show List**.
5. Select the system configuration template you want to delete from the UCM and Application Server Templates list.
6. Click **Delete**.

   The system displays the system template instance you selected for deletion.
7. Do one of the following:
   - Click **Delete** to delete the template.
   - Click **Cancel** to cancel the delete operation, and return to the UCM and Application Server Templates landing page.

Applying a UCM and Application Server Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **UCM and Application Server Configuration**.
3. On the UCM and Application Server Templates page, In the **Supported System Types** section, select one of the following system types:
   - IP Office Application Server
   - Unified Communications Module
4. Click **Show List**.
5. From the UCM and Application Server Configuration List, select the system template you want to apply to a device.
6. Click **Apply**.

   You will be directed to a new page where you can select a device to apply the template.
7. From the list of IP Office devices, select the IP Office device on which you want to apply the selected UCM and Application Server Configuration template.

   Important:

   When you apply a template on a device, the data of the template that you wish to apply may override the existing system configuration data on the device.
8. Do one of the following:
   - Click **Now** to perform apply the template immediately.
   - Click **Schedule** to apply the template at a specified time in **Scheduler**.
   - Click **Cancel** to cancel this task and return to the UCM and Application Server Templates landing page.

UCM and Application Server Templates field descriptions

Name	Description
Name	The name of the system configuration template of UCM and Application Server.
System Type	The type of system associated with the template. The options are: • **Unified Communications Module**: For UCM core unit • **Application Server**: For Application Server core unit

Table continues…

Name	Description
Version	The version number of the template.
Last Modified Time	The date and time when the UCM and Application Server System Configuration template was last modified.

Button	Description
Details	Displays the application where you can add or edit the template details.

Chapter 6: Configuration

Voicemail configuration

This section provides the procedures to configure the voicemail system that the IP Office system will use. If Embedded Voicemail or Voicemail Pro are configured, see one of the following documents for information on how to configure user mailboxes, hunt group mailboxes, and auto attendants:

- *Avaya IP Office Implementing Embedded Voicemail*
- *Avaya IP Office Implementing Voicemail Pro*

Voicemail options

The following IP Office voicemail options are supported:

Local voicemail options

IP Office systems deployed as Distributed or stand-alone enterprise branches can be configured to use the following local voice mail options:

- **Embedded Voicemail** — Embedded Voicemail is the IP Office default voicemail option. It uses the system SD card in the IP Office system control unit for storage of prompts and messages. Embedded Voicemail supports mailboxes for all local extension numbers, announcements to waiting callers, and auto attendants (up to 40) for external calls. The capacity is limited to 15 hours of recorded messages, prompts and announcements.
- **Voicemail Pro** — Voicemail Pro runs on an external server connected to IP Office or on Unified Communications Module and provides a wide range of features. Voicemail Pro supports 40 voice channels, which includes:
- Message/greeting recording
- Message playing
- System/custom IVR prompt playing
- Call recording and prompt playing to outcalls made from VoicemailPro

Mailbox messages, greetings, recordings, and announcements are stored locally on Unified Communications Module or on a standalone computer where Voicemail Pro is running. Management of the Voicemail Pro call flows in the branches can be done from a remote central Voicemail Pro client. Use of the Voicemail Pro client to remotely manage the calls flows is available only when Voicemail Pro is running on an external server, not when it is deployed on Unified Communications Module. The Voicemail Pro client can also connect to Voicemail Pro that

runs the Unified Communications Module server and can therefore, be used in the management. For enterprise branch deployments with multple Voicemail Pro servers, the Voicemail Pro client provides an export or import feature that allows the same Voicemail Pro configuration including call flows to be deployed on multiple Voicemail Pro servers.

Note:

If the IP Office 500v2 systems are present in the enterprise deployment with System Manager, you can manage Voicemail Pro callflow.

Voicemail Pro is the only option that supports manual call recording for IP Office users and automatic call recording for the IP Office system.

Note:

If security of signaling links is a concern, the Voicemail Pro application should run on a co-resident Unified Communications Module blade. Security enhancements such as TLS are not applicable to links with external servers running Voicemail Pro. You can now manage Voicemail Pro from Avaya Aura® System Manager.

The local voicemail options can be configured only in Distributed enterprise branch deployments where there are only IP Office users. They cannot be configured in Centralized or Mixed enterprise branch deployments with Centralized users. Only one type of voicemail system can be configured for an IP Office branch. This does not preclude the use of local auto-attendant in Centralized or Mixed enterprise branch deployments.

Centralized voicemail options

IP Office systems deployed in Distributed, Mixed, or Centralized enterprise branch environments can be configured to use the following Centralized voicemail options. Stand-alone branches cannot use Centralized voicemail systems.

- **Avaya Aura Messaging** — An IP Office system can be configured to use Avaya Aura® Messaging as its voicemail server when Session Manager is used as the core SIP router.
- **Modular Messaging** — An IP Office system can be configured to use Modular Messaging as its voicemail server when Session Manager is used as the core SIP router.

When a central voicemail system is configured for the branch, the mailboxes of the branch users are on the central voicemail system. However, you still have the option to use the automated attendant of the IP Office local Embedded Voicemail or the call flows of a local Voicemail Pro, even though the embedded voicemail or Voicemail Pro are not used for the voicemail messages of the branch users. This configuration requires the use of Embedded Voicemail or Voicemail Pro port licenses. If the configuration requires more ports than the number of ports that are licensed and come with the IP Office system, additional port licenses are required.

When Messaging or Modular Messaging is used as the central voicemail system, IP Office users and Centralized users in Rainy day can leave and retrieve voicemail over the PSTN when the SM Lines are unavailable. DTMF digits are used to indicate a specific mailbox. Message Waiting Indication is not provided.

Related links

Voicemail considerations on page 33

About the Park and Page feature

The Park and Page feature is supported when the system voicemail type is configured as Embedded Voicemail or Voicemail Pro. Park and Page is also supported on systems where Avaya Aura® Messaging or Modular Messaging is configured as the central voicemail system and the local Embedded Voicemail provides auto attendant operation, or Voicemail Pro provides customized call flow actions created for the mailbox.

The Park and Page feature allows a call to be parked while a page is made to a hunt group or extension. A caller can press a digit and the call is parked while an announcement is made to a paging zone, overhead paging system, or both. The page is repeated based on how the feature is configured until the parked call is picked up or the park timeout occurs. If the park timeout occurs, the caller hears the Park and Page error prompt and is then returned to the call flow that initiated the Park and Page and hears either the subscriber's personal greeting or the auto attendant main menu prompt.

The Park and Page feature can also be configured to automatically send an unanswered call to an auto attendant. When configured in this way, the caller is provided with a message, then the call is automatically parked, and a page is issued to notify that the call needs to be picked up. When the automatic Park and Page feature is configured, their is no action required by the caller or an operator.

The called party can use a short code or a programmed button on their phone to park and unpark incoming calls. For more information about short codes and button programming, see the Manager on-line help. The called party can also use the **Conference** button or the **Answer** soft key on their phone while the Page is occurring.

The procedure to configure Park and Page is provided in the following documents:

- *Avaya IP Office, Administering Voicemail Pro*
- *Avaya IP Office Administering Embedded Voicemail*

Configuring IP Office to use Embedded Voicemail

About this task

Embedded Voicemail is the default voicemail configuration for IP Office. It provides basic voicemail mailbox operation and auto-attendant operation without requiring a separate voicemail server computer.

If you are using WebLM centralized licensing, in addition to performing this task, you must also configure IP Office to request the required number of Embedded Voicemail licenses from the WebLM server. See Configuring IP Office to request required licenses from WebLM on page 46 for more information.

For more information about Embedded Voicemail including information on how to configure user mailboxes, hunt group mailboxes, and auto attendants, see *Avaya IP Office Implementing Embedded Voicemail*.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **System**.
3. Click the **Voicemail** tab.
4. In the **Voicemail Type** drop-down box, select **Embedded Voicemail**.

   Note:

   Fields applicable to this mode of voicemail support are enabled. If the field is not applicable, the field is disabled.

5. In the **Voicemail Mode** drop-down box, select either **IP Office Mode** or **Intuity Mode**.

   The mode selected determines which key presses the end users will use for mailbox functions. End users should be provided with the appropriate mailbox user guide for the mode selected. For more information, see the IP Office Manager on-line help

6. If you want the users to be presented with a display menu for access to their mailbox, check the **Messages Button Goes to Visual Voice** check box. For more information, see the IP Office Manager on-line help.
7. In the **Minimum Password Length** field, use the up and down arrows to set the appropriate minimum password length.
8. In the **Maximum Record Time (secs)** field, use the up and down arrows to set the maximum record time in seconds for recorded announcement and auto attendant prompts. messages and prompts.
9. In the **Reception/Breakout (DTMF 0)** drop-down box, select the number to which a caller is transferred if they press **0** while listening to the mailbox greeting rather than leaving a message. Do one of the following:
   a. To configure Park and Page for this DTMF breakout, select **Park & Page** and then do the following:
      a. In the **Paging Number** drop-down box, select the appropriate hunt group of user extension.
      b. In the **Retries** field, use the up and down arrows to set the number of times to repeat the page.
      c. In the **Retry Timeout** field, use the up and down arrows to set the amount of time to elapse before the page is repeated. This time is set in 15-second increments.
   b. To configure a user extension for this DTMF breakout, select the appropriate user extension number from the **Reception/Breakout (DTMF 0)** drop-down box.
   c. To configure a group extension for this DTMF breakout, select the appropriate group extension number from the **Reception/Breakout (DTMF 0)** drop-down box.
   d. To configure the main extension for this DTMF breakout, select **Main** from the **Reception/Breakout (DTMF 0)** drop-down box.

10. For the **Breakout (DTMF 2)** drop-down box, repeat step 9.
11. For the **Breakout (DTMF 3)** drop-down box, repeat step 9.
12. In the **SIP Name** field, enter the appropriate name.
13. In the **SIP Display Name (Alias)** field, enter the appropriate name.
14. In the **Contact** field, enter the appropriate name.
15. Configure the **Anonymous** check box as appropriate. This feature is enabled when this check box is selected.

    Note:

    For more information about the fields in the SIP Settings section, see the IP Office Manager on-line help.

Voicemail Pro configuration from IP Office

About this task

The IP Office system can be configured to use Voicemail Pro. Voicemail Pro runs on a Windows or Linux server connected to IP Office. If security of signaling links is a concern, the Voicemail Pro application must run on a co-resident UCM blade. Security enhancements such as TLS are not applicable to links with external servers running Voicemail Pro.

If you are using WebLM centralized licensing, in addition to performing this task, you must also configure IP Office to request the required number of Voicemail Pro licenses from the WebLM server. See Configuring IP Office to request required licenses from WebLM on page 46 for more information.

Note:

There can be multiple Voicemail Pro servers in an IP Office deployed in an enterprise branch environment. If multiple Voicemail Pro servers are installed:

- Upgrades can be performed through the Web control or IP Office shell where a remote connection to Web control over https is feasible for each Voicemail Pro server.
- Backups can be performed through the Voicemail Pro client. The Voicemail Pro client must connect to each Voicemail Pro server. It can be configured to store backups at a central location by setting up SFTP.
- Restores can be performed through the Voicemail Pro client. The Voicemail Pro client must connect to each Voicemail Pro server. It can be configured to restore from backups at a central location by setting up SFTP.

For the procedures to perform upgrades, backups, and restores as well as procedures to configure user mailboxes, hunt group mailboxes, and auto attendants, see:

- *Avaya IP Office, Implementing Voicemail Pro*
- *Avaya IP Office, Administering Voicemail Pro*(Windows server installation)
- *Avaya IP Office, IP Office Application Server, Installation and Maintenance* (Linux server installation)

Note:

Centralized management of call flows on the Voicemail Pro servers deployed in an IP Office enterprise branch environment is not supported. The Voicemail Pro client is used to perform administration of the user call flows and prompts. Using the Voicemail Pro client, common or customized call flows and prompts can be configured for all Voicemail Pro users and hunt groups on the system. For more information, see Call flow management for Voicemail Pro servers in IP Office enterprise branch deployments on page 135.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **System**.
3. Click the **Voicemail** tab.
4. In the **Voicemail Type** drop-down box, select **Voicemail Lite/Pro**.

   Note:

   The **Voicemail Lite/Pro** option is used for Voicemail Lite or Voicemail Pro. Fields applicable to this mode of voicemail support are enabled. If the field is not applicable, the field is disabled.
5. If you want the users to be presented with a display menu for access to their mailbox, select **Messages Button Goes to Visual Voice**.

   For more information, see the IP Office Manager online help.
6. In **Voicemail IP Address**, enter the IP address of the Linux server where Voicemail Pro is installed.
7. In **Backup Voicemail IP Address**, enter the IP address of the backup voicemail server.

   An additional server can be set up but left unused. If contact to the voicemail server specified in the **Voicemail IP Address** field is lost, responsibility for voicemail services is temporarily transferred to this backup server address.
8. To configure the **Voicemail Channel Reservation** feature, do the following:
   a. In **Auto-Attendant**, set the number of channels reserved for users accessing mailboxes to collect messages.
   b. In **Announcements**, set the number of channels reserved for announcements.

      When no channels are available, calls continue without announcements.
   c. In **Voice Recording**, set the number of channels reserved for voice recording other than mandatory voice recording.

      When no channels are available, recording does not occur (although recording progress may be indicated).
   d. In **Mandatory Voice Recording**, set the number of channels reserved for mandatory voice recording.

When no channels are available for a call set to mandatory recording, the call is barred and the caller hears busy tone.

e. In **Mailbox Access**, set the number of channels reserved for users accessing mailboxes to collect messages.

Note:

For more information about the fields in the Voicemail Channel Reservation section, see the IP Office Manager online help.

9. In **Reception/Breakout (DTMF 0)**, select the number to which a caller is transferred if they press **0** while listening to the mailbox greeting rather than leaving a message, and then do the following:
   a. To configure Park and Page for this DTMF breakout, select **Park & Page** and then do the following:
      a. In **Paging Number** , select the appropriate hunt group of user extension.
      b. In **Retries**, use the up and down arrows to set the number of times to repeat the page.
      c. In **Retry Timeout**, use the up and down arrows to set the amount of time to elapse before the page is repeated. This time is set in 15-second increments.
   b. To configure a user extension for this DTMF breakout, select the appropriate user extension number from the **Reception/Breakout (DTMF 0)** drop-down box.
   c. To configure a group extension for this DTMF breakout, select the appropriate group extension number from the **Reception/Breakout (DTMF 0)** drop-down box.
   d. To configure the main extension for this DTMF breakout, select **Main** from the **Reception/Breakout (DTMF 0)** drop-down box.
10. For the **Breakout (DTMF 2)** drop-down box, repeat step 9.
11. For the **Breakout (DTMF 3)** drop-down box, repeat step 9.
12. In **SIP Name**, enter the appropriate name.
13. In **SIP Display Name (Alias)**, enter the appropriate name.
14. In **Contact**, enter the appropriate name.
15. Configure the **Anonymous** check box as appropriate.

Note:

This feature is enabled when this check box is selected. For more information about the fields in the SIP Settings section, see the IP Office Manager online help.

16. To configure the **Call Recording** feature, do the following:
    a. In **Auto Restart Paused Recording (sec)**, enter the appropriate number of seconds. If recording of a call is halted using the Pause Recording button, this timer determines when recording is restarted if the button is not pressed again.

b. Configure the **Hide Auto Recording** check box as appropriate. This feature is enabled when this check box is checked. During call recording by Voicemail Pro, some Avaya phones display REC or something similar to show that the call is being recorded. When this feature is enabled, this recording indication is suppressed.

