Migrating an IP Office or B5800 Branch Gateway to an IP Office Enterprise Branch

Release 11.1.1
Issue 4
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 7
Purpose 7
Document conventions 7
Change history 7
Chapter 2: IP Office as an enterprise branch overview 9
Topology 10
Branch deployment options 11
Supported telephones 13
Chapter 3: Migrating a standalone or Distributed enterprise branch to a Centralized enterprise branch 14
Checklist to migrate IP Office standalone or Distributed branch to IP Office Centralized branch 16
Turning off the automatic backup feature 18
Removing scheduled backup jobs 19
System configuration backup 19
Creating a backup of the system configuration using IP Office Manager 19
Backing up the system configuration using System Manager 20
IP Office upgrade options 21
Using the upgrade wizard 21
Upgrading the IP Office using System Manager 23
Upgrading the administration applications 25
Enabling secure communication after upgrading IP Office Manager 26
Bulk import of users 26
Exporting users to an xml file 27
Editing the xml file containing the users 27
Importing the users in bulk 29
About migrating individual PLDS license files to a WebLM server 30
Deleting the PLDS license file from the branch 30
Migration of IP Office users to Centralized users 31
User management changes for migration 31
9600 Series phone changes for migration 38
Licensing changes for migration 47
IP Office configuration changes for migration 47
Session Manager configuration changes for migration 48
Communication Manager configuration changes required for migration 48
Chapter 4: Upgrading a B5800 Branch Gateway to IP Office 49
Checklist to upgrade B5800 Branch Gateway to IP Office 50
Replacing B5800 Branch Gateway PLDS licenses with IP Office PLDS licenses 51
Reverting an IP Office system to a B5800 Branch Gateway system 52
Reapplying the IP Office user template to existing IP Office users in System Manager 54

Chapter 5: Upgrading an IP Office with a service pack 56
Service pack installation checklist 56
Synchronizing IP Office with System Manager 57
Configuration changes performed through IP Office Manager that cannot be synced with System Manager 57
Remote Software Library for IP Office upgrades 58
System requirements for the external server 59
Setting up the external server to work as a remote software library for upgrades 59
Getting inventory 60
Setting IP Office SNMP attributes 60
Configuring user PLDS access 61
Creating a software library 62
Chapter 6: Resources 63
Documentation 63
Finding documents on the Avaya Support website 63
Training 63
Viewing Avaya Mentor videos 64
Additional IP Office resources 65
Support 65
Using the Avaya InSite Knowledge Base 66
Accessing Avaya DevConnect Application Notes 66
Glossary 67

Chapter 1: Introduction

Purpose

This document is a supplemental guide that provides the tasks required to migrate a standalone IP Office system to an IP Office Distributed, Mixed, or Centralized enterprise branch.

Use this document in combination with *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

Document conventions

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

Table 1: Documentation terminology

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

Change history

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

Issue	Date	Summary of changes
Release 10.0, Issue 1	July 2016	• Moved Resources out of Introduction to an independent chapter called Resources. • Updated release number references and document title references throughout the document. • Rephrased information in checklists.

Table continues…

Issue	Date	Summary of changes
Release 11.0, Issue 1	June 2018	Added support for new phones: • Avaya J100 series IP desk phones: - Avaya J129 series desk phones. - Avaya J169/J179 phones (standard SIP phones only)
Release 11.0 SP1	August 2018	Added support phone: J139 support as standard SIP phone
Release 11.0.4.2	December 2019	Added support phone: J159 support as standard SIP phone
Release 11.1.FP1	January 2021	Added support phone: J189 support as standard SIP phone

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

Topology on page 10
Branch deployment options on page 11
Supported telephones on page 13

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.