Call flow management for Voicemail Pro servers in IP Office enterprise branch deployments

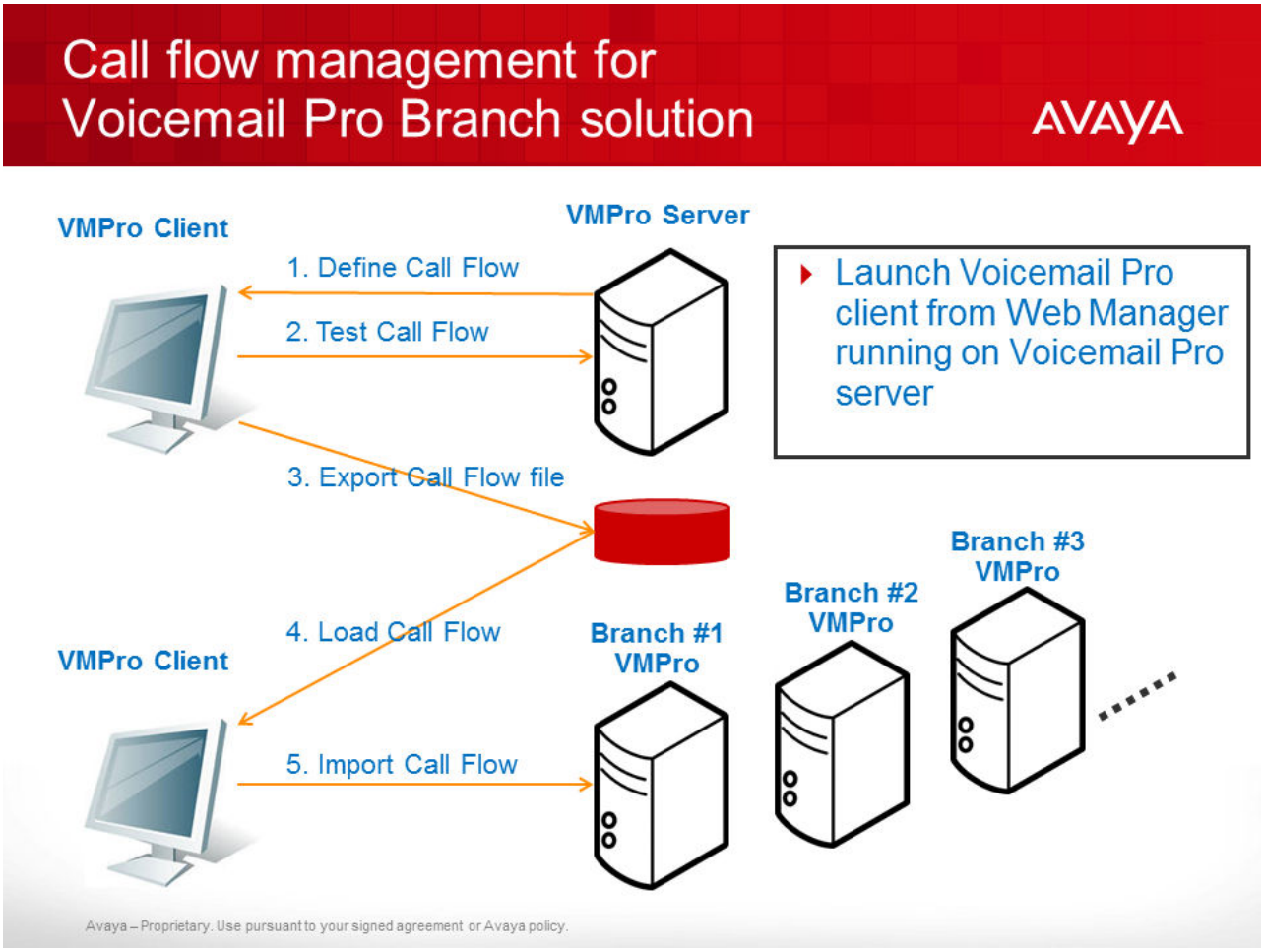
For enterprise branch deployments with multple Voicemail Pro servers, the Voicemail Pro client provides an export/import feature that allows the same Voicemail Pro configuration (including call flows and prompts) to be deployed on multiple Voicemail Pro servers. This prevents the administrator from having to design the same call flow and prompts at each node on every Voicemail Pro server in the enterprise branch deployment.

To support the call flow management, Web Manager provides an option to launch the Voicemail Pro client via an applet in offline mode. An export/import wizard is provided to facilitate the export of the call flow configuration file from a Voicemail Pro server to the Voicemail Pro client where the call flow configuration is imported to other Voicemail Pro servers in the enterprise branch deployment.

Note:

Voicemail Pro can be installed on a Linux server or Windows server. However, launching the Voicemail Pro client in offline mode and using the export/import feature for call flow management is available on Web Manager only on the IP Office Application Server deployment of Voicemail Pro which is deployed on a Linux server. The offline mode and export/import feature for call flow management is not available on Web Manager for IP Office Server Edition deployments of Voicemail Pro.

Other features, such as Park and Page and security enhancements are available on both the Windows and Linux versions of Voicemail Pro.



Importing a call flow configuration file

Before you begin

Define and test call flows on a Voicemail Pro server and export the entire configuration (system settings, callflows, and prompts) as a **.tar.gz** file.

About this task

Use this task to deploy a pre-defined Voicemail Pro configuration on multiple Voicemail Pro servers in an enterprise branch deployment.

Procedure

1. Launch your browser and go to the Avaya IP Office Web Manager.
2. In the **User Name** field, enter your user name.
3. In the **Password** field, enter your password.

   Note:

   The default user name and password is `Administrator`.

4. Click the drop-down arrow next to **Application Server** and select **Launch Voicemail Pro**.
5. If prompted **Do you want to Continue?**, click **Continue**.
6. In the **Security Warning** dialog box, click the check box for **I accept the risk and want to run this application**, and click **Run**.

   The Voicemail Pro client is launched in Web Offline mode.
7. Import the **.tar.gz** configuration file on the Voicemail Pro server as follows:
   a. Click **File > Import or Export**.
   b. In the **Import or Export Data** dialog box, select **Import Data** and click **Next**.
   c. In the **Import Data from which file?** field, browse to and select the exported configuration archive you want to import.
   d. Click **Open**.
   e. In the **Import Data** dialog box, click **Next**.
   f. Click **Finish**.
8. Click **File > Save & Make Live**.
9. In the **Confirm** dialog box, click **Yes**.

   The call flow configuration file is imported and made live on the Voicemail Pro server in the enterprise branch deployment.
10. Repeat this task for each Voicemail Pro server in the enterprise branch deployment.

Configuring IP Office to use Avaya Aura® Messaging

About this task

The IP Office system can be configured to use Avaya Aura® Messaging as its voicemail server.

In addition to performing this task, you must also configure IP Office to request the required number of SIP Sessions licenses from the WebLM server. See Configuring IP Office to request required licenses from WebLM on page 46 for more information.

Note:

When Avaya Aura® Messaging is used as the central voicemail system, you are able to still use the local Embedded Voicemail for auto attendant operation and announcements to waiting calls or you can use Voicemail Pro for customized call flow actions created for the mailboxes. If you do use either of these voicemail systems, you must also configure IP Office to request the required number of Embedded Voicemail licenses or Voicemail Pro licenses, depending on which you use, from the WebLM server.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.

2. In the left navigation pane, click **System**.
3. Click the **Voicemail** tab.
4. In the **Voicemail Type** drop-down box, select **Avaya Aura Messaging**.

   Note:

   Fields applicable to this mode of voicemail support remain enabled.

5. If you want the users to be presented with a display menu for access to their mailbox, check the **Messages Button Goes to Visual Voice** check box. For more information, see the IP Office Manager on-line help.
6. For the **Use local system for AA and Announcements or Call Flows** drop-down box, do one of the following:
   a. To enable the local IP Office system features for Embedded Voicemail auto attendants and announcements, in the **Use local system for AA and Announcements or Call Flows** drop-down box, select **Embedded**.

      Note:

      The announcements are those that the callers hear when the call in on hold. You must also enable the announcements. Do this by selecting the check box for **Announcements On** which appears when you select **Hunt Group > Announcements** tab and **Users > Announcements** tab.

   b. To enable the local IP Office system to use the Voicemail Pro call flows where customized actions are created for the mailbox, in the **Use local system for AA and Announcements or Call Flows** drop-down box, select **Voicemail Pro**.
7. In the **AAM Number** field, enter the extension number configured for mailbox access to the Avaya Aura® Messaging system. Note that this number is automatically routed via the active SM Line. It does not need to be routed through the normal branch call routing.
8. In the **AAM PSTN Number** field, enter the PSTN number to which you want to reroute attempts to access mailboxes when the SM Line(s) are out of service. (This field is optional.)

   When calls to access voicemail are routed by this method, the calls go through the PSTN trunk that is configured on the IP Office.

   Note:

   The PSTN voicemail number requires a corresponding Short Code entry so that the calls are routed to the correct line during Rainy day operation.

9. For the **Enable Voicemail Instructions Using DTMF** check box, do one of the following:
   a. To send the voicemail instructions as DTMF tones, ensure the **Enable Voicemail Instructions Using DTMF** check box is selected (that is, checked).

      When this check box is selected, the voicemail mail box number of the recipient and the appropriate digit(s), such as # or ## that are used to leave or collect a message,

are automatically sent as DTMF tones so the caller does not need to enter those digits.

b. To require the caller to dial the user's voicemail mail box to send the required DTMF digits, do not select this check box (that is, the check box is not checked).

The capability to turn this feature off is provided because there may be networks where the DTMF digits may not correctly reach the messaging system due to a provider's network characteristics. When this feature is turned off, the DTMF digits are not automatically sent. Instead, the caller will dial the user's mail box number to manually send the required DTMF digits to access the mailbox.

10. In the **Maximum Record Time (secs)** field, use the up and down arrows to set the maximum recording length in seconds for recorded announcement and auto attendant prompts.

Note:

You can set a number in this field only if you selected one of the two voicemail options in the **Use local system for AA and Announcements or Call Flows** drop-down box.

11. Click **OK**.
12. Select **File** > **Save Configuration**.

Configuring IP Office to use Modular Messaging

About this task

The IP Office system can be configured to use Modular Messaging as its voicemail server.

In addition to performing this task, you must also configure IP Office to request the required number of SIP Sessions licenses from the WebLM server. See Configuring IP Office to request required licenses from WebLM on page 46 for more information.

Note:

When Modular Messaging is used as the central voicemail system, you are able to still use the local Embedded Voicemail for auto attendant operation and announcements to waiting calls or you can use Voicemail Pro for customized call flow actions created for the mailboxes. If you do use either of these voicemail systems, you must also configure IP Office to request the required number of Embedded Voicemail licenses or Voicemail Pro licenses, depending on which you use, from the WebLM server.

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **System**.
3. Click the **Voicemail** tab.
4. In the **Voicemail Type** drop-down box, select **Modular Messaging over SIP**.

Note:

Fields applicable to this mode of voicemail support remain enabled.

5. If you want the users to be presented with a display menu for access to their mailbox, check the **Messages Button Goes to Visual Voice** check box. For more information, see the IP Office Manager on-line help.
6. For the **Use local system for AA and Announcements or Call Flows** drop-down box, do one of the following:
   a. To enable the local IP Office system features for Embedded Voicemail auto attendants and announcements, in the **Use local system for AA and Announcements or Call Flows** drop-down box, select **Embedded**.

      Note:

      The announcements are those that the callers hear when the call in on hold. You must also enable the announcements. Do this by selecting the check box for **Announcements On** which appears when you select **Hunt Group > Announcements** tab and **Users > Announcements** tab.

   b. To enable the local IP Office system to use the Voicemail Pro call flows where customized actions are created for the mailbox, in the **Use local system for AA and Announcements or Call Flows** drop-down box, select **Voicemail Pro**.
7. In the **MM Number** field, enter the extension number configured for mailbox access to the Modular Messaging system. Note that this number is automatically routed via the active Avaya Aura®Session Manager line. It does not need to be routed through the normal branch call routing.
8. In the **MM PSTN Number** field, enter the PSTN number to which you want to reroute attempts to access mailboxes when the Avaya Aura®Session Manager line(s) are out of service. (This field is optional.)

   This number needs to be a valid DID number from the branch to the Modular Messaging system. When calls to access voicemail are routed by this method, the caller will be prompted by Modular Messaging to indicate the action they are performing (leaving or collecting messages) and the target mailbox.

   Depending on the call routing being used by the branch system for external PSTN calls, you may need to do additional configuration to ensure that this number is routed via a branch PSTN trunk. See Modular Messaging and Avaya Aura Messaging PSTN Fallback on page 141 for more information.
9. For the **Enable Voicemail Instructions Using DTMF** check box, do one of the following:
   a. To send the voicemail instructions as DTMF tones, ensure the **Enable Voicemail Instructions Using DTMF** check box is selected (that is, checked).

      When this check box is selected, the voicemail mail box number of the recipient and the appropriate digit(s), such as # or ## that are used to leave or collect a message, are automatically sent as DTMF tones so the caller does not need to enter those digits.

b. To require the caller to dial the user's voicemail mail box to send the required DTMF digits, do not select this check box (that is, the check box is not checked).

   The capability to turn this feature off is provided because there may be networks where the DTMF digits may not correctly reach the messaging system due to a provider's network characteristics. When this feature is turned off, the DTMF digits are not automatically sent. Instead, the caller will dial the user's mail box number to manually send the required DTMF digits to access the mailbox.

10. In the **Maximum Record Time (secs)** field, use the up and down arrows to set the maximum recording length in seconds for recorded announcement and auto attendant prompts.

    Note:

    You can set a number in this field only if you selected one of the two voicemail options in the **Use local system for AA and Announcements or Call Flows** drop-down box.

11. Click **OK**.
12. Select **File > Save Configuration**.

Modular Messaging and Avaya Aura Messaging PSTN Fallback

When the branch is configured to use Modular Messaging over SIP or Avaya Aura Messaging for its voicemail services, that configuration includes setting an internal Modular Messaging or Avaya Aura Messaging number (800700 for the following example) for calls to Modular Messaging or Avaya Aura Messaging which are automatically routed via the SM Line.

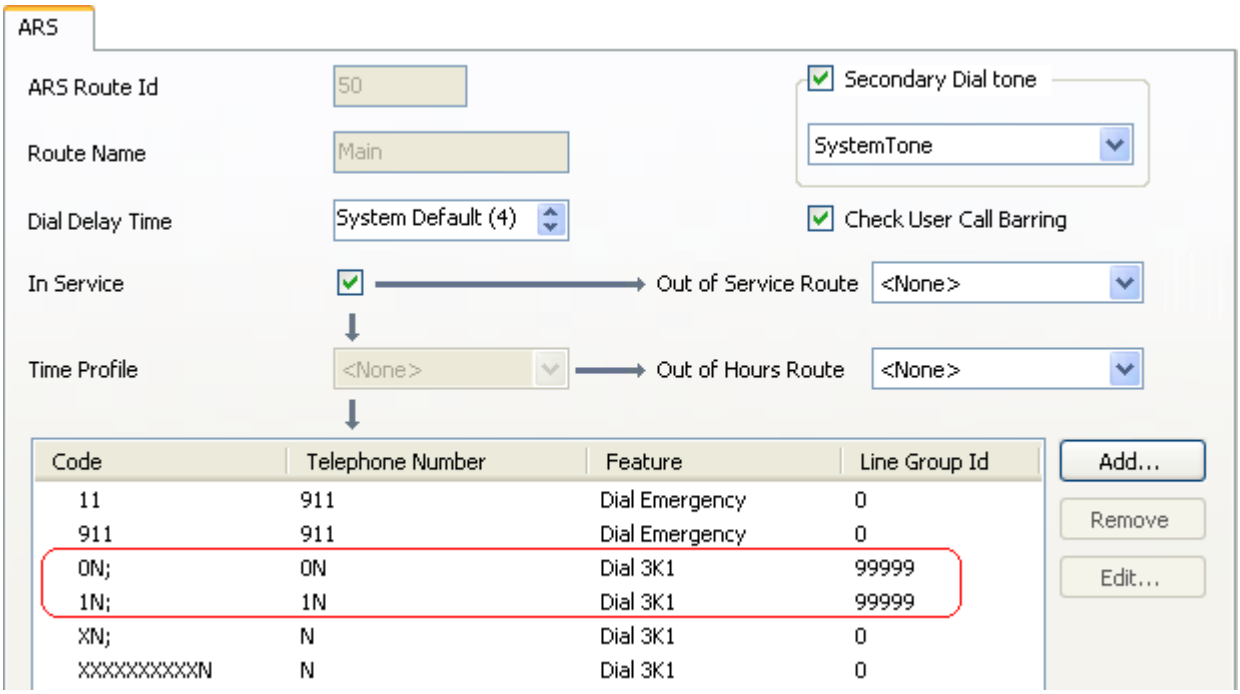
An additional Modular Messaging or Avaya Aura Messaging PSTN number can also be configured for use when the SM Line is not in service (915553800701 for the following example). However, it may also require additional configuration to ensure that this number is correctly routed to a branch PSTN trunk. That could be done using a system short code, but doing it in the ARS form keeps all the branch PSTN call routing in one place for ease of maintenance.

Adding an overriding short code

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **ARS**.

3. Click **50: Main**.



Within the ARS form, the default **1N;** short code is the one used for national calls. It would match the MM PSTN Number or AAM PSTN Number and attempt to route it to the SM Line which we know is out of service if the MM PSTN Number or AAM PSTN Number is being used for calls to voicemail. We can change the routing by adding a specific short code for the MM PSTN Number or AAM PSTN Number.

4. To add a short code, click the **Add...** button.
5. Make the changes as follows:
   a. In the **Code** field, set this to match the external PSTN number for Modular Messaging or Avaya Aura Messaging without the external dialing prefix.
   b. In the **Feature** drop-down box, select **Dial3K1**.
   c. In the **Telephone Number** field, set this to **N** to match the whole number in the **Code** field.

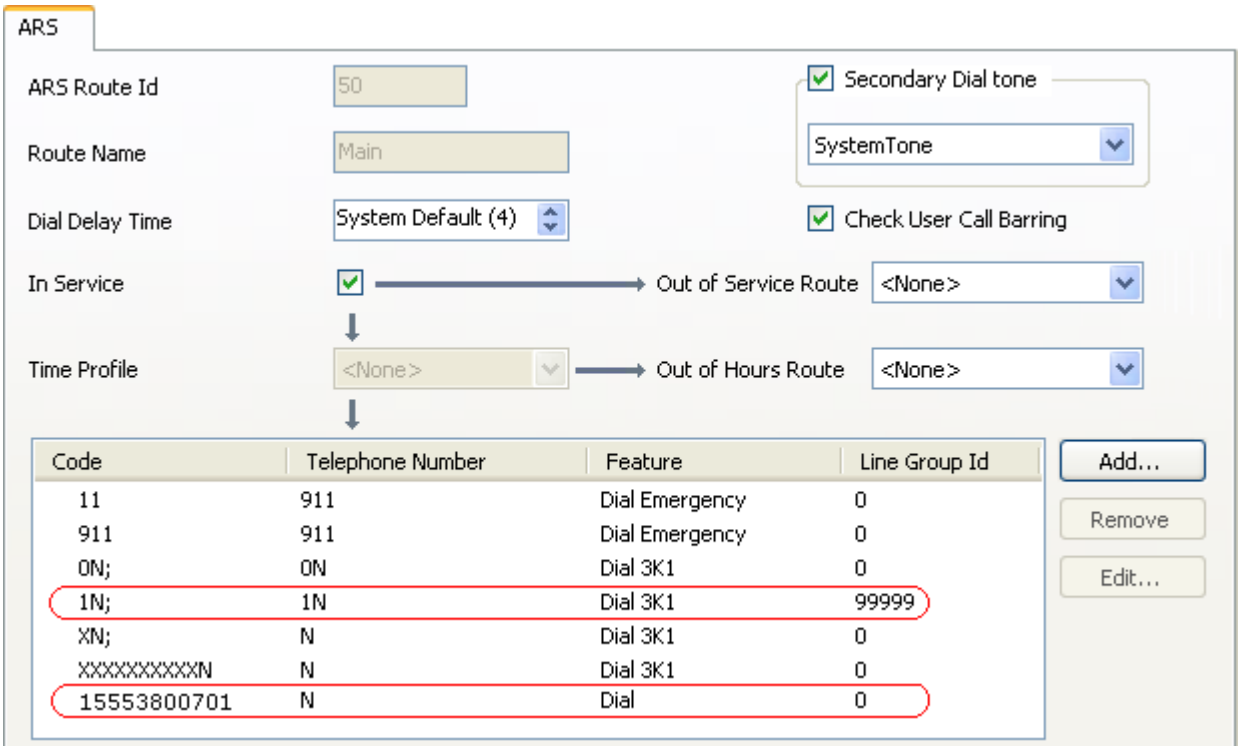
      Note:

      For a setup where the voicemail mail box numbers configured on Modular Messaging or Avaya Aura Messaging are the same as the caller's DID, the short code to route the PSTN call should be configured so that the caller ID is withheld. To do this, enter a `W` in the **Telephone Number** field of the short code. This ensures that during Rainy day operation, the voicemail system does not automatically go to the voicemail mail box of the caller based on the caller ID.

   d. In the **Line Group Id** drop-down box, select the line group ID being used for the branch's PSTN trunks. The default is 0.

6. Click **OK**.

   The ARS now has two short codes that will potentially match external national calls. However, one is a more exact match for certain calls and therefore will be applied to those calls.



7. Click **OK**.
8. Click **File > Save Configuration**.

Uploading an auto attendant audio file

About this task

You are able to upload and convert audio files to System Manager that can be used in the IP Office system configuration auto attendant feature. Once uploaded, from IP Office Manager you are able to select the audio files from the Auto Attendant page. For more information about the field options in System Manager, see *Avaya Aura® System Manager Online Help*.

Note:

If you are using a system template, you can add the audio file to the template to push the audio file down to multiple IP Office systems.

Procedure

1. From the System Manager console, under **Services**, select **Templates**.
2. On the **Templates** page, click **IP Office System Configuration**.

3. On the **IP Office System Configuration Templates** page, under **Templates List**, select **More Options > Manage Audio**.
4. On the **Manage Audio** page, click the **Browse** button to locate the .WAV file you want to upload.
5. Click the **Upload** button.

   The voice file is uploaded to System Manager in the .C11 format that is required for Embedded Voicemail on IP Office systems. The file is automatically converted from the .WAV format to the .C11 format.
6. When finished, click the **Done** button.

IP Office management configuration from System Manager

This section provides tasks to configure IP Office systems that are managed from System Manager.

Related links

Using System Manager File Transfer to load files to the IP Office system on page 144
Viewing an IP Office system configuration from System Manager on page 145
IP Office system configuration field descriptions on page 148

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*.

Related links

IP Office management configuration from System Manager on page 144

Viewing an IP Office system configuration from System Manager

About this task

Use this procedure to edit an IP Office system configuration using different browsers.

Procedure

1. From 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 **View**.
   - For Mozilla Firefox browser (all supported versions), and IP Office version 11.0 onwards, IP Office Web Manager application launches.
   - For Internet Explorer 11.x browser, and IP Office version 11.0 onwards, IP Office Web Manager application launches. for IP Office earlier to 11.0 versions IP Office Manager application launches.
5. Edit the IP Office system configuration.

Related links

IP Office management configuration from System Manager on page 144

Editing an IP Office system configuration from System Manager

Before you begin

Avaya Aura® System Manager has been set up to launch IP Office Manager. See Setting up System Manager to launch IP Office Manager on page 38.

About this task

Use this procedure to edit an IP Office system configuration using different browsers.

Note:

You cannot configure users when editing an IP Office system configuration from System Manager. User configuration is performed from System Manager User Management. For more information, see Restrictions when editing an IP Office system configuration from System Manager on page 147.

Procedure

1. From 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**.
   - For Mozilla Firefox browser (all supported versions), and IP Office version 11.0 onwards, IP Office Web Manager application launches.
   - For Internet Explorer 11.x browser, and IP Office version 11.0 onwards, IP Office Web Manager application launches. for IP Office earlier to 11.0 versions IP Office Manager application launches.

   Note:

   - If the IPOAdminLite.exe file has not been downloaded to the System Manager server, an error message appears that says **The system cannot find the file specified**. If you receive this message, click **OK**. Then see Manually transferring the IPOAdminLite.exe file to the System Manager server on page 38 for the procedure to install the IPOAdminLite.exe file on the System Manager server.
   - If this is the first time you are attempting to edit an IP Office device through System Manager from this computer, and IP Office Manager has not yet been installed on this computer, the following message appears:

     IP Office Manager is not installed on this machine. To complete the current task, you must download and install IP Office Manager. After you complete this installation restart the machine. Refer to the Release Notes/Online help.

Do you want to download IP Office Manager from the server now?

If you receive this message, click **Yes**. Then go to step 4 in Installing IP Office Manager from the System Manager server to your computer on page 42 for the procedure to install IP Office Manager on the computer.

5. Edit the IP Office system configuration as appropriate.
6. To edit the system configuration for another IP Office system, repeat steps 1 through 5.

Note:

You cannot edit the system configuration of multiple IP Office systems from a single instance of IP Office Manager. You must open a new **IP Office** tab from the System Manager console and open another instance of IP Office Manager for that IP Office device.

Restrictions when editing an IP Office system configuration from System Manager

When you edit the system configuration of an IP Office device that is managed fromSystem Manager, IP Office Manager is launched in system mode. The following restrictions apply when editing an IP Office system configuration from System Manager with IP Office Manager in system mode.

- **Extension** is visible in the **Extn** tab only but is disabled.
- All users (other than **NoUser** and **RemoteManager**) are visible in the **User** tab only but are disabled.
- **NoUser** has **User** and **Source Number** tabs visable and editable.
- **RemoteManager** has the **User** tab visable and editable. The rest of the tabs are not visable and therefore not editable.

The User Management feature available in System Manager is used to manage users and extensions on IP Office systems that are centrally managed from System Manager. See User administration on page 190 for more information.

Note:

Do not use IP Office Manager that is connected directly to the IP Office device to edit users and extensions on systems that are centrally managed from System Manager. Changes made to users and extensions in this way will not be synced back to System Manager.

For more information about the two management methods, that is, central management from System Manager or local management from IP Office Manager, see Management on page 15. Do not use both of these management methods to configure and manage users and extensions on an IP Office system.

System Manager does not support the configuration of User Rights on IP Office systems. Similar functionality of applying selected user settings to groups of users is available from the System Manager user template capability.

IP Office system configuration field descriptions

Name	Description
Device Name	The name of the IP Office device.
IP Address	The IP address associated with the IP Office device.
System Type	The type of system associated with the IP Office device. The valid options are: • **IP Office**: for IP Office core unit • **IP Office Select**: for IP Office Select core unit
Last Operation on Device	The operation that has been performed last on the device.
Status	The status of the operation that is currently running or was last run.
System Configuration Template	The current IP Office System Configuration template that exists on the IP Office device.
Last Modified Time of System Configuration	The date and time you last modified the system configuration.
Last Backup Time	The date and time when you last performed a backup.

Buttons

Name	Description
View	Click to view the IP Office system configuration field descriptions.
Edit	Click to edit the IP Office system configuration field descriptions.
Download	Click to download the IP Office system configuration field descriptions.

About disabling the System Manager administration feature for an IP Office

If the IP Office is centrally managed by System Manager and you want to administer the IP Office using IP Office Manager that is directly connected to the branch, for example to install an individual PLDS license file, you must first disable the System Manager administration feature for the branch. Disabling the System Manager administration feature for a branch can be performed from System Manager or from IP Office Manager if the network connection to System Manager is not available.

After you disable the System Manager administration feature for a branch and administer the branch using IP Office Manager, you must synchronize the IP Office with System Manager to synchronize the changes and return the System Manager administration feature for the branch to the enabled state.

Related links

Disabling the System Manager administration feature for the branch from IP Office Manager on page 149
Disabling the System Manager administration feature for the branch from System Manager on page 149
Synchronizing IP Office with System Manager on page 151

Disabling the System Manager administration feature for the branch from System Manager

Procedure

1. From the System Manager console, under **Elements**, click **IP Office**.
2. On the **IP Office Element Management** page, in the left navigation pane, click **Security Configuration**.
3. On the **IP Office Security Configuration** page, click the radio button for the appropriate branch.
4. Click **Edit**.
5. In the **Security Settings** pane, select **Services > Configuration**.
6. Click the **Service Details** tab.
7. In the **Service Access Secure** drop-down box, select **Unrestricted**.

   Note:

   To be able to use IP Office Manager to administer the branch, **Unrestricted** must be selected.
8. Click **OK**.
9. Click **File > Save Configuration**.

Disabling the System Manager administration feature for the branch from IP Office Manager

Procedure

1. Start IP Office Manager.
2. Select **File > Advanced > Security Settings**.

   Note:

   If the **Security Settings** option does not appear under **Advanced**, do the following:

   a. Select **File > Preferences**.

b. In the IP Office Manager Preferences dialog box, click the **Set Simplified View as default** check box to deselect this option

c. Click **OK**.

d. Close and restart IP Office Manager.

3. In the **Select IP Office** window, click the check box for the appropriate system.
4. Click **OK**.
5. In the **Security Service User Login** window, enter a user name and password of an account that has security configuration access to the IP Office system.

   The defaults are **security** and **securitypwd**.
6. In the **Security Settings** pane, select **Services > Configuration**.
7. Click the **Service Details** tab.
8. In the **Service Access Secure** drop-down box, select **Unrestricted**.

   Note:

   To be able to use IP Office Manager to administer the branch, **Unrestricted** must be selected.
9. Click **OK**.
10. Select **File > Save Security Settings**.

Enabling the Security Settings option for the branch

About this task

To disable the System Manager administration feature for a branch that is centrally managed by System Manager, you must have access to the Security Settings for that branch. If the branch configuration has not yet been opened from IP Office Manager, the **Security Settings** option is not available. To enable the **Security Settings** option, you must clear the **Set Simplified View as default** option in the IP Office Manager Preferences window. When that is done, the **Security Settings** option becomes available for that branch.

Note:

This task needs to be performed only one time.

Procedure

1. Start IP Office Manager.
2. Click **File** > **Preferences**.
3. In the **Preferences** tab, clear **Set Simplified View as default**.
4. Click **OK**.
5. Close IP Office Manager.

Synchronizing IP Office with System Manager

About this task

If you used IP Office Manager to administer a branch that is centrally managed by System Manager, you must synchronize the changes you made and return the System Manager administration feature for the branch to the enabled state.

Some configuration changes cannot be synced with System Manager. See Configuration changes performed through Manager that cannot be synced with System Manager on page 151.

Procedure

1. On the System Manager console, under **Services**, click **Inventory**.
2. In the left navigation pane, click **Synchronization > IP Office**.
3. Click the check box for the IP Office system whose configuration you want to sync with System Manager.
4. Do one of the following:
   - Click **System Configuration** to sync only system configuration data with System Manager.
   - Click **User** to sync only user data with System Manager.
   - Click **System Configuration and Users** to sync system configuration and user data with System Manager.
5. Do one of the following:
   - Click **Now** to run the synchronization job now.
   - Click **Schedule** to run the synchronization job at a scheduled date and time.

Configuration changes performed through IP Office Manager that cannot be synced with System Manager

You can disable System Manager administration for an IP Office and configure the IP Office device locally through IP Office Manager. To do this, you must first disable System Administration for the branch and then enable System Administration for the branch after you make your configuration changes. Then you must synchronize those changes with System Manager.

There are some configuration changes that cannot be synchronized with System Manager. Those tasks should not be performed locally through IP Office Manager for branches that are centrally managed bySystem Manager. Configuration changes that cannot be synchronized and therefore should not be performed locally are:

- Adding users or extensions
- Editing user core attributes (that is, name, number, password, or extension number)

- Changing any of the following security configuration settings:
  - BranchAdmin user settings
  - SCEP settings
  - Certificate settings
  - Web services settings

The User Rights feature is not integrated with System Manager. The User Rights feature is available only in the local IP Office Manager and is intended only for IP Office systems that are not configured to be managed centrally through System Manager.

IP Office security configuration

Security Configuration

Use the **Security Configuration** pages to view and edit the security configuration values of IP Office, UCM, or Application Server devices through System Manager. However, Client computers need JRE for System Manager to support the IP Office application. For more information, see JRE requirement for client computers in *Avaya Aura® System Manager Online Help*.

To view or edit security configuration values, you must launch the IP Office Manager in the online mode through System Manager. System Manager uses web services to obtain the latest security configuration from an IP Office, UCM, or Application Server device and passes the configuration to the IP Office element manager. After you save the modifications on the IP Office element manager, System Manager retrieves the modified security configuration file and pushes the file to the IP Office, UCM, or Application Server device. After the security configuration files are successfully uploaded to the device, System Manager deletes the local copy of these security configuration files.

Viewing a security configuration

About this task

From IP Office version 11.0 onwards, Security Configuration is supported through System Configuration.

You can use different browsers to view the Security Configuration through System Configuration for IP Office version 11.0 onwards.

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **IP Office** > **Security Configuration**.

3. On the IP Office Security Configuration page, select the IP Office device whose Security Configuration you want to view.
4. Click **View**.

Browser	IP Office version	Procedure
Mozilla Firefox (all supported versions). and Internet Explorer 11.x	11.0 onwards	IP Office Web Manager application launches. In the right pane of the IP Office Web Manager window, you can view the details of the selected IP Office Security Configuration. All the fields are read-only. • Click **Update**.
Internet Explorer 11.x	Below 11.0	IP Office Manager application launches. In the right pane of the IP Office Manager window, you can view the details of the selected IP Office Security Configuration. All the fields are read-only. • To exit the IP OfficeManager application and return to the IP Office Security Configuration page, click **File** > **Exit**.

Related links

IP Office security configuration field descriptions on page 154

Editing a security configuration

About this task

From IP Office version 11.0 onwards, Security Configuration is supported through System Configuration.

You can use different browsers to edit the Security Configuration through System Configuration for IP Office version 11.0 onwards.

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **IP Office** > **Security Configuration**.
3. On the IP Office Security Configuration page, select the device whose security configuration you want to edit.
4. Click **Edit**.

Browser	IP Office version	Procedure

Table continues…

Mozilla Firefox (all supported versions). and Internet Explorer 11.x	11.0 onwards	IP Office Web Manager application launches. a. On the IP Office Web Manager window, edit the required fields on the right pane. b. Click **Update**. The system directs you to the IP Office System Configuration landing page.
Internet Explorer 11.x	Below 11.0	IP Office Manager application launches. a. On the IP Office Manager window, edit the required fields on the right pane. b. Click **File** > **Save Security Settings and Exit** to save the modifications and exit the IP Office Manager application. The system directs you to the IP Office Security Configuration landing page.

After you save the configuration, System Manager retrieves the edited security configuration file from the IP Office Manager application and pushes the file to the IP Office device.