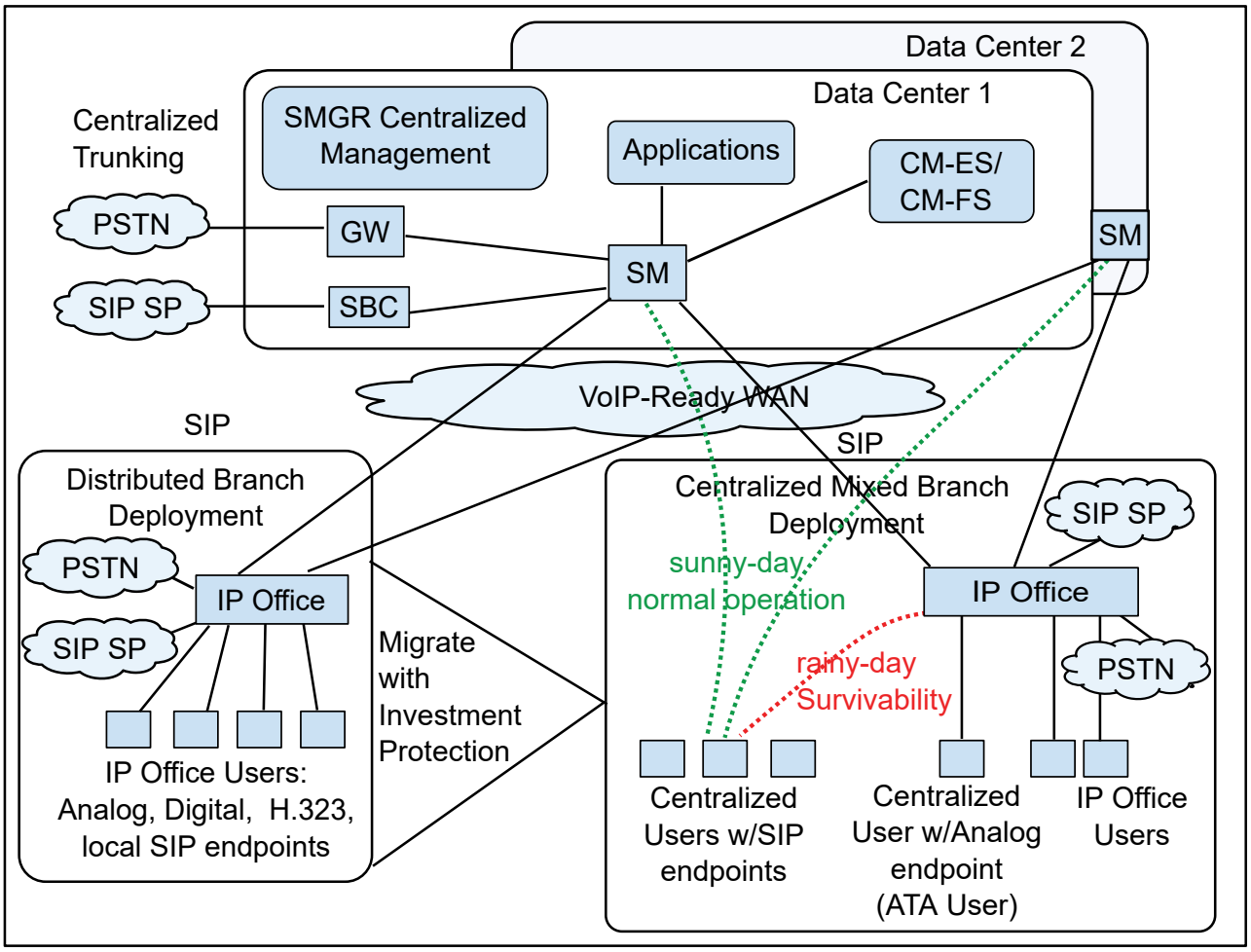

Figure 1: Topology of solution architecture

Related links

IP Office as an enterprise branch overview on page 9

Branch deployment options

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

standalone IP Office system. Existing IP Office systems can also be migrated to one of these deployment options.

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

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

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

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

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

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

Related links

IP Office as an enterprise branch overview on page 9

Supported telephones

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

- The following Avaya 9600 series phones running SIP firmware:
  - 9620 SIP 2.6.12
  - 9630 SIP 2.6.12
  - 9640 SIP 2.6.12
  - 9650 SIP 2.6.12
  - 9601 SIP 6.4
  - 9608 SIP 6.4
  - 9611G SIP 6.4
  - 9621G SIP 6.4
  - 9641G SIP 6.4
- Avaya one-X® Communicator SIP 6.2 (audio only)
- B179 phone
- 11xx and 12xx series SIP 4.4 phones
- Avaya J100 Series IP Phones:
  - Avaya J129 IP Phone
  - Avaya J139 IP Phone
  - Avaya J159 IP Phone
  - Avaya J169/J179 IP Phone
  - Avaya J189 IP Phone

Note:

The 9600 series SIP phones, and Avaya one-X® Communicator SIP are supported only as Centralized phones for use by Centralized users. They are not supported as IP Office phones for use by IP Office users.