Related links

IP Office security configuration field descriptions on page 154

IP Office security configuration field descriptions

Device list

Name	Description
Device Name	The name of the IP Office device.
IP Address	The IP address associated with the IP Office device.
System Type	The type of system associated with the IP Office device. The valid options are: • **IP Office**: for IP Office core unit • **IP Office Select**: for IP Office Select core unit
Last Operation on Device	The last operation that you performed on the device.
Status	The status of the operation that is currently running or was last run.
System Configuration Template	The current IP Office System Configuration template that exists on the IP Office device.

Table continues…

Name	Description
Last Modified Time of System Configuration	The date and time of the last system configuration operation.
Last BackupTime	The date and time when you last performed the backup activity on the IP Office device.

Buttons

Name	Description
View	Click to view the IP Office security configuration field descriptions.
Edit	Click to edit the IP Office security configuration field descriptions.

Voicemail Pro Call Flow configuration

Viewing the Voice Mail Pro call flow

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **VMPro** > **Call Flow**.
3. On the VMPro Call Flow page, select the **Voice Mail Pro** device whose call flow you want to view.
4. Click **View**.

   The system starts the Voicemail Pro Client application in Offline and Read only mode.
5. To exit Voicemail Pro Client , click **File** > **Exit**.

   The system displays the VMPro Call Flow page.

Editing the Voice Mail Pro call flow

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **Applications**.
3. In the left navigation pane, click **VMPro** > **Call Flow**.
4. On the VMPro Call Flow page, select the IP Office device whose call flow you want to edit.

5. Click **Edit**.

   The system starts the Voicemail Pro Client application in Offline and Editable mode.

6. Do one of the following:

   - To exit Voicemail Pro Client without saving, click **File** > **Exit**.
   - To return to the Voicemail Pro Client page after saving, click **File** > **Save and Make Live**.

   The system displays the VMPro Call Flow page.

Downloading the Voice Mail Pro call flow

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **Applications**.
3. In the left navigation pane, click **VMPro** > **Call Flow**.
4. On the VMPro Call Flow page, select the IP Office device whose call flow you want to edit.
5. Click **Download**.
6. Do one of the following:

   - For Firefox, click **Save File** and click **OK**.

     The system saves the configuration file with the device name to the default location.

   - For Internet Explorer, provide the file name and location, and click **Save**.

     The system saves the configuration file to the default location.

Viewing the status of a Voice Mail Pro call flow

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **Applications**.
3. In the left navigation pane, click **VMPro** > **Call Flow**.
4. On the VMPro Call Flow page, select the **Voice Mail Pro** device whose call flow status you want to know.
5. Click **Status**.

   The system refreshes the VMPro Call Flow page and displays the status of the VMPro call flow in the Status column.

Saving Voice Mail Pro call flow as a template

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **VMPro** > **Call Flow**.
3. On the VMPro Call Flow page, select the **Voice Mail Pro** device whose call flow you want to save as a template.
4. Click **Save As Template**.
   a. Type the name for the Voice Mail Pro call flow template.
   b. Select the version.
   c. Click **Commit**.
5. On the System Manager web console, click **Services** > **Templates**.
6. In the left navigation pane, click **VMPro Callflow Template**.

   The VMPro Call Flow Templates page displays the VMPro call flow that you saved as a template.

VMPro Call Flow field descriptions

Device List

Name	Description
Device Name	The name of the IP Office device.
IP Address	The IP Address of the IP Office device.
Device Version	The version name of the IP Office device.
Last Operation on Device	The name of last operation performed on the IP Office device.
Status	The status of the IP Office device.
VMPro Call Flow Template	The name of the VMPro Call Flow Template applied to the IP Office device.
Last Modified Time of System Configuration	The time when the system configuration was last modified.
Last Backup Time	The time of the last back up.

Button	Description
View	Click to view the Voice Mail Pro call flow field descriptions.

Table continues…

Button	Description
Download	Click to download the Voice Mail Pro call flow field descriptions.
Save As Template	Saves the Voice Mail Pro call flow field descriptions as a template.
Edit	Click to edit the Voice Mail Pro call flow field descriptions.
Status	Displays the status of the operation that is currently running on or was last run.

Viewing the Voice Mail Pro system configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **VMPro** > **System Configuration**.
3. On the VMPro System Configuration page, select the IP Office device whose system configuration you want to view.
4. Click **View**.

   In the right pane, in the Voicemail Pro - System Preferences window, you can view the details of the selected **Voice Mail Pro** system configuration.

   The system starts **Voice Mail Pro** in **Read Only** mode.

Next steps

For Voice Mail Pro system preferences, see *Implementing Voice Mail Pro*.

Editing the Voice Mail Pro system configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **VMPro** > **System Configuration**.
3. On the VMPro System Configuration page, select the **Voice Mail Pro** device whose system configuration you want to edit.
4. Click **Edit**.

   The system displays Voicemail Pro - System Preferences page.
5. In the right pane, on the Voicemail Pro - System Preferences page, edit the required fields.
6. Do one of the following:
   - To save the modifications, click **Update** .

- To save the modification and exit, click **Save and Exit**.

Next steps

For Voice Mail Pro system preferences, see *Implementing Voice Mail Pro*.

Saving Voice Mail Pro system configuration as a template

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **VMPro** > **System Configuration**.
3. On the VMPro System Configuration page, select the Voice Mail Pro device whose system configuration you want to save a template.
4. Click **Save As Template**.
   a. Type a name for the Voice Mail Pro system configuration template.
   b. Select the version.
   c. Click **Commit**.
5. On the System Manager web console, click **Services** > **Templates**.
6. In the left navigation pane, click **VMPro System Configuration Template**.

   The VMPro System Configuration Templates page displays the VMPro system configuration that you saved as a template.

VMPro system configuration field descriptions

Button	Description
View	Displays the Voice Mail Pro System Configuration page in read only format.
Edit	Displays the Voice Mail Pro System Configuration page where you can modify details.
Save As Template	Saves the Voice Mail Pro system configuration data as template.

Synchronizing the VMPro system configuration

Before you begin

To synchronize VMPro devices successfully, perform the following:

- Configure VMPro IP Address in IP Office System Configuration.

- Password of VMPro should be same forIP Office, UCM and Application Server and VMPro System Preferences.

  Note:

  - You can change the password for Application Sever through security setting using IP Office Manager.
  - You can change the password for VMPro System Preferences through Web Manager.
- You must give access rights to VMPro Application from security setting of IP Office and UCM and Application Server through IP Office Manager.
- You must have valid IP Office licenses for VMPro instances.

Procedure

1. On the System Manager console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **VMPro**.
3. Select the device you want to synchronize.
4. In the device list, select any of the following options that you want to synchronize for the selected device.
5. Click **Now** to perform the synchronization now or click **Schedule** to perform the synchronization at a specified time.

   Note:

   To view the status of synchronization, click **Services** > **Scheduler** on the System Manager console.

Result

If the operation of synchronizing the VMPro succeeds, you can work on the latest updated vmpro system configuration and avoid data corruption.

If the operation of synchronizing the VMPro fails, you can work only on local available system configuration in System Manager.

If the operation of synchronizing the VMPro fails and if it is first time that you attempted data synchronization, you can work only on the default configuration.

Configuring UCM and Application Server

Synchronizing the UCM and Application Server system configuration

About this task

Use the procedure to synchronize the configuration of a UCM and Application Server device with the local machine.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **UCM and Application Server**.
3. Select the device that you want to synchronize.

   System Configuration is selected by default.
4. Do one of the following:
   - To perform the synchronization now, click **Now**.
   - To perform the synchronization at a specified time, click **Schedule**.
5. To view the status of synchronization, click **Services** > **Scheduler**.

Managing the security configuration of Unified Communications Module and Application Server with System Manager

About this task

You can manage the security configuration of the Unified Communications Module and Application Server with System Manager manually.

Procedure

1. On the System Manager web console, from **Home** > **Elements** > **IP Office** > **UCM and Application Server** > **Security Configuration**, select the device.
2. Select one of the following options:
   - To view the system configuration of the Unified Communications Module and Application Server, click **View**.
   - To edit the system configuration of the Unified Communications Module and Application Server, click **Edit**.

Important:

To work with another IP Office system, you must open a new IP Office tab from the dashboard and launch another instance of IP Office Manager. You cannot edit multiple IP Office systems from a single instance of IP Office Manager.

IP Office Web Manager launches.

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

Managing the system configuration of Unified Communications Module and Application Server with System Manager

About this task

You can synchronize the Unified Communications Module and Application Server system configuration with System Manager manually.

Procedure

1. On the System Manager web console, from **Home** > **Elements** > **IP Office** > **UCM and Application Server** > **System Configuration**, select the device.
2. Select one of the following options:
   - To view the system configuration of the Unified Communications Module and Application Server, click **View**.
   - To download the system configuration of the Unified Communications Module and Application Server, click **Download**.
   - To edit the system configuration of the Unified Communications Module and Application Server, click **Edit**.

   Important:

   To work with another IP Office system, you must open a new IP Office tab from the dashboard and launch another instance of IP Office Manager. You cannot edit multiple IP Office systems from a single instance of IP Office Manager.

   IP Office Web Manager launches.
3. To save the updates and return to System Manager, from the **File** menu, click **Save Configuration and Exit**.

Creating a backup of the UCM and Application Server device configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **UCM and Application Server** > **Backup**.
3. On the UCM and Application Server Backup page, in Device List, click the UCM and Application Server device for which you want to create a backup.
4. Click **Backup**.

   The system displays the UCM and Application Server device that you selected in **Device List**.
5. Select a remote server from the **Remote Server** field. Alternatively, click **Add Server** to add a remote server.
6. Configure the settings for **Backup Configuration** using the following parameters:
   - In the **Select Voicemail Pro Sets** field, choose voice mail pro sets.
   - In the **Select One-x Portal Sets** field, choose one-x portal sets.
   - In the **Select Contact Recorder Sets** field, choose contact recorder sets.
   - In the **Backup Label** field, type the backup file name.
7. Do one of the following:
   - Click **Now** to perform the backup task immediately.
   - Click **Schedule** to perform the backup task at a specified time.
8. To view the status of the backup task for the selected device, click **Status**.

Restoring the UCM and Application Server device configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation page, click **UCM and Application Server** > **Restore**.
3. On the UCM and Application Server Backup page, select the UCM and Application Server device whose backed— up configuration you want to restore.
4. Click **Restore**.

   The system displays the UCM and Application Server device that you selected in **Device List**.

5. Do the following:
   a. In the **Remote Server** field, click a Remote Server . Alternatively, click **Add Server** to add a remote server.

      The system activates the **Get Restore Point** button.

   b. Click **Get Restore Point**.

      The system displays the **Restore Points** list with the restore point that you added:

Field name	Field description
Restore Point	Displays the name of the restore point.
IP Address	Displays the IP address associated with the restore point.
Version	Displays the version of the restore point.
Set	Displays the set of the restore point.
Time Stamp	Displays the time stamp associated with the restore point.

6. Do one of the following:
   - Click **Now** to perform the restore task immediately.
   - Click **Schedule** to perform the restore task at a specified time.

     To view the status of the restoration task for the selected device, click **Status**.

Downloading the UCM and Application Server system configuration

About this task

Use this procedure to copy the configuration of UCM and Application Server instances to the local computer.

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **UCM and Application Server** > **System Configuration**.
3. On the UCM and Application Server System Configuration page, select the device whose security configuration you want to download.
4. Click **Download**.
5. Do one of the following:
   - For Firefox, click **Save File**, and then click **OK**.

     The system saves the configuration file with the device name to the location that you specified.

- For Microsoft Internet Explorer, type the file name and the location, and click **Save**.

  The system saves the configuration file to the location that you specified.

UCM and Application Server Backup field descriptions

Remote Server

Name	Description
Select Remote Server	The Remote server location to store the backup.

Backup On Remote Server

Name	Description
Select Remote Server	The Remote Server location to store the backup. The options are: • **Select**: To select a remote server. • **Add Server**: To add a remote server.
Add Server	The configuration parameters for adding a remote server. The parameters are: • **Backup Label**: The name of the backup • **New Server Name**: The name of the new server • **New Server IP**: The IP address of the new server • **Port**: The port number of the new server • **Backup Path**: The backup path of the new server • **Selected Protocol**: The protocol of the new server • **User Name**: The name of the user • **Password**: The password of the user
Selected Protocol	The protocol of the new server. The options are: • **http** • **https** • **scp** • **sftp** • **ftp**

Backup Configuration

Name	Description
Select voice mail Pro Sets	The voice mail pro sets.
Select one-X Portal Sets	The one-X Portal sets.

Table continues…

Name	Description
Select Contact Recorder Sets	The contact recorder sets.
Backup Label	The name of the backup file.

Buttons

Button	Description
Backup	Opens the UCM and Application Server Backup page.
Status	Displays the status of the last operation.
Save	Saves the remote server and backup configuration.
Edit	Modifies the remote server and backup configuration.
Delete	Deletes the remote server and backup configuration.
Now	Performs the backup job, as applicable, immediately.
Schedule	Schedules the backup at a later time and opens the UCM and Application Server Backup page.
Cancel	Cancels the backup job and opens the UCM and Application Server Backup page.
Stop	Stops the backup job.

UCM and Application Server Restore field descriptions

Remote Server

Name	Description
Select Remote Server	The list of available remote servers
New Server Name	The name of the new server
New Server IP	The IP address of the new server
Port	The port address
Backup Path	The path of the latest backup
Selected Protocol	The protocol for the new server
User Name	The user name for the new server
Password	The password for the new server

Button	Description
Restore	Opens the **UCM and Application Server Restore** page. Use this page to restore the backed up system configuration and the messages, the recording and the one-X configuration to a UCM and Application Server device.
Status	Displays the status of the operation that is currently running or was last run.

Table continues…

Button	Description
Save	Saves the remote server and backup configuration.
Now	Performs the restore operation immediately.
Schedule	Displays the **IP Office Job Scheduler** page. Use this page to schedule a Restore operation.
Cancel	Cancels the restore job, as applicable, and directs you to the **Restore** landing page.
Get Restore Point	Creates a restore point on the selected remote server.

Restore Backup stored on Remote Server

Name	Description
Remote Server	The Remote Server location where the last backup was stored. Do one of the following: • **Select**: Select a remote server. • **Add Server**: Add a remote server.
Add Server	The configuration for a remote server • **New Server Name**: Name of the new server • **New Server IP**: IP address of the new server • **Port**: Port number of the new server • **Backup Path**: Backup path of the new server • **Selected Protocol**: Protocol of the new server • **User Name**: Name of the user • **Password**: Password of the user
Selected Protocol	Protocol of the new server. Select a protocol from the following: • **http**: for the http protocol • **https**: for the https protocol • **scp**: for the scp protocol • **sftp**: for the sftp protocol • **ftp**: for the ftp protocol
Restore Point(s)	The restore point from where you want to restore the last backup

Viewing a UCM and Application Server system configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **UCM and Application Server** > **System Configuration**.
3. On the System Configuration page, select the UCM and Application Server device whose system configuration you want to view.
4. Click **View**.

   In the right pane of the UCM and Application Server window, you can view the details of the selected UCM and Application Server system configuration.

   Note:

   All the fields are view only.

   The system starts the UCM and Application Server Manager application.
5. Click **File** > **Exit** to exit the UCM and Application Server Manager application.

   The UCM and Application Server System Configuration landing page opens.

Editing a UCM and Application Server system configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **UCM and Application Server** > **System Configuration**.
3. On the UCM and Application Server System Configuration page, select the UCM and Application Server device whose system configuration you want to edit.
4. Click **Edit**.

   The system starts the UCM and Application Server Manager application.
5. On the UCM and Application Server Manager window, edit the required fields on the right pane.
6. Click **File** > **Save Configuration and Exit** to save the modifications and exit the UCM and Application Server Manager application.

   On the UCM and Application Server System Configuration Edit page, the system displays selected UCM and Application Server device in the device list. Perform one of the following:

   - Click **Commit** to apply the changes immediately.
   - Click **Schedule** to apply the changes at a specified time.

UCM and Application Server system configuration field descriptions

Name	Description
Device Name	The name of the UCM and Application Server device.
IP Address	The IP address associated with the UCM and Application Server device.
System Type	The type of system associated with the UCM and Application Server device.
Last Operation on Device	The operation that has been performed last on the device.
Status	The status of the operation that is currently running or was last run.
System Configuration Template	The current UCM and Application Server System Configuration template that exists on the UCM and Application Server device.
Last Modified Time of System Configuration	The date and time you last modified the system configuration.
Last Backup Time	The date and time when you last performed a backup.

Button

Name	Description
View	Click to view the UCM and Application Server system configuration field descriptions.
Edit	Click to edit the UCM and Application Server system configuration field descriptions.
Download	Click to download the UCM and Application Server system configuration field descriptions.

Viewing UCM and Application Server security configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **UCM and Application Server** > **Security Configuration**.
3. On the UCM and Application Server Security Configuration page, select the UCM and Application Server device whose Security Configuration you want to view.
4. Click **View**.

The system starts the UCM and Application Server Manager application.

5. In the right pane of the UCM and Application Server Manager window, you can view the details of the selected UCM and Application Server Security Configuration. All the fields are read-only.
6. Click **File** > **Exit** to exit the UCM and Application Server Manager application and return to the UCM and Application Server Security Configuration landing page.