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

Related links

IP Office as an enterprise branch overview on page 9

Chapter 3: Migrating a standalone or Distributed enterprise branch to a Centralized enterprise branch

One of the main capabilities of IP Office is support of the branch evolution phases. A standalone IP Office branch can migrate to a centralized solution in phases. For example, a standalone IP Office can first migrate to a Distributed enterprise branch deployment. Then at a later time evolve to include centralized management and licensing, centralized Avaya Aura® applications, and centralized SIP clients. For more information about the branch evolution phases, see *Avaya IP Office™ Platform in a Branch Environment Reference Configuration*.

This chapter describes the areas involved when migrating from a standalone IP Office to a fully centralized enterprise branch deployment, including Centralized users. A checklist that lists all the tasks required to migrate an IP Office to a Centralized enterprise branch is also provided. The migration process does not need to include all migration tasks described in this chapter. You can evolve the branch in phases as described in Checklist to migrate IP Office standalone or Distributed branch to IP Office Centralized branch on page 16.

The following areas are involved when migrating from a standalone IP Office system to a Centralized enterprise branch deployment including Centralized users:

- **Software upgrade to IP Office** — to enable the enterprise branch functionality, IP Office must be upgraded. Avaya recommends using the latest version of IP Office software.
- **Security settings** — to support IP Office, move to a more secure environment. When the Initial Configuration utility is run, new security settings are applied. During an upgrade, if the security settings are set to default, the Initial Configuration utility applies the new security settings. If the security settings are not set to default, the Initial Configuration utility does not apply the new security settings. All existing security settings remain, and the new configuration items are disabled. When the Initial Configuration utility is run, the Avaya SIP CA certificate automatically gets installed. This CA certificate is required for IP Office to trust the Session Manager identity certificate when connecting to Session Manager as well as the identity certificates of the WebLM server and of centralized 9600 Series SIP phones if applicable.
- **Avaya Aura System Manager centralized management** — migrating an IP Office to be managed by Avaya Aura® System Manager involves exporting IP Office users to an xml file, editing the xml file, and then importing them to System Manager. These tasks are performed using both IP Office Manager that is connected directly to the IP Office system and Avaya Aura® System Manager where some procedures are performed from the System Manager web console. The Initial Configuration utility (which is run after the users are exported to the xml file)

helps set up the IP Office connection to System Manager. Migrating IP Office users to Centralized users requires additional steps.

- **Licensing** — IP Office deployed as an enterprise branch supports centralized licensing by WebLM where a single license file is generated in Avaya Product Licensing and Delivery System (PLDS) for multiple branches. When WebLM centralized licensing is used, a WebLM license is required and connection to the WebLM server must be configured. Although centralized WebLM licensing is the recommended method, other licensing methods are supported including separate PLDS licenses, ADI licenses, and hybrid licensing where both PLDS and ADI licenses on the same IP Office are supported. It is recommended that IP Office systems using ADI licenses that are migrating to an enterprise branch deployment, convert their ADI licenses to PLDS. Converting ADI licenses to PLDS licensing must be performed manually.

  To add Centralized users to a deployment, Centralized IP Endpoints license is required. The Centralized IP Endpoints license and the WebLM license is available from PLDS.

- **IP Office connection to Avaya Aura® Session Manager** — An SM Line must be added to the IP Office configuration. If multiple Session Manager are available at the headquarters site, an additional SM Line can be added for SM Line redundancy. An IP Office SM Line, which connects to the Avaya Aura®Session Manager across the enterprise WAN, provides access to and from the Avaya Aura® network and allows for VoIP connectivity to other sites in the enterprise, to centralized trunking, and to centralized applications.

  If the IP Office has already been connected to Avaya Aura® Session Manager through an IP Office SIP trunk, the configuration should be changed to use the IP Office SM Line instead of the SIP trunk.

- **Centralized voicemail** — migrating an IP Office to a Centralized enterprise branch deployment includes configuring a centralized voice mail system. In an Avaya Aura®environment, Avaya Aura® Messaging and Modular Messaging are supported.

- **Services** — a standalone Secure Access Link (SAL) gateway must be deployed to provide remote delivery of service to the IP Office system.

- **Centralized users** — migrating IP Office users to Centralized users involves the following areas:

  - **Licensing**:

    - IP Endpoint licenses are uplifted to Aura licenses in PLDS. Investment credit is provided and Aura licenses are priced as an upgrade. IP Endpoint licenses are decremented in the same quantity as the purchased quantity of Avaya Aura® licenses. This is a manual process if the IP Endpoint licenses are ADI licenses, and an uplift process in PLDS if the IP Endpoint licenses are IP Office PLDS licenses.
    - Centralized IP Endpoint licenses are required.
    - SIP Trunk Channel licenses may be required.
    - To implement WebLM centralized licensing, the WebLM Model license is required. This license must be installed on the WebLM server and the IP Office systems must be configured to work with the WebLM server.

- **User Management** — Using Avaya Aura® Session Manager, Centralized users must be administered on Session Manager, Communication Manager, and on the IP Office system. This administration must be performed for Centralized users using SIP phones and Analog Terminal Adapters (ATAs). This administration is performed manually from Avaya Aura® System Manager for each user.
- **9600 Series phone firmware conversion** — Phone firmware must be converted from H.323 firmware to SIP firmware. Changes must be made to the phone settings and upgrade files. The Centralized SIP phones firmware files, settings, and upgrade files as well as the System Manager CA root certificate and SIP Product CA root certificate must be loaded on the file server. If IP Office is used as the file server for the Centralized SIP phones in their respective branches, these files can be pushed onto each IP Office in bulk from System Manager using the System Manager generic file transfer capabilities.
- **Optional configuration changes** — Optional configuration changes include changing the short-form dialing length, enabling SRTP, and changing SM Line monitoring settings and failback policy.

Related links

Checklist to migrate IP Office standalone or Distributed branch to IP Office Centralized branch on page 16
Turning off the automatic backup feature on page 18
Removing scheduled backup jobs on page 19
System configuration backup on page 19
IP Office upgrade options on page 21

Checklist to migrate IP Office standalone or Distributed branch to IP Office Centralized branch

Use this checklist to monitor your progress when you migrate an IP Office standalone or Distributed enterprise branch to an IP Office Centralized enterprise branch including Centralized users. Every task listed in the checklist need not be performed. The tasks you perform depend upon the capability and features you want to implement. For example, you might want to implement use of centralized applications, but not Centralized users. In this case, you would skip the tasks on configuring Centralized users.

#	Description	Notes	✔
1	Confirm that your version of Avaya Aura® System Manager is R6.3.	None.	
2	Turn the Automatic Backup setting off.	See Turning off the automatic backup feature on page 18.	

Table continues…

#	Description	Notes	✔
3	Create a backup of the system configuration.	See one of the following: • Creating a backup of the system configuration using IP Office Manager on page 19. • Creating a backup of the system configuration using System Manager on page 20.	
4	Upgrade IP Office. The upgrade wizard upgrades all of the IP Office components including the modules, cards, and phone firmware.	See one of the following: • Using the upgrade wizard on page 21. • Upgrading the IP Office using System Manager on page 23.	
5	Upgrade the administration applications.	See Upgrading the administration applications on page 25.	
6	To implement centralized management using Avaya Aura® System Manager, you must: • Add the IP Office systems to Avaya Aura® System Manager. • Perform a bulk import of the users. This includes exporting the users to an xml file, editing the file, and then importing the users to System Manager. • Generate an identity certificate for IP Office in Avaya Aura® System Manager. • Run the Initial Configuration utility. • Upload the auto attendant audio file.	See the following information in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*: • Adding IP Office to System Manager. This section describes the three different methods available to add IP Office systems to System Manager. • Preparing System Manager to issue an identify certificate for IP Office. • Running the Initial Configuration utility. • Uploading an auto attendant audio file. To perform a bulk import of users, see Bulk import of users on page 26.	
7	To migrate a standalone IP Office to a Distributed branch, you must configure an IP Office SM Line to Avaya Aura® Session Manager.	Review the information about administering an SM Line in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*. This section describes the tasks required to configure an SM Line between each branch site and the headquarters site.	
8	To implement centralized licensing by WebLM, you must: • Install the license file on the WebLM server. • Enable WebLM licensing for the branch.	See the following information in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*: • Moving activated license entitlements. • Enabling WebLM licensing for the branch. • Installing the shared PLDS license file on the System Manager WebLM server.	

Table continues…

#	Description	Notes	✔
9	To implement centralized voice mail, you must configure a centralized voice mail system.	See the following information in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*: • Configuring IP Office to use Avaya Aura® Messaging. • Configuring IP Office to use Modular Messaging.	
10	To migrate IP Office users to Centralized users, multiple configuration changes are required, including licensing changes, user management changes, and conversion of 9600 Series phone firmware from H.323 to SIP. When you add Centralized users to a branch, the branch is referred to as: • A Centralized enterprise branch where all users are Centralized users. • A Mixed enterprise branch where there are both IP Office users and Centralized users.	See Migration of IP Office users to Centralized users on page 31.	