Editing UCM and Application Server security configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **UCM and Application Server** > **Security Configuration**.
3. On the UCM and Application Server Security Configuration page, select the device whose security configuration you want to edit.
4. Click **Edit**.

   The system starts the UCM and Application Server Manager application.
5. The system starts the UCM and Application Server Manager window, edit the required fields on the right pane.
6. Click **File** > **Save Security Settings and Exit** to save the modifications and exit the UCM and Application Server Manager application.

   The system directs you to the IP Office Security Configuration landing page.

   After you save the configuration, System Manager retrieves the edited security configuration file from the UCM and Application Server Manager application and pushes the file to the UCM and Application Server device.

UCM and Application Server security configuration field descriptions

Device list

Name	Description
Device Name	The name of the UCM and Application Server device.
IP Address	The IP address of the UCM and Application Server device.
System Type	The type of system associated with the UCM and Application Server device.

Table continues…

Name	Description
Last Operation on Device	The last operation that you performed on the device.
Status	The status of the operation that is currently running or was last run.
System Configuration Template	The current system configuration template that exists on the UCM and Application Server device.
Last Modified Time of System Configuration	The date and time of the last system configuration operation.
Last Backup Time	The date and time when you last performed the backup activity on the UCM and Application Server device.

Buttons

Name	Description
View	Click to view the UCM and Application Server security configuration field descriptions.
Edit	Click to edit the UCM and Application Server security configuration field descriptions.

Transferring custom prompt files to a UCM or Application Server device

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **UCM and Application Server** > **File Transfer**.
3. In **Select File Type**, click **Custom Prompts**.
4. In **Select Files to Upload**, click the audio file that you want to upload.

   List Audio Files displays the list of audio files that you have uploaded by using **Manage Custom Prompts** in the UCM or Application Server system configuration templates.

   In the **Enter Destination Folder Location to Push Files** field, the system displays the default location where you want to transfer the file.
5. In **Devices List**, select the IP Office Application Server or UCM device where you want to upload the audio file.
6. Click **Commit**.
7. On the File Transfer page, perform one of the following:
   - Click **Now** to upload the audio file to the IP Office Application Server or UCM device.
   - Click **Schedule** to upload the audio file at the scheduled time.

Note:

Until the transfer is complete, do not delete the file. The file transfer operation fails if you delete the file that you want to transfer.

Using the file transfer capability, you cannot upload PLDS license files. For information about uploading a PLDS license file to the IP Office Application Server or UCM device, see *Deploying IP Office in an Avaya Aura® Branch Environment*. For uploading files to System Manager, see Uploading files to the System Manager repository. To delete a file, see Deleting an uploaded file.

8. To check the status of the file transfer, click **Services** > **Scheduler**.

Avaya Aura® Session Manager Configuration

Avaya Aura® Session Manager handles call admission control, call re-direction, digit analysis, dial plan management, internal network call accounting feeds, toll by-pass, inter-office routing and international least cost routing. All administration and management of the enterprise-wide private global dial plan network is handled by this communications appliance, and managed as a single enterprise with Avaya Aura® System Manager. Using SIP as the control plane, Session Manager controls and directs connection requests between users of Avaya Aura® Communication Manager, the Avaya Aura® applications/services and users of the IP Office system. The subsequent media path that is established and connects the endpoints (phones, services and applications) is always routed directly and does not involve Session Manager.

The role that Session Manager plays in IP Office branch deployments is different depending on the specific type of deployment. In Distributed enterprise branch deployments, Session Manager acts as a SIP proxy to route SIP sessions to and from the SIP trunk connected to the IP Office system. In Centralized enterprise branch deployments, Session Manager plays a larger role where the Centralized phones register directly with Session Manager in the enterprise core to receive services from the core applications such as Communication Manager Feature Server or Evolution Server.

This chapter provides procedures to configure Session Manager to support calls to and from IP Office systems. Avaya Aura® System Manager is used to administer Session Manager. Perform the following procedures:

1. View the SIP domains for which the Session Manager provides call management. Multiple domains can be listed. See Viewing the SIP domains on page 174.
2. Identify logical and/or physical locations where SIP entities reside. IP address patterns can be used to define different locations within the Avaya Aura® network, for example the IP address range of each IP Office system. The creation of locations allows features such as bandwidth management to be applied to connections from those locations. See Creating locations on page 174.
3. Create a set of digit adaptations in order to ensure correct routing. If the digits to or from a branch need alteration in order to be routed correctly at either end, this can be done using

a table of digit adaptations. Each SIP entity (branch) is associated with its own set of digit adaptations. See Creating adaptations on page 175.

4. Add each IP Office system to the list of SIP entities that send calls to and from the Avaya Aura® network. See Creating SIP entities on page 175.
5. Add an entity link for each SIP entity including each IP Office. An entity link must be added to define the ports and transport method used for connections between the SIP entity and the Session Manager. See Creating entity links on page 177.
6. Create time ranges to control when different routing policies are used. See Creating time ranges on page 177.
7. Add a routing policy. A routing policy consists of a selected SIP entity as its destination and a number of time ranges that define when the policy can be used. See Creating routing policies on page 178.
8. Add dial patterns. Dial patterns are used to match digits received to a destination. Each dial pattern has an associated routing policy that defines the target entity for matched calls and when the match should be used. See Creating dial patterns on page 178.

Note:

You must complete fields marked with an asterisk. Fields not marked with an asterisk are optional.

For more information about administering Session Manager, see “Managing Session Manager routing” in *Administering Avaya Aura® Session Manager*.

Configuring Session Manager checklist

Use this checklist to monitor your progress as you configure Avaya Aura®Session Manager.

#	Description	Section	✔
1	View a list of the SIP domains.	See Viewing the SIP domains on page 174.	
2	Create a location.	See Creating locations on page 174.	
3	Create a digit adaptation.	See Creating adaptations on page 175.	
4	Create a SIP entity.	See Creating SIP entities on page 175.	
5	Create an entity link.	See Creating entity links on page 177.	
6	Create a time range.	See Creating time ranges on page 177.	
7	Create a routing policy.	See Creating routing policies on page 178.	
8	Create a dial pattern.	See Creating dial patterns on page 178.	

Table continues…

#	Description	Section	✔
9	Add IP Office users and Centralized users. This task is performed from Avaya Aura® System Manager using the User Management feature.	See User administration on page 190.	
10	After the IP Office system has been successfully configured and you are satisfied with the configuration, perform a backup of the system configuration from Avaya Aura® System Manager to save a backup to the IP Office internal SD card.	See Backing up the system configuration using System Manager on page 195.	

Viewing the SIP domains

The domain for which the Session Manager is authoritative was added when Session Manager was initially configured for the IP Office system. The domain name set in the IP Office system's SM Line configuration (see Adding an SM Line on page 96) should match one of the entries that is listed on the Domain Management page.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **Domains**.

   The SIP domains are listed on the Domain Management page.

Creating locations

Locations are used to identify logical and/or physical locations where SIP entities reside. The location entries in Session Manager allow bandwidth management and call control to be applied for connections to and from those locations.

Typically locations are added for each IP Office branch site.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **Locations**.
3. On the **Location page**, click **New** to add a new location.
4. On the **Location Details** page, in the **Name** field, enter a name to identify the location.
5. In the **Notes** field, enter notes about the location, as appropriate.

6. In the **Dial Plan Transparency in Survivable Mode** section, accept the default settings.
7. In the **Overall Managed Bandwidth** section, accept the default settings.
8. In the **Per-Call Bandwidth Parameters** section, accept the default settings.
9. In the **Alarm Threshold** section, accept the default settings.
10. In the **Location Pattern** section, click **Add** to add a location pattern.
11. In the **IP Address Pattern** field, enter an IP address pattern that matches the IP LAN address range.

    The * character can be used as a match-all wildcard. For example, the pattern 192.168.42.* matches all addresses in the range 192.168.42.1 to 192.168.42.255.
12. In the **Notes** field, enter notes about this location pattern, as appropriate.
13. Click **Commit**.

Creating adaptations

Occasionally calls to or from the branch may require digit conversion in order to ensure correct routing. For example, reinserting an external dialing prefix. This is done using a set of digit conversions stored by the digit adaptation associated with the SIP entity.

Adaptations are optional and are deployment specific. For more information, see “Adaptations” in *Administering Avaya Aura®Session Manager*.

Creating SIP entities

A SIP entity is required for each branch system. This is in addition to the SIP entities that should already exist for Session Manager and Communication Manager or Communication Manager Feature Server or Evolution Server.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **SIP Entities**.
3. On the SIP Entities page, click **New** to create a new SIP Entity.
4. On the SIP Entity Details page, in the **Name** field, enter the name of the SIP entity.
5. In the **FQDN or IP Address** field, enter the IP address of the IP Office system LAN interface configured for the SM Line operation.
6. In the **Type** drop-down box, do one of the following:
   - If this branch is used in a Distributed enterprise branch deployment select **SIP Trunk**.
   - If this branch is used in a Centralized or Mixed enterprise branch deployment and has Centralized users configured, select **Survivability Server**.

     This SIP Entity will be provided as a choice in the **Survivability Server** drop-down box when you add a Centralized user to System Manager. See “Adding Centralized SIP

users to System Manager" in *Administering Centralized Users for an IP Office Enterprise Branch*.

7. In the **Notes** field, enter a description to help identify this SIP entity, as appropriate.
8. In the **Adaptation** drop-down box, select the adaptation that contains the digit conversions to apply to calls to and from the location.
9. In the **Location** drop-down box, select the location that matches the location you configured in Creating locations on page 174.
10. In the **Time Zone** drop-down box, select the time zone for the location.
11. For the **Override Port & Transport with DNS SRV** check box, accept the default setting, unchecked.
12. In the **SIP Timer B/F (in seconds)** field, accept the default setting, 4.

    Note:

    If you see that calls are abnormally terminated, you should increase this number.
13. In the **Credential Name** field, accept the default setting, blank.
14. In the **Call Detail Recording** field, accept the default setting.
15. In the **Loop Detection Mode** field, accept the default setting.
16. In the **SIP Link Monitoring** drop-down box, accept the default, **Use Session Manager Configuration**.
17. Under **Port**, click **Add**.
18. Depending on what protocol the phones should use to connect to the IP Office system in Rainy day, do one of the following:
    - If the IP Office system was configured for the phones to use TCP to connect in Rainy day, in the **Port** field, enter `5060`. Then in the **Protocol** drop-down box, select **TCP**.
    - If the IP Office system was configured for the phones to use TLS to connect in Rainy day, in the **Port** field, enter `5061`. Then in the **Protocol** drop-down box, select **TLS**.

    Note:

    The port and protocol that you configure here will be pushed to the phones along with the IP Office IP address when this SIP entity is selected as the survivability server for the user. This will be the port and protocol that the phones will use to connect to the IP Office system in Rainy day.
19. Click **Commit**.

Creating entity links

For each SIP entity communicating with the Avaya Aura® Session Manager, an entity link needs to be configured. That includes one for each IP Office.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **Entity Links**.
3. On the Entity Links page, click **New**.
4. In the **Name** field, enter a name to describe this link.
5. In the **SIP Entity 1** drop-down box, select the name of the Session Manager system that is at one end of the link.

   SIP Entity 1 must always be a Session Manager instance. For an SM Line from an IP Office system, this should match the Session Manager set as the **SM Address** in the SM Line's configuration.
6. In the **Protocol** drop-down box, select **TCP**.

   When TCP is selected, the **Port** field is automatically set as **5060**. This is the port to which the SIP Entity 2 sends SIP requests.
7. In the **SIP Entity 2** drop-down box, select the name of the IP Office system that is at the other end of the link.

   When you selected TCP in the previous step, the **Port** field was automatically set as **5060**.
8. In the **Connection Policy** drop-down box, select **trusted**.

   The selection in this field must be **trusted**. If it is not, calls from the associated SIP Entity 2 will be denied by Session Manager
9. For the **Deny New Service** check box, accept the default setting (unchecked) .
10. In the **Notes** field, enter notes regarding this entity link, as appropriate.
11. Click **Commit**.

Creating time ranges

Additional time ranges can be created and used with a routing policy to define when the routing policy is active. For most IP Office branch implementations, you do not need to define additional time ranges. If you need to add or adjust a time range, see "Creating Time Ranges" in *Administering Avaya Aura Session Manager*.

Creating routing policies

A routing policy is a collection of multiple time ranges and a destination SIP entity. For each dial pattern configured to route calls received by the Session Manager, the routing policy associated with that dial pattern defines when and where matching calls are directed.

Separate routing policies are required for each IP Office entity to which the Session Manager routes calls.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **Routing Policies**.
3. On the **Routing Policies** page, click **New** to create a new routing policy.
4. On the **Routing Policies Details** page, in the **Name** field, enter a name to describe this routing policy.
5. For the **Disabled** check box, accept the default, unchecked.
6. In the **Retries** field, enter the number of retries for the destination SIP entity. Valid numbers are 0 – 5.
7. In the **Notes** field, enter notes about this routing policy, as appropriate.
8. In the **SIP Entity as Destination** section, do the following:
    a. Click **Select**.
    b. On the **SIP Entities** page, select the SIP entity to which the routing policy applies.
    c. Click **Select**.
9. Skip the **Time of Day** section, **Dial Patterns** section, and **Regular Expressions** section. You do not need to configure these settings.
10. Click **Commit**.

Creating dial patterns

A dial pattern is defined to direct calls prefixed with the branch prefix to each branch.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **Dial Patterns**.
3. On the **Dial Patterns** page, click **New** to create a new dial pattern.
4. On the **Dial Pattern Details** page, in the **Pattern** field, enter the branch prefix.

    This is the dialed number or number prefix that the dial pattern is intended to match.
5. In the **Min** field, enter the minimum length (1 to 36) of the dialed number that the pattern should match. For example, if the branch prefix is 3 digits and the extension number length is 4 digits, you would enter 7.

6. In the **Max** field, enter the maximum length (1 to 36) of the dialed number that the pattern should match. For example, if you set this to the same value as the **Min** value, the dial pattern will match only internal calls.
7. For the **Emergency Call** check box, leave the check box set to the default setting, unchecked.
8. In the **Emergency Priority** field, enter a value between 1 and 10 for the priority of the emergency number.
9. In the **Emergency type** field, enter the type of emergency number, for example police or fire.
10. In the **SIP Domain** drop-down box, select the appropriate SIP domains that should be matched, or select **All** to allow calls from all SIP domains to be routed.
11. In the **Notes** field, enter notes to describe this dial pattern, as appropriate.
12. In the **Originating Locations and Routing Policies** section, click **Add**.
13. In the **Originating Location** section, click the check box for **Apply The Selected Routing Policies to All Originating Locations**.
14. In the **Routing Policies** section, click the check box for the routing policy that was created for the branch.
15. Click **Select**.
16. If you need to specify that calls from certain locations be denied, do the following:
    a. In the **Denied Originating Locations** section, click **Add**.
    b. Do one of the following:
        - Click the **Apply to All Originating Locations** check box.
        - Click the check box(es) for the locations that should be denied.
    c. Click **Select**.
17. On the Dial Patterns Detail page, click **Commit**.

Traffic and Quality of Service configuration

Voice quality monitoring

QoS monitoring

IP Office supports QoS monitoring and provides QoS alarms of excessive jitter, delay, or loss on certain types of calls. IR Prognosis application integrates with Avaya Aura® to provide enhanced QoS monitoring. Prognosis is an external collector that receives RTCP monitoring messages from H.323 phones.

Enabling feature

The enabling feature instructs the IP Office H.323 phones to send their RTCP monitoring messages to Prognosis. IP Office sends the address of the external RTCP collector to the H.323 phones. If the enabling feature is configured, IP Office instructs the Avaya H.323 phones at registration to send their RTCP monitoring messages to the configured collector IP address. It provides the H.323 phones with the IP address of the external collector. The enabling feature is supported in the following deployments:

- IPOL and IP500 V2 Platforms
- Essential, Preferred, Server, and select server editions
- Mid-market and in branch deployments

Configuring RTCP collector IP address for phones

Before you begin

To configure the enabling feature, the administrator needs to restart the phone.

Procedure

1. Clear the **Enable RTCP Monitor On Port 5005** check box.

   This configuration cannot be used together with the existingIP Office configuration.

2. In **LAN** > **VoIP**, the default value of the **RTCP collector IP address for phones** is `0.0.0.0`. This indicates the enabling feature is disabled.

Geographic Redundancy configuration

Avaya Aura® provides System Manager Geographic Redundancy, a resiliency feature that handles scenarios where the primary System Manager server fails or the data network partially loses connectivity. To use this feature, you must have a primary and secondary System Manager.

Before configuring Geographic Redundancy, you must install System Manager on standalone servers with separate IP addresses. If a managed product that supports Geographic Redundancy loses connectivity to the primary System Manager server, the secondary System Manager server provides the complete functionality. Failover does not occur automatically. You must manually activate the secondary System Manager server. For more information about System Manager Geographic Redundancy, see *Administering Avaya Aura® System Manager*.