Related links

Migrating a standalone or Distributed enterprise branch to a Centralized enterprise branch on page 14

Turning off the automatic backup feature

About this task

When B5800 Branch Gateway systems or IP Office systems are upgraded and managed from System Manager, you must turn off the Automatic Backup setting in IP Office Manager.

In IP Office, the Automatic Backup functionality that automatically schedules internal backups on the IP Office system when added to System Manager has been removed. When B5800 Branch Gateways or IP Office systems are upgraded, this feature becomes active. To avoid the possibility of a corrupt backup, you must turn the Automatic Backup setting off. Backups in IP Office ust be performed manually.

Procedure

1. Start IP Office Manager.
2. Select **File** > **Open Configuration**.
3. In the Select IP Office window, select the appropriate system.

4. In the left navigation pane, select **System**.
5. On the **System** tab, clear **Automatic Backup** .
6. Click **OK**.
7. Perform steps 1 on page 18 through 6 on page 19 for each B5800 Branch Gateway or IP Office that is upgraded.
8. If there are scheduled backup tasks already pending for these systems, remove the scheduled backup jobs. See Removing scheduled backup jobs on page 19.

Removing scheduled backup jobs

Procedure

1. On the System Manager console, in **Services**, select **Scheduler**.
2. In the left navigation pane, click **Pending Jobs**.
3. On the **Pending Jobs** page, click the check for the scheduled backup jobs you want to remove.
4. Click **More Actions** > **Disable**.

System configuration backup

You can use IP Office Manager or System Manager to create a backup of the system configuration.

Creating a backup of the system configuration using IP Office Manager

About this task

Before performing an upgrade, ensure you have a current backup of the IP Office system configuration. If you do not, use this procedure to create a backup of the system configuration.

Procedure

1. Start IP Office Manager.
2. Select **File** > **Open Configuration**.
3. In the Select IP Office window, select the appropriate system.
4. Click **OK**.

5. Enter the name and password for a service user account on that system.
6. Click **OK**.

   A BOOTP entry for the system is created in IP Office Manager. This also confirms communication between the computer that has IP Office Manager installed and the IP Office system.
7. Select **File** > **Save Configuration As...** and save a copy of the configuration file onto the computer.

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.

IP Office upgrade options

You can use the IP Office Manager upgrade wizard or System Manager to upgrade an IP Office system.

Related links

Migrating a standalone or Distributed enterprise branch to a Centralized enterprise branch on page 14
Using the upgrade wizard on page 21
Upgrading the IP Office using System Manager on page 23

Using the upgrade wizard

Before you begin

- Ensure that you have a current backup of the system configuration. See Creating a backup of the system configuration using IP Office Manager on page 19
- Uninstall the earlier version of IP Office Manager and install the latest version. See Upgrading the administration applications on page 25.

Procedure

1. Start IP Office Manager.
2. Click **File** > **Advanced** > **Upgrade**.
3. Select the check box for the appropriate system.
4. Click **Upgrade**.

   The **UpgradeWiz** scans for IP Office modules using the address specified in the **Unit/Broadcast Address** field.
5. If the expected control units are not shown, adjust the address in the **Unit/Broadcast Address** field, and click **Refresh**.

   The current version of each IP Office .bin file held in the control units memory is displayed. This is regardless of whether that .bin file is currently being used by any module in the system.

   In the **Available** column, IP Office Manager lists the versions of the available software. If IP Office Manager detects that there is a higher version available, the check box for that row is selected automatically.

   The information displayed depends on the type of control unit.

   - For IP500v2 control units, the current version of each IP Office .bin file held in the control units memory is displayed. This is regardless of whether that .bin file is currently being used by any module in the system.
   - For other control units, the current software version of the control unit and each external expansion module present in the system is displayed.

- If any of the modules have pre-version 2.1 software installed, an upgrade with **Validate** unchecked is required. If this is the case, only continue with the upgrade process using a PC with a fixed IP address on the same LAN domain and physical LAN segment as the IP Office control unit and only upgrade the pre-2.1 system.
- If a multi-stage upgrade is necessary, use the following additional steps to select the appropriate interim software:
  a. Right-click the upgrade wizard, and then click **Select Directory**.
  b. Locate and select the directory containing the bin file for the intermediate software level.

     The upgrade wizard should now list just the control unit as having upgrade software available.

6. Click the check box for the modules you want to upgrade.

   Note:

   If WAN3 modules are included in the system, do not check those modules. Each WAN3 module should be upgraded separately after the control unit and other modules in the same system have been upgraded.

7. Click the check box for validate.

   When this option is selected, the upgrade wizard checks the amount of free RAM memory available in the control unit to temporarily store the new bin files. If insufficient memory is available, you will be prompted whether to continue with an off-line upgrade or cancel upgrading. If offline is selected, the system is rebooted into offline mode. It may be necessary to use the **Refresh** option within the upgrade wizard to reconnect following the reboot. Validate upgrade can then be attempted again to check the amount of available RAM memory for transfer of bin files. If the memory is still insufficient, the option is offered to either do an unvalidated upgrade or cancel.

   During a validated upgrade, the bin files required are transferred to the system and stored in temporary memory. The backup system files and upload system files actions are performed. Once all file transfers are completed, the upgrade wizard prompts whether it is okay to proceed with the upgrade process. Select **Yes** to continue. Each module being upgraded will delete its existing core software, restart and load the new software file that was transferred. This process may take several minutes for each unit.

   Note:

   Ensure that the **Validate** check box is cleared only for IP Office systems with pre-2.1 software. An unvalidated upgrade must be done from a Manager computer with a fixed IP address running on the same LAN segment and subnet as the IP Office system. During the upgrade, the units and modules erase their current software and then request the new software file from Manager.

8. Select the following options as appropriate:
   - Click the check box for **Backup System Files** if, before upgrading to the new software, you want the current files in the System SD cards **/primary** folder copied to a **/backup** folder.
   - Click the check box for **Upload System Files** if you want the full set of software files that Manager has to be copied to the **/primary** folder on the System SD card. In addition to control unit and module software this will include phone software files. Following the reboot, the phone will upgrade using those files if necessary.
   - Click the check box for **Restart IP Phones** if you want all Avaya IP phones to be restarted following the upgrade and reboot. This will cause them to recheck whether the firmware they currently have loaded matches that on their configured file server. Use this option if the IP Office system is the file server and the upgrade included new IP phone firmware.
9. Click **Upgrade**.

   The system password for each system is requested.
10. Enter the system password and click **OK**.
11. Repeat this upgrade procedure again if you are performing a multi-stage control unit upgrade or if there are WAN3 modules in the system that are being upgraded separately.

Related links

IP Office upgrade options on page 21

Upgrading the IP Office using System Manager

About this task

Use this procedure to upgrade IP Office. The steps include:

- Analyzing the software to determine if a new version is available.
- Downloading the firmware files from Avaya PLDS.

PLDS will automatically determine if a new software version than what is currently installed is available. If there is a new version available, you can download the new version to upgrade IP Office. To determine if there is a new software version available, PLDS uses the `versions_sp.xml` file that is available on the Avaya Support Site to compare the current installed software on the device with the latest available on PLDS. The `versions_sp.xml` file is regularly updated with the latest firmware or software releases available for upgrade.

Procedure

1. On the System Manager console, in **Services**, select **Software Management**.
2. On the Software Management page, click **Manage Software > IP Office**.
3. On the IP Office page, click **Analyze** , and then select **Now**.
4. When the analyze job finishes, 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 **Library** , select the appropriate library.
   b. In **Protocol**, 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 IP Office being upgraded, then click **Status**.

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.

Note:

When a B5800 Branch Gateway is upgraded to IP Office, in the **Operation Status** section on the IP Office page, one of the tasks displays **Processing** in the **Status** column. After successful upgrade, **Processing** continues to appear in the **Status** column for that task. On the lower portion of the IP Office page, for the element (control unit) that was upgraded, the **Status** column displays **IDLE** and the **Current Version** column displays the new version. This information indicates the upgrade was successful.

Related links

IP Office upgrade options on page 21

Upgrading the administration applications

About this task

Use this task to upgrade the IP Office administration applications. The IP Office administration applications are Manager, System Status, and System Monitor.

Procedure

1. Using the **Add or Remove Programs** option in the Windows Control Panel, check that the PC does not have an earlier version of the IP Office Administration Suite installed. It there is, uninstall it.
2. Insert the IP Office Administrator Applications DVD.
3. Select IP Office Administration Suite.
4. Double-click on **setup.exe**.
5. Select the language you want to use for the installation process.

   This does not affect the language used by Manager when running.
6. Click **Next**.
7. Select who should be able to run the Administration Suite applications.
8. Click **Next**.
9. If required, select the destination to which the applications should be installed.

   It is recommended that you accept the default destination.
10. Click **Next**.

    The Custom Setup window appears.

11. Select the applications that you want to install. At a minimum select **System Monitor** and **Manager**.

    When you select an application, a description of the application appears. Click ▼ next to each application to change the installation selection.