Note:

Geographic Redundancy is supported with System Manager Release 7.0 and later.

Geographic Redundancy operational modes

This section describes server connectivity scenarios.

Normal Day connectivity

The primary System Manager server runs in Active mode while the secondary System Manager server runs in Standby mode. Standby mode provides limited functionality. In Active mode, the primary System Manager server manages all elements, including IP Office. Data is replicated from the primary to the secondary server.

Abnormal Day connectivity

The primary System Manager server fails or loses connectivity. The administrator can activate the secondary System Manager server, and the secondary server manages all elements.

To acquire licenses, IP Office sends a request to the secondary WebLM server and then to the primary server.

IP Office sends traps on the secondary server.

Management operations on IP Office, including backup and restore, can be done with System Manager through IP Office web services. Data replication takes place on the secondary server. All the jobs scheduled on the primary server are replicated on the secondary server and executed on schedule.

Split mode

One of the following conditions exist in Split mode:

- The primary and secondary System Manager servers run in Active mode but cannot communicate with each other due to a network connectivity outage.
- Managed elements cannot communicate with a System Manager server, but both System Manager servers can communicate with each other.

Licensing with Geographic Redundancy

The license file that you install on the primary System Manager server is replicated on the secondary System Manager server. When you activate the secondary System Manager server, the same license file works.

You must generate the license file by using the host ID of the primary System Manager server.

Sever data and file replication

Replication ensures consistency of the following data between the primary and the secondary System Manager servers:

- Inventories
- Scheduled jobs
- Users
- System configurations
- Templates that are stored in the database

The data and file replication process also replicates certificates from the primary to the secondary System Manager server. When you perform the Simple Certificate Enrollment Protocol (SCEP) process between IP Office and the primary System Manager server, secure and trusted interactions will also work between IP Office and the secondary System Manager server.

Geographic Redundancy configuration on IP Office, Unified Communication Module, and Application Server

Most of the following procedures can be performed on the IP Office, Unified Communication Module (UCM), and Application Server. Differences are clarified within the procedures.

You can configure IP Office for Geographic Redundancy using the IP Office Initial Configuration Utility (ICU). Alternatively, you can use IP Office Manager or IP Office Web Manager to perform the configuration. IP Office Manager can be accessed from System Manager.

Important:

Before you perform these procedures, you must enable Geographic Redundancy in System Manager. For information about the standard Geographic Redundancy configuration on System Manager, see *Administering Avaya Aura® System Manager*.

Adding the secondary server IP address in the Initial Configuration Utility

About this task

You can add additional System Manager servers to the IP Office Initial Configuration Utility (ICU), which can be registered as primary and secondary servers. The IP Office License configuration process stores the primary and secondary IP addresses for WebLM.

You can add the secondary server IP address when you:

- Deploy IP Office as an Enterprise branch with System Manager for the first time. ICU runs automatically.
- Reset or upgrade IP Office Branch to Release 10.0.

Note:

This configuration does not apply to the UCM and Application Server.

Procedure

On the Avaya IP Office Initial Configuration web console, in **Redundant SMGR Address**, type the secondary server IP address.

Setting the trap destination

About this task

The trap destination is automatically configured for both the primary and secondary servers when you configure Geographic Redundancy in the ICU. If you did not configure Geographic Redundancy in the ICU, use this procedure to add additional trap destinations that point to the primary and secondary System Manager servers.

Procedure

1. On the System Manager web console, in the **Elements** area, click **IP Office**.
2. For IP Office configuration, in the left navigation pane, click **System Configuration**.
3. In **Device List**, select an IP Office, and then click **Edit** to open IP Office Manager.

   Perform the following steps in IP Office Manager.
4. In the left navigation pane, click **System**.
5. Click the **System Events** tab, and then click **Alarms**.
6. In the **SNMP Traps** area, click a Server Address, and then click **Add**.
7. In the **New Alarm** area, select **Trap**, and do the following:
   a. In **Server Address**, type the secondary server IP address.
   b. In **Port**, type `10162`.
   c. In **Community**, type `public`.
   d. In **Format**, click **SMGR**.
   e. In **Minimum Security Level**, click **Warming**.
8. Click **OK**.
9. For UCM and Application Server configuration, in the left navigation pane of System Manager web console, click **UCM and Application Server** > **System Configuration**.

   Repeat steps 3 on page 183 to 8 on page 183 for completing the UCM and Application Server configuration.

IP Office licensing with Geographic Redundancy

IP Office requests a license from the WebLM server deployed on the synchronized primary and secondary System Manager servers.

IP Office sends license requests to the primary WebLM server. If the IP Office gets a response, then IP Office can acquire licenses and periodically check for licenses. If there is no response after three attempts, then the IP Office sends the request to the secondary WebLM server.

When the secondary WebLM server is nonfunctional , then the IP Office can acquire licenses from the primary WebLM server. This process continues until IP Office acquires licenses from one of the servers. If IP Office is rebooted, then the process restarts from the primary WebLM server.

Setting WebLM for licensing

About this task

The secondary WebLM server is automatically configured on the IP Office when you configure Geographic Redundancy in the ICU. If you do not configure Geographic Redundancy in the ICU, use this procedure to set the secondary WebLM for IP Office.

Note:

This configuration does not apply to the UCM and Application Server.

Procedure

1. On the System Manager web console, in the **Elements** area, click **IP Office** > **System Configuration**.
2. In **Device List**, select an IP Office, and then click **Edit** to open IP Office Manager.

   Perform the following steps in IP Office Manager.
3. In the left navigation pane, click **Licenses**.
4. Click the **Remote Server** tab.
5. In **Secondary Domain Name (URL)**, type the secondary server URL.
6. Click **OK**.

Setting SCEP

About this task

When you install a new IP Office for branch deployment, perform the installation when the primary System Manager is active and reachable. In this case, no configuration is needed for SCEP with the secondary System Manager server. The SCEP process is done between IP Office and the primary System Manager server. Synchronization between the two System Manager servers enables secure and trusted interactions to also work between IP Office and the secondary System Manager server. If you install a new IP Office while the primary System Manager is not active, then you must use this procedure to modify the IP Office security settings to point to the secondary server for SCEP exchange.

Procedure

1. On the System Manager web console, in the **Elements** area, click **IP Office**.
2. For IP Office configuration, in the left navigation pane, click **System Configuration**.
3. In **Device List**, select an IP Office, and then click **Edit** to open IP Office Manager.

   Perform the following steps in IP Office Manager.
4. In the left navigation pane, click **System**.
5. Click the **Certificates** tab.
6. In **SCEP Server IP/Name**, type the secondary server URL.
7. Click **OK**.
8. For UCM and Application Server configuration, in the left navigation pane of System Manager web console, click **UCM and Application Server** > **System Configuration**.

   Repeat steps 3 on page 184 to 7 on page 184 for completing the UCM and Application Server configuration.

Additional tasks for Geographic Redundancy

Additional tasks that you can perform include the following:

- Enable the Geographic Redundancy replication
- Disable the Geographic Redundancy replication
- Activate the secondary System Manager server
- Deactivate the secondary System Manager server
- Restore the primary System Manager server

For more information about these tasks, see *Administering Avaya Aura® System Manager*.

Note:

Geographic Redundancy is supported with System Manager Release 7.0 and later.

Optional standalone Secure Access Link Gateway configuration for remote service

Avaya Client Services (ACS) uses the Secure Access Link (SAL) Gateway to provide remote delivery of service to the IP Office. The supported configuration requires a standalone SAL Gateway that is deployed in the enterprise headquarters or data center and using the IP Office administration applications — Manager, System Status, and System Monitor.

SAL Gateway must be installed on a customer-provided server in the enterprise at a central location that allows for network connectivity to each deployed branch. The SAL Gateway manages the IP Office servers in multiple branches, relaying alarms from the IP Office back to Avaya, and proxying connection requests for support engineers. The SAL solution is fully customer controlled through the deployment and use of the optional SAL policy server.

Note:

System Platform's Virtual SAL Gateway (VSALGW) is not supported in managing each individual branch. The VSALGW is only officially supported by Avaya in management of system platform “on-board” devices such as System Platform, Session Manager, and System Manager. Each IP Office branch is considered as an “off-board” device.

Use of SAL to access the IP Office administration tools and System Manager

You are able to access the IP Office administration tools and Avaya Aura® System Manager through SAL.

- **Manager**

  Manager is an administration tool used to configure and upgrade the IP Office system. You can use Manager to administer each branch individually. You are able to use SAL to access the Manager application for local or remote configuration management of the IP Office system.

  Note:

  For IP Office upgrades and Embedded File Management, you must access Manager that is installed on a computer that resides within the customer network.

- **System Status Application**

  System Status is an administration tool used to monitor the current status of individual branches in the IP Office system. You are able to use SAL to access the System Status Application that is installed locally or remotely.

- **System Monitor** (Tier3/4 tool only)

  System Monitor is an administration tool that provides detailed traces of all activity on the IP Office system. System Monitor can connect to IP Office from outside the enterprise network through SAL. To connect System Monitor to IP Office through SAL, you must select **TCP** (and not use the default **UDP**) as the protocol when you start System Monitor. For more information, see *Using IP Office System Monitor*.

- **Avaya Aura System Manager**

  System Manager is a central management system that delivers a set of shared management services and a common console for System Manager and its components. System Manager provides a single access interface to administer multiple branch locations and multiple IP Officeusers or Centralized users. For more information about System Manager, see Management on page 15.

SAL Gateway installation and registration

To install SAL Gateway, see *SAL Gateway Implementation Guide*, which is available on the Avaya Support website http://support.avaya.com. You can also download the SAL Gateway software from the Avaya Support site.

Registering a product with Avaya is a process that uniquely identifies the device so that Avaya can service it. A SAL Gateway registration form is provided with your software download. For more information, see Universal Install SAL Registration Request Form on page 189. To register the

SAL Gateway, complete step 1 on the form and send it to salreg@avaya.com. The following information is requested in step 1:

- Your company name
- Avaya Sold-to Number (customer number)
- Your contact information, so that Avaya can contact you if there are questions

Avaya uses this information to register your gateway. When the registration is complete, Avaya will send you an email that provides the following information:

- The Solution Element ID and Product ID numbers
- A list of the devices currently registered at this location
- A list of other locations for your company

Note:

Optional: If you want to get Solution Element IDs (SEID) from other locations, complete the step 2 tab of the registration sheet and send it to salreg@avaya.com using the link included on the sheet. Avaya will send you a list of SEIDs from the locations you selected.

IP Office registration and SAL Gateway on-boarding

You must register each deployed IP Office with Avaya. To add managed devices to your SAL Gateway using the Solution Element IDs (SEID) provided to you during SAL Gateway registration. For more information, see “Managed element configuration” in *SAL Gateway Implementation Guide*.

When you have added all your managed devices, complete step 2 of the SAL Gateway registration form. For each managed device you added to your SAL Gateway, send the form to salreg@avaya.com. When this form is received, the Avaya registration team makes the appropriate changes to allow access to your managed devices through the SAL Gateway. Avaya will then confirm through an email notification that remote access to your product has been enabled through your SAL Gateway.

IP Office SAL-based alarming

The SAL Gateway supports alarming for the IP Office managed device. You must change the alarm destination on your IP Office managed device so that alarms are routed to your centralized SAL Gateway. During the registration and on-boarding process of each branch, the Avaya registration team also tests alarming through the SAL Gateway and back into Avaya alarm receivers.

Configuring the SAL Gateway as a trap destination in IP Office

About this task

Use this procedure to configure the SAL Gateway as a trap destination. A maximum of 5 Simple Network Management Protocol (SNMP) management stations can be configured as trap destinations.

System Manager is also configured as a trap destination. However, the configuration of System Manager as a trap destination is performed automatically when you run the Initial Configuration Utility. See Running the Initial Configuration Utility on page 61 for more information.

For more information about SNMP, see *IP Office Installing IP500/IP500 V2*.

Procedure

1. Start Manager and then connect to the IP Office system.
2. In the left navigation pane, click **System**.
3. Click the **System Events** tab.
4. In the **Configuration** sub-tab, in the **SNMP Agent** area, ensure that the **SNMP Enabled** check box is selected.
5. In **Community (Read-only)** , enter the SNMP community name to which the system belongs.

   This community name must match that used by the SNMP manager application when sending requests to the device. The community public is frequently used to establish communication and then changed (at both the SNMP agent and manager ends) for security.
6. In **SNMP Port**, accept the default.
7. In **Device ID**, enter the alarm ID or PID of the registered system.

   Note:

   This enables product alarming back to Avaya through the SAL. The unique alarm ID is included in the var-bind of all SNMP trap notifications sent by the system. The alarm ID, or PID, is parsed out of the alarm and used for automatic case creation by matching the registered system's customer record with the alarm event.
8. In **Contact**, enter contact information as appropriate.
9. In **Location**, enter location information as appropriate.
10. Click the **Alarms** tab.
11. Click **Add**.
12. In the **New Alarm** area, do the following:
    a. Click **Trap**.

b. In **IP Address** , enter the IP address of the computer running the SNMP manager application that you are adding as a trap destination.

   For example, the SAL Gateway.

c. In **Port**, enter the port on which the trap messages must be sent.

   This is the UDP port on which the IP Office system sends SNMP trap messages. The default is 162.

d. In **Community**, enter the community that will be used by the agent and the SNMP manager.

13. In **Events** area, select the check boxes for the events that you want to send.

    See the Manager online help for a description of the events.

14. Click **OK**.

15. Click **File** > **Save Configuration** to send the configuration back to the IP Office system, and then click **reboot**.

Universal Install or SAL Registration Request Form

Use this procedure to download the registration request form from the Avaya Support website.

1. Go to the Avaya Support website http://support.avaya.com.
2. Click **More Resources** > **Equipment Registration**.
3. In **Non-Regional (Product) Specific Documentation**, click **Universal Install/SAL Registration Request Form**.
4. Complete the registration form as instructed.

Chapter 7: Initial administration

User administration

This chapter provides the procedures to administer IP Office users from Avaya Aura® System Manager. All users are added to System Manager to enable centralized user management.

IP Office users are configured with an IP Office Endpoint profile and get their telephony features and services from the local IP Office. Centralized users are configured with a Session Manager profile and a CM Endpoint Profile, as well as an IP Office Endpoint profile that is based on a Centralized user template. Configuration of the Session Manager profile and CM 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 Rainy day. For more information about Centralized users, including the procedure to administer Centralized users, see *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*.

Note:

If the IP Office is not managed from System Manager, you are able to administer users from IP Office Manager. For more information, see Centralized management on page 15.

For an IP Office under System Manager Administration, if you add new hardware with Analog or Digital extension ports to a configured IP Office, then you might need to make a manual change to the IP Office configuration. This applies to adding:

- A new Analog or Digital extension card
- An Analog or Digital expansion unit
- A combo card

In such cases, you must do the following:

- Access the IP Office in unrestricted mode using IP Office Manager.
- Clear the **Base Extension** field of the Analog or Digital Extension records that were created due to this new hardware installation.

Otherwise, these Analog or Digital extensions will have extension numbers that block System Manager from being able to give the same numbers to users with IP extensions. If the Analog and Digital extension hardware is in place at the time of IP Office initial configuration, then the ICU automatically clears the **Base Extension** field of the Analog and Digital Extension records. The manual action is needed only if you add new hardware at a later stage.

Adding IP Office users to System Manager

About this task

When you add an IP Office user to System Manager, you must configure an IP Office Endpoint profile on System Manager. A Session Manager Profile and a CM Endpoint Profile are not configured for an IP Office user like they are when you add a Centralized user to System Manager. For information about adding Centralized users to System Manager, see *Administering Centralized Users for an IP Office Enterprise Branch*.

Procedure

1. On the System Manager console, under **Users**, click **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **New**.
4. On the New User Profile page, in the Identity section, do the following:
   a. In the **Last Name** field, enter the user's last name.

      Note:

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

   b. In the **Last Name** field, enter the user's last name.
   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. In the **Language** drop-down box, select the language for displaying the user name.
    b. In the **Display Name** field, enter the user's name.
    c. Click **Add**.
6. To add a TDM or IP endpoint, or a distributed SIP endpoint, click the **Communication Profile** tab.
7. Accept the default values for the **Communication Profile Password** field, **Confirm Password** field, **Name** field, and **Default** check box.
8. Click the **IP Office Endpoint Profile** check box, and do the following:
    a. In the **System** drop-down box, select the appropriate system.
    b. In the **Template** drop-down box, select the appropriate template. The templates listed in this drop-down box are IP Office 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. To assign an extension 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.

d. To change other parameters such as call appearances or feature buttons for this user, click the **Endpoint Editor** button and do the following:

   a. Update the fields as appropriate.

   b. Click **Save** to save your changes.

   c. Click **Exit** to exit the Endpoint Editor.

   This updates parameters for this user. The changes are not reflected in the template.