12. Click **Next**.
13. Click **Install**.

    Installation of Windows .Net2 components may be required. If dialogs for this appear, follow the prompts to install .Net.

14. If requested, reboot the computer.

Enabling secure communication after upgrading IP Office Manager

About this task

If an earlier version of IP Office Manager is installed and you cannot connect to IP Office after IP Office Manager has been upgraded, you must enable the secure communication feature in IP Office Manager.

Procedure

1. Start IP Office Manager.
2. Select **File > Preferences**.
3. Click the **Security** tab.
4. Select **Secure Communications** .
5. Click **OK**.

Bulk import of users

To import users to System Manager in bulk, you must perform the following tasks:

- Export the users to an xml file – see Exporting users to an xml file on page 27
- Edit the xml file – see Editing the xml file containing the users on page 27
- Import the users to System Manager– see Importing the users in bulk on page 29

Note:

Under certain circumstances, you may need to reboot IP Office after users are added through System Manager import of a user xml file. If existing users are exported to an xml file from IP Office that does not have the WebLM server enabled, the exported users will not have the

Reserve License field set appropriately for WebLM. At a later time, IP Office may have the WebLM server enabled, for example after running the Initial Configuration utility to set the IP Office up to connect to System Manager and WebLM. If at that later time the users in that xml file are imported to System Manager, these users will be added to IP Office from System Manager without the **Reserve License** field set appropriately for WebLM. Rebooting IP Office after completing the System Manager import process will adjust the IP Office user configuration.

Exporting users to an xml file

About this task

Use this task to export users from a standalone IP Office system to an xml file.

Be sure to perform this task before you launch the Initial Configuration utility. After you launch the Initial Configuration utility, the System Manager administration feature for the branch is enabled and the users on the IP Office are deleted so they will not be available for export.

Procedure

1. Start Manager and connect to the IP Office system.
2. Select **Tools > Export > Users**.
3. In the **Export Users** dialog box, click the check boxes for the users you want to export.

   Note:

   Do not include **NoUser** or **RemoteUser**.
4. In the **Domain Name** field, enter the appropriate domain name.
5. Browse to the folder where you want to save the .xml file.
6. Click **OK**.
7. In the **Export Users** dialog box, click **OK**.

Editing the xml file containing the users

About this task

Use this task to edit the fields in the xml file so that the data matches the requirements for the corresponding fields in System Manager. The fields described in this task are those required for IP Office users.

Procedure

1. Using a text editor, open the xml file that contains the exported users.

2. For each user, edit the following fields to match the System Manager field constraints:
   a. Edit the **<authenticationType>** field to specify **basic**, for example **<authenticationType>basic</authenticationType>**.
   b. If the **<givenName>** field does not contain an entry, edit the **<givenName>***first name*</**givenName>** field where *first name* is the user's first name.

      Note:

      The entry for this field is derived from the **Full Name** field that is configured when a user is added to the system. The **Full Name** field is configured in IP Office Manager in the **User > User** tab. If the **Full Name** field was not completed when the user was added to the system, the **<givenName>** field for the user will be blank when the user is exported to the xml file. The **<givenName>** field must contain a value. Do not use punctuation characters such as **#**, **?**, **/**, or **,**. Do not begin the entry with a space.
   c. Edit the **<loginName>***login name for the user*</**loginName>** field where *login name for the user* is in the format *loginname@somedomain.com*, for example **Extn5411000@avaya.com**.
   d. Edit the **<preferredLanguage>** field to specify **en_US**, for example **<preferredLanguage>en_US</preferredLanguage>**.
   e. If the **<surname>** field does not contain an entry, edit the **<surname>***last name*</**surname>** field where *last name* is the user's last name.

      Note:

      The entry for this field is derived from the **Full Name** field that is configured when a user is added to the system. The **Full Name** field is configured in IP Office Manager in the **User > User** tab. If the **Full Name** field was not completed when the user was added to the system, the **<surname>** field for the user will be blank when the user is exported to the xml file. The **<surname>** field must contain a value. Do not use punctuation characters such as **#**, **?**, **/**, or **,**. Do not begin the entry with a space.
   f. Edit the **<userPassword>***password for the user*</**userPassword>** field so that the password complies with System Manager user password constraints. The System Manager user password cannot be only numeric. This is the password used to log into System Manager.
   g. Edit the **<commProfileType>** field to specify **IP Office**, for example **<commProfileType>IP Office</commProfileType>**.
   h. Edit the **<csm:deviceName>***name of device*</**csm:deviceName>** field to match the Managed Element name of the device as it was added in System Manager.

      This field is exported as the System name field in the IP Office configuration so it must be changed to match the Managed Element name of the device in System Manager.
   i. Edit the **<csm:userTemplate>***name of template*</**csm:userTemplate>** field where *name of template* is the appropriate endpoint template for this user. The template

must match the name of the IP Office Endpoint template that was created in System Manager.

The IP Office Endpoint template can be an H.323, analog, or digital template. Enter the appropriate endpoint template for each user that you are migrating. For more information about the IP Office Endpoint template, see *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

j. Edit the **<csm:extension>***user's extension***</csm:extension>** field where *user's extension* is the user's extension.

k. Edit the **<csm:extensionType>** field to specify **SIP**, for example **<csm:extensionType>SIP</csm:extensionType>**.

l. Edit the **<csm:deleteExtOnUserDelete>** field to specify **true**, for example **<csm:deleteExtOnUserDelete>true</csm:deleteExtOnUserDelete>**.

3. Save and close the xml file.

Importing the users in bulk

About this task

Use this procedure to import the users to System Manager.

Procedure

1. On the System Manager console, in **Services**, select **Bulk Import and Export**.
2. Click **Import > User Management > Users**.
3. On the Import users page, in **Select File**, click **Browse** and select the appropriate xml file.
4. For **Select error configuration**, select one of the following options:
   - **Abort on first error**
   - **Continue processing other records**
5. For **Select import type**, select **Complete** .
6. For **If a matching record already exists**, select one of the following options:
   - To skip users in the import file that match the existing user records in the database, click **Skip**.
   - To update and merge the user attributes data from the imported file to the existing data, click **Merge**.
   - To replace the users in the database with the new users from the imported file, click **Replace**. Use this option to import new users and retain the existing users.
   - To delete the user records in the database that match the records in the imported file, click **Delete**.

7. To run the job, in the **Job Schedule** section, select one of the following options:
   - To import the users immediately, click **Run immediately**.
   - To import the users at a specified time, click **Schedule later**, and set the date and time.
8. Click **Import**.

   Note:

   The operations, Communication Manager Synchronization and Bulk Import of users, must not overlap in time. If Bulk Import of users is in progress and Communication Manager Synchronization is started, the current records under process fail. After the synchronization is complete, the remaining bulk import records process successfully. You must reimport the records that fail during synchronization.
9. To verify the file was exported successfully, click **View job**. **SUCCESSFUL** should appear in the **Status** column.

About migrating individual PLDS license files to a WebLM server

You can migrate the individual PLDS license files to the System Manager WebLM server. This requires that you first move the individual PLDS license files from one license host to another license host (that is, from the IP Office to the System Manager WebLM server) and then install the shared license file on the System Manager WebLM server. To perform these tasks, see the following topics in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

- Moving activated license entitlements (to move the activated license entitlements from the current host ID, which is the individual IP Office, to the host ID of the WebLM server).
- Enabling WebLM licensing for the branch.
- Installing the shared PLDS license file on the System Manager WebLM server.

Also see Deleting the PLDS license file from the branch on page 30.

Deleting the PLDS license file from the branch

About this task

After the license entitlements in PLDS have been moved from the individual IP Office license file to the shared WebLM license file, the individual license file installed on each IP Office must be deleted.

Note:

Failure to delete the individual license file on the IP Office will create a violation of the end user license agreement.

Procedure

1. Start Manager and connect to the IP Office system.
2. Select **File > Advanced > Embedded File Management**.
3. Do the following:
   a. Select the first IP Office system.
   b. Right-click the file name **PLDSkeys.xml**.
   c. Click **Delete**.
4. Repeat Step 3 on page 31 for each branch.

Migration of IP Office users to Centralized users

The migration of IP Office users to Centralized users involves several areas including user management changes, licensing changes, and 9600 Series phone firmware conversion from H.323 to SIP.

As you migrate IP Office users to Centralized users, see *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*. This guide is a supplemental guide that provides the tasks required to add Centralized users to an IP Office enterprise branch and is intended to be used in conjunction with the information provided in this section.

User management changes for migration

To migrate IP Office users to Centralized users, each user must have a profile on the central Session Manager and Communication Manager, as well as centralized user and extension records on the IP Office. When you add a Centralized user to System Manager, you must configure a Session Manager profile and a Communication Manager profile. These steps must be performed manually from Avaya Aura® System Manager for each user.

To migrate a Centralized user to an IP Office user, the user's Session