   Note:

   Parameters for this user can also be configured using the endpoint template. See Creating an endpoint template on page 80 for more information.

e. For the **Delete Extension On User Delete** check box, do one of the following:

   - Accept the default, unchecked, if you are using an analog or digital set type template and this feature is checked for other set types.
   - Select this check box if you want the extension to be deleted when the extension is unassigned or the communication profile is deleted.

9. Click **Commit**.

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

10. Repeat this procedure for each distributed user you want to add.

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 Setting the branch prefix and other fields in the Session Manager System Telephony tab on page 92.

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**.

Routine maintenance

IP Office upgrades

In branch deployments when IP Office is managed by Avaya Aura® System Manager, use the System Manager to perform IP Office software upgrades. For more information, see *Administering Avaya Aura® System Manager*.

Note:

You must deploy an external server next to System Manager so that System Manager uses it as a remote software library. System Manager manages the software download and the IP Office upgrade process, but the library storing the IP Office software image files must be on an external server.

When the IP Office is centrally managed by System Manager, the IP Office Manager Upgrade Wizard capability is disabled and cannot be used. If you must use the IP Office Manager Upgrade Wizard instead of System Manager, then edit the IP Office Security Configuration by selecting **Systems** > **Unsecured Interfaces** and enabling **Program Code**. For more information about IP Office upgrades, see *Deploying Avaya IP Office™ Platform IP500/IP500 V2*.

Backing up the system configuration using System Manager

About this task

Use this procedure to back up the IP Office device configuration. The IP Office device configuration contains the system configuration data and the user data. You can create a backup locally or on a remote server.

When you perform a backup of the system configuration from System Manager, the backup is stored on the local IP Office. To store the system configuration backup on the System Manager server, you must synchronize IP Office with System Manager. For more information on backup and restoration of IP Office devices, see *Administering 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 **Backups**.
3. On the IP Office Backup page, in **Backup Options**, click one of the following:
   - **Backup On Device**
   - **Backup On Remote Server**
4. In **Device List**, select the IP Office device for which you want to create a backup.
5. Click **Backups**.
6. If you clicked **Backup On Remote Server**:
   a. In **Select Remote Server**, click a remote server where you want to save the backup.
   b. **(Optional)** If you want to add a remote server, click **Add Server**.
   c. In **Backup Label**, type a name for the backup.
7. Choose on of the following options:
   a. Click **Now** to perform the backup immediately.
   b. Click **Schedule** to perform the backup at a specified time.

Related links

Synchronizing IP Office with System Manager on page 151

Restoring the system configuration using System Manager

About this task

Use this procedure to restore the IP Office device configuration. The IP Office device configuration contains the system configuration data and the user data. You can perform the restore operation from a local storage or a remote server.

Procedure

1. On the System Manager console, in the **Elements** area, click **IP Office**.
2. In the left navigation pane, click **Restore**.
3. On the IP Office Restore page, in **Restore Options**, click one of the following:
   - **Restore Backup Stored on Device(s)**
   - **Restore Backup Stored on Remote Server**
4. In **Device List**, select one or more IP Office devices for which you want to restore the configuration.
5. Click **Restore**.
6. **(Optional)** If you clicked **Restore Backup Stored on Device(s)**, in **Restore Options**, click one of the following:
   - **System Configuration**: To restore the respective system configurations to the IP Office device.

     The configuration you restore must be the latest configuration available in System Manager.
   - **User**: To restore the respective users from System Manager to the IP Office device.
   - **System Configuration and User**: To restore the respective system configurations and users from System Manager to the IP Office device.
   - **Restore Backup Stored on Devices**: To restore the locally backed up configuration to the IP Office device.
7. **(Optional)** If you clicked **Restore Backup Stored on Remote Server**:
   a. In **Select Remote Server**, click a remote server where you want to save the restore.

      If you want to add a remote server, click **Add Server**.
   b. Click **Get Restore Point**.
   c. In **Restore Point(s)**, select a restore point.
8. Choose one of the following options:
   a. Click **Now** to perform the restoration immediately.
   b. Click **Schedule** to perform the restoration at a specified time.

Configuring the http or https protocol for a remote server

About this task

Use this procedure to configure the remote server for using the HTTP or HTTPS protocol.

Procedure

1. On the remote server, install and activate the HTTPS and PHP packages.
2. On the System Manager server, do the following:
   a. Navigate to the `$ABG_HOME/httpfiles/` location.
   b. Copy the files with the `.php` extension to the backup location on the remote server.
3. On the remote server, grant full access permissions to the files that you copied in Step 2.
4. Start a browser and test the accessibility of the remote server in the network.

Upgrading the IP Office using System Manager

About this task

Use this procedure to upgrade the IP Office from System Manager. The steps include:

- Analyze the software to determine if a new version is available.
- Download the firmware files from Avaya PLDS to the software library that System Manager uses on an external server.

Avaya PLDS will automatically determine if a newer software version than what is currently installed is available. If there is a newer version available, you can download the newer version to upgrade the IP Office. To determine if there is a new software version available, Avaya PLDS uses the file *versions_sp.xml* that is available from the Avaya Support Site to compare the current installed software on the device with the latest available on Avaya PLDS. The file *versions_sp.xml* is regularly updated with the latest firmware/software releases available for upgrade.

Procedure

1. From the System Manager console, under **Services**, select **Software Management**.
2. On the **Software Management** page, click **Manage Software > IP Office**.
3. On the **IP Office** page, click the **Analyze** drop-down box and select **Now**.
4. When the analyze job is finished running, refresh the table.

   A red **x** indicates there is a newer firmware version available that has not been downloaded to the software library.
5. Select the control unit for upgrade, and click **Download**.
6. On the **Download Manager** page, do the following:
   a. In the **Library** drop-down box, select the appropriate library.

b. In the **Protocol** drop-down box, accept the protocol displayed.

Note:

The appropriate protocol is automatically selected based on the selected library.

c. Expand the tree to show a list of the upgrade packages that are available.

d. Under the Device Type **IP Office**, select the latest package.

7. Do one of the following:
   - Click **Now** to download the software.
   - Click **Schedule** to schedule the download at a specified time.
8. Click **Download**.

   The system displays the End User License Agreement page.
9. Click **Accept** to download the software.
10. When the download is complete, go to **Home** > **Services** > **Solution Deployment Manager** > **Manage Software** > **IP Office** > **UCM and IPO Application Server**.

    A yellow `i` indicates there is a newer version of software downloaded to the remote software library and the device can be upgraded.
11. Click the check box for the appropriate control unit.
12. Select your IP Office(s) and click **Get Inventory** and check if the **Job** is successful.
13. Select your IP Office(s) and click **Analyze Now** and check if the **Job** is successful.
14. Click **Upgrade**.

    The **Upgrade** button is enabled only if the state of the device is yellow.
15. On the **IP Office Upgrade Configuration** page, select the appropriate library and the release to which you want to upgrade.

    By default, the library which has the latest upgrade package is automatically selected.
16. Do one of the following:
    - Click **Now** to start the upgrade.
    - Click **Schedule** to schedule the upgrade at a specified time.
17. To view the upgrade status, on the **IP Office** page, click the IP Office being upgraded, then click **Status**.

Note:

Do not click the **Get Inventory** button while the upgrade is in progress. If you click this button, then the upgrade status hangs as **Running** even if the upgrade has completed. Moreover, if you click on the **Running** status link, the Operation Status area does not display correct and latest status updates for the upgrade tasks. As a workaround to resolve these false status-related issues, delete the respective IP Office element from

System Manager, restart the JBoss server, and then add the IP Office element back to System Manager.

When the upgrade is complete, a final status window is displayed. The state of the device turns green showing that it has the latest firmware installed.

Chapter 8: 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: Branch PSTN call routing examples

Each IP Office system can support its own external PSTN trunks. When deployed in an Avaya Aura® network, you have considerable flexibility over where outgoing PSTN calls should emerge from the network and similarly where incoming calls should be routed.

The following examples demonstrate some of the options available:

- Centralized call control on page 204 — External calls at a branch site can be rerouted to be dialed out at another site. This can be done for reasons of call cost and call control. For example, the central site may have a bulk call tariff for national and international calls that would benefit all branches.
- Branch PSTN Override on page 207 — Having configured the branch to send outgoing external calls to the Avaya Aura® Session Manager for onward routing, there may be cases where a specific number should still be routed via the branches own PSTN trunks.
- PSTN Fallback on page 209 — The IP Office can be configured to allow some calls that would normally use the SM Line to be routed via the PSTN when the Avaya Aura® SM Line is not available.

The various methods used in these examples can be combined to match the customer's needs. However the main aim should be as follows:

- To keep the branch configuration as generic as possible, i.e. to use the same PSTN call control in all branch configurations. This simplifies maintenance of multiple branches.
- To centralize as much of the PSTN call control in the Avaya Aura® Session Manager as possible. Again this simplifies maintenance and control.

Centralized call control

External calls at a branch site can be rerouted to be dialed out at another site, typically the headquarters site. This can be done for reasons of call cost and control and to reduce the external PSTN capacity required at the individual branch sites.

For example, we can route all national and international calls to the headquarters site to benefit from a bulk cost reduction available for calls from that site. The Avaya Aura® Session Manager there routes the calls out via PSTN services at that site. Note, however, that the Avaya Aura®

Session Manager could alternately use the trunks at a branch for some calls. For example, if the national call is to an area code that is local to a particular branch, the call could be routed to that branch for dialing on its PSTN trunks.

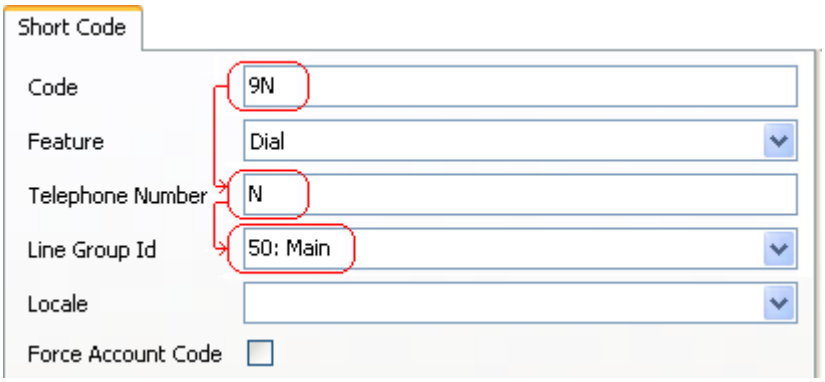
Routing IP Office calls — example

About this task

This example assumes that all the branches were initially setup with the default North American locale. For IP Office that means that a dial 9 prefix is used for external calls. For calls in other locales or between branches in different locals, the example would be adjusted to ensure that the resulting number received at the remote branch would be routed to an external PSTN trunk and is suitable for external dialing.

At each IP Office, we need to ensure that calls starting with 90, the external and then international number prefixes, are routed to the branch's SM Line rather than direct to an external PSTN line.

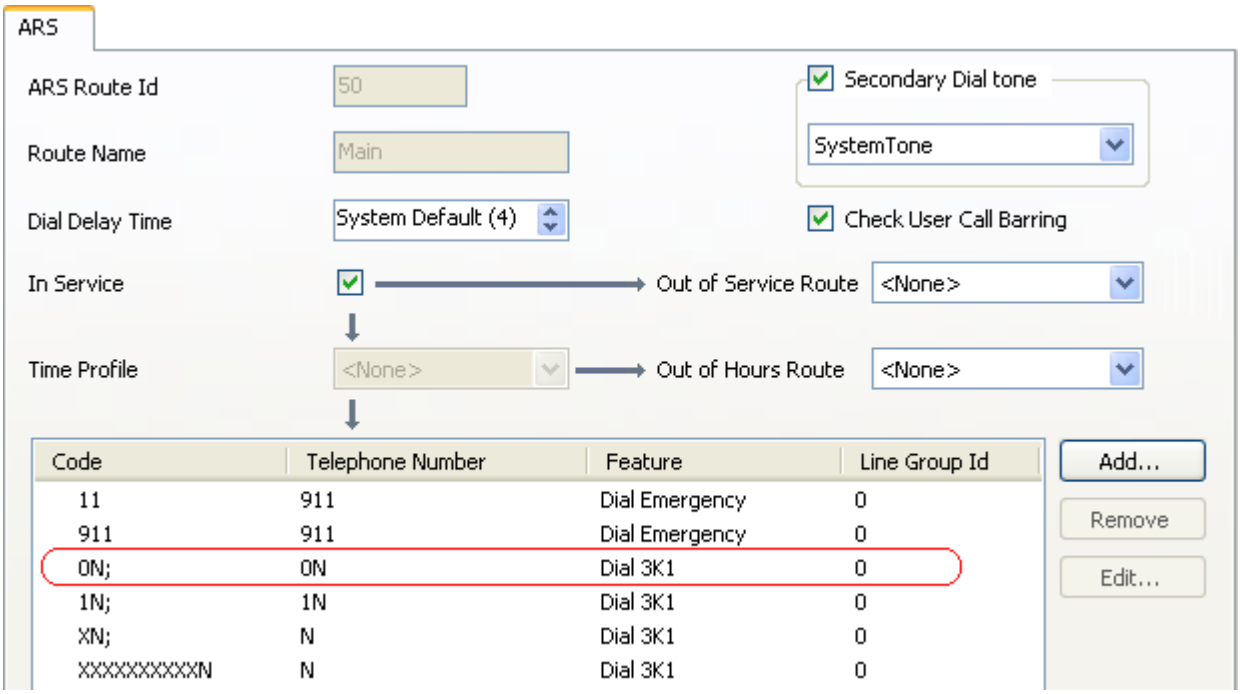
In the IP Office system configuration, the default system short code **9N** is used to match calls prefixed with a 9. The short code removes the 9 prefix and routes the call to the branch's ARS form **50: Main**.



Procedure

1. Start Manager and connect to the IP Office system.
2. In the left navigation pane, click **ARS**.

3. Click **50: Main**.



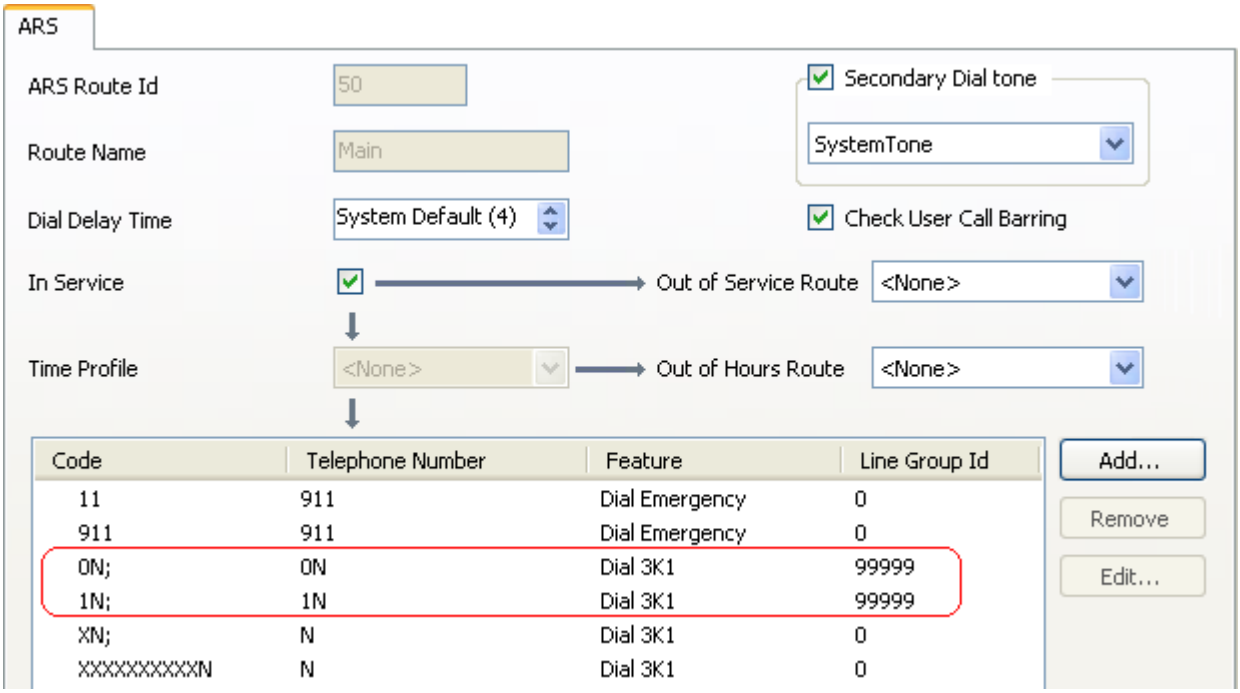
Within the ARS window, the default **0N;** short code that matches international numbers currently routes those calls to any available trunk in line group 0.

4. To edit the short code, click the short code.
5. Click the **Edit...** button.
6. Make the following changes:
   a. In the **Code** field, leave this set to **0N;**.
   b. In the **Feature** field, change this to **Dial**.
   c. In the **Telephone Number** field, change this to **90N**.

      The **9** has been added back as it matches the dial pattern typically used at the Avaya Aura® site for matching a call that needs routing to the PSTN.

   d. In the **Line Group ID** field, change this to match the SM Line Outgoing Group ID. The default is **99999**.
7. Click **OK**.
8. Repeat Steps 4 through 7 for the **1N;** short code which is used for national calls.

   The branch system's default ARS form is now set to route all national and international calls to the SM Line and thus to the Avaya Aura® Session Manager.



9. Click **OK**.
10. Click **File > Save Configuration**.

Branch PSTN override

In the example described in Centralized call control on page 204, we configured the branch system so that all national and international calls go to the headquarters site for routing to the PSTN. There may occasionally be scenarios where a particular number needs to override this and be dialed via the branch system's own PSTN trunks.

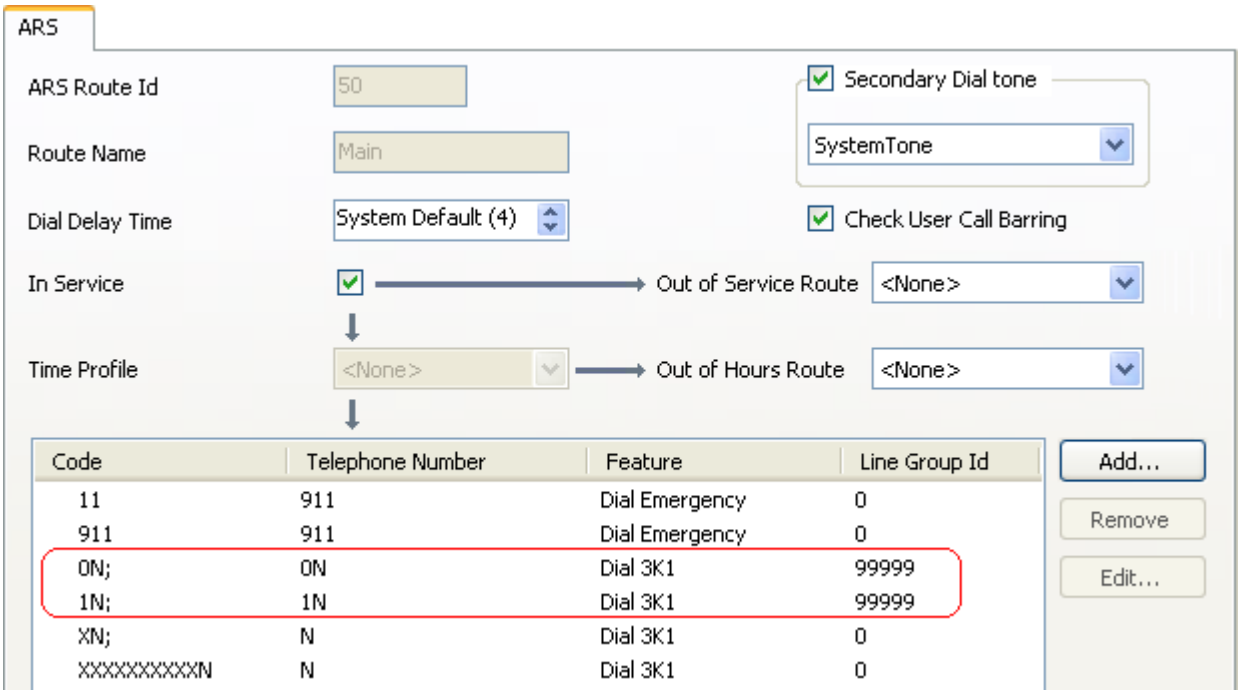
One example is the Avaya Aura Messaging or Modular Messaging PSTN number that can be configured for access to voicemail when the branch's SM Line is out of service. Another might be to provide a maintenance number to the headquarters site to report suspected loss of the SM Line connection.

Adding an overriding short code

Procedure

1. From the System Manager console, select the IP Office device and click **Edit** to edit the system configuration for the device. IP Office Manager starts on your computer.
2. In the left navigation pane, click **ARS**.

3. Click **50: Main**.



Within the ARS form, the default **1N;** short code is the one used for national calls. It would match the MM PSTN Number or AAM PSTN Number and attempt to route it to the SM Line which we know is out of service if the MM PSTN Number or AAM PSTN Number is being used for calls to voicemail. We can change the routing by adding a specific short code for the MM PSTN Number or AAM PSTN Number.

4. To add a short code, click the **Add...** button.
5. Make the changes as follows:
   a. In the **Code** field, set this to match the external PSTN number for Modular Messaging or Avaya Aura Messaging without the external dialing prefix.
   b. In the **Feature** drop-down box, select **Dial3K1**.
   c. In the **Telephone Number** field, set this to **N** to match the whole number in the **Code** field.

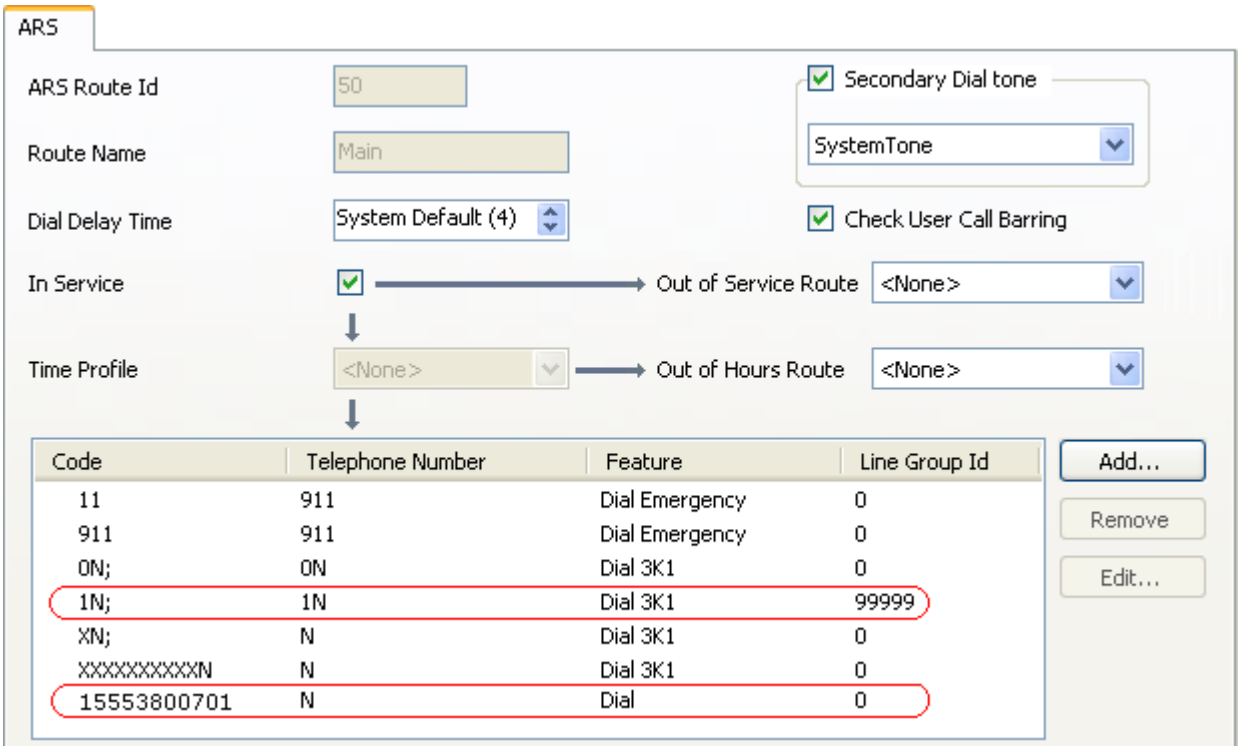
      Note:

      For a setup where the voicemail mail box numbers configured on Modular Messaging or Avaya Aura Messaging are the same as the caller's DID, the short code to route the PSTN call should be configured so that the caller ID is withheld. To do this, enter a `W` in the **Telephone Number** field of the short code. This ensures that during Rainy day operation, the voicemail system does not automatically go to the voicemail mail box of the caller based on the caller ID.

   d. In the **Line Group Id** drop-down box, select the line group ID being used for the branch's PSTN trunks. The default is 0.

6. Click **OK**.

   The ARS now has two short codes that will potentially match external national calls. However, one is a more exact match for certain calls and therefore will be applied to those calls.



7. Click **OK**.
8. Click **File > Save Configuration**.

PSTN trunk fallback

In branch scenarios where centralized call control and trunking (see Centralized call control on page 204) has been configured for certain calls, loss of the SM Line connection will impact making those calls. For instance, in our example where all branch national and international calls are routed via the headquarters site, loss of the SM Line will leave the branch users only able to make local calls (that includes any centralized extension users at the site who may be operating in survival mode).

Since loss of the SM Line should be infrequent and temporary, some restriction during that state may be acceptable. However the following options can be used to allow continued branch operation:

- If the headquarters site has multiple Avaya Aura®Session Managers for redundancy, each branch can also be configured with multiple SM Lines. See SM Line redundancy on page 105 for more information.
- As in our example business, centralized call control has not been applied to all branch local calls. Therefore local calls are still available without any additional configuration for the loss of the SM Line connection.
- Since loss of the SM Line should be infrequent and temporary, the loss of some services may be tolerable until the SM Line issue is resolved. However, even if that is the case, it may be recommended to configure a headquarters PSTN number that can be dialed to report the SM Line issue. See Branch PSTN override on page 207 for more information.
- Provide PSTN trunk fallback within the branch configuration. See Configuring PSTN trunk fallback on page 210. Note however that PSTN fallback will also occur when the number of external calls exceeds the available SIP trunk licenses.

Note:

If you want to have long distance routing on local trunks, be sure that the appropriate trunks have been ordered from the local provider. Do not create a route for international phone calls if you do not have that service.

Configuring PSTN trunk fallback

About this task

Use this procedure to provide PSTN trunk fallback with the branch configuration.

Procedure

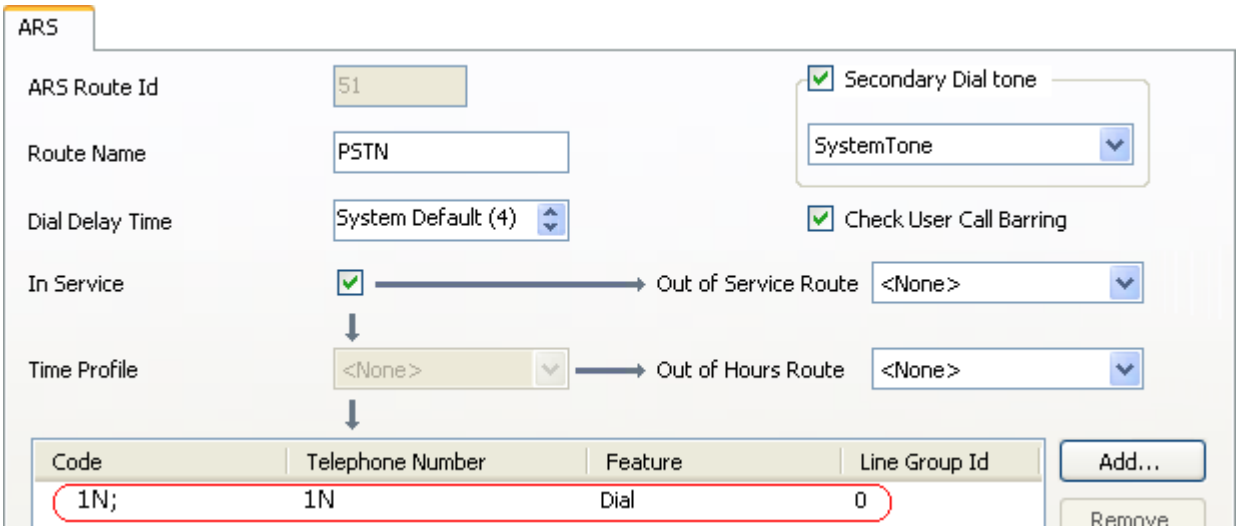
1. Start Manager and connect to the IP Office system.
2. In the left navigation pane, click **ARS**.
3. Click the **New** icon and select **ARS**.
4. Enter a **Route Name**, for example **PSTN**.
5. To add a short code click the **Add...** button.

   A short code is required that will send the national calls to the branch's own PSTN. Enter the normal defaults for such a short code as follows:
6. Make the changes as follows:
   a. In the **Code** field, enter **1N;**. For this example, **1N;** will match any national number dialing.
   b. In the **Feature** field, leave the entry set as **Dial3K1**.

c. In the **Telephone Number** field, enter **1N**. For this example **1N** will match the number dialed by the user after the dial 9 prefix.

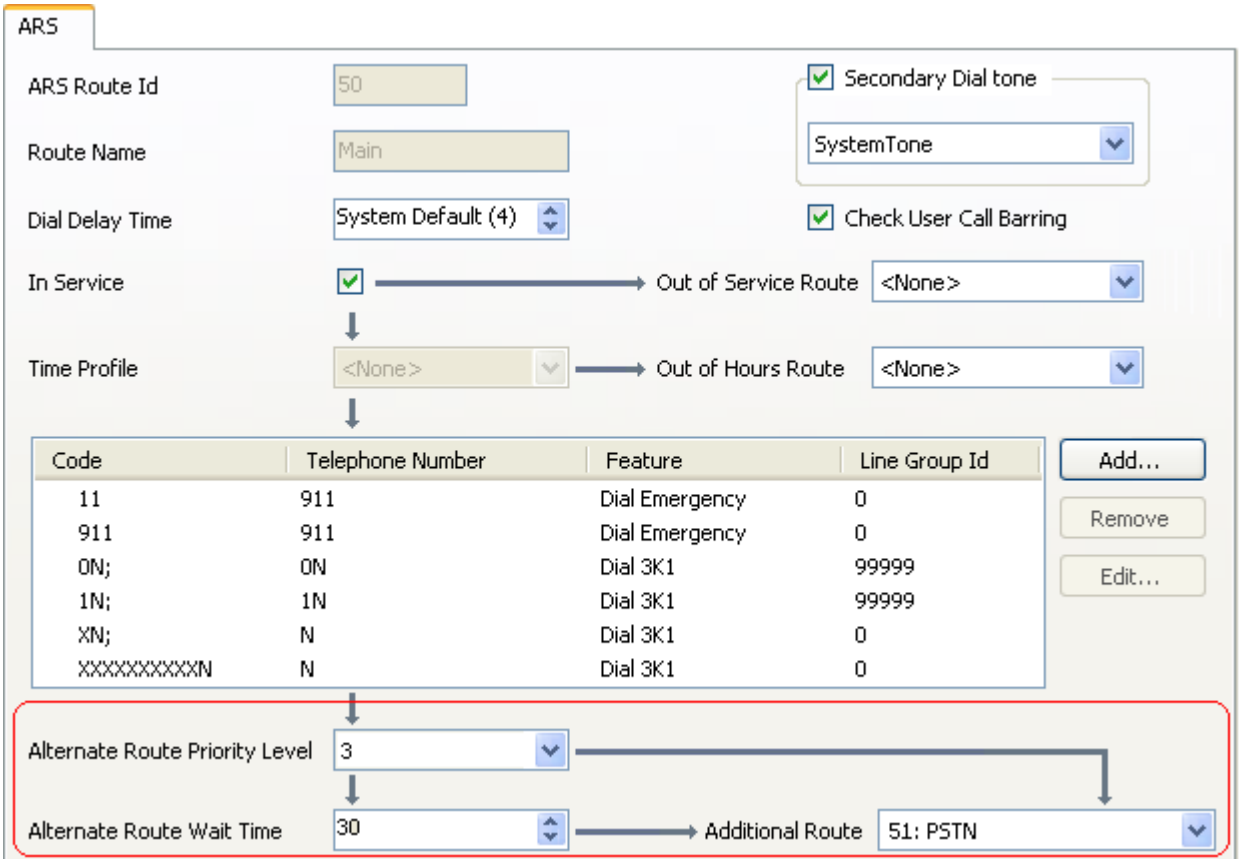
d. In the **Line Group Id** drop-down box, select the line group used for the IP Office system's external trunks. The default is 0.

7. Click **OK**.



8. Click **OK**.

9. Double click on the existing default ARS that was reconfigured to send all branch national and international calls to the SM Line.



10. In the **Additional Route** drop-down box , select the PSTN ARS form just created above.

    The form is now set such that, if the SM Line is not available (out of service or all licensed channels busy) calls can be checked for a dialing match in the PSTN ARS form. This works as follows:

    - The **Alternate Route Priority Level** controls which users are able to use the alternate route immediately, ie. those user's whose priority is equal or higher than this setting. The default priority for users is **5**.
    - The **Alternate Route Wait Time** is used for caller's whose priority is not sufficient to use the alternate route immediately. The default setting is 30 seconds. However, you may want to adjust this setting to one that meets your requirements.
    - Since the only short code match in the alternate route in our example is for national calls, international calls will continue to wait for the SM Line.

11. Click **File > Save Configuration**.

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

E

F

H

I

L

M

N

O

P

R

S

T

U

V

W

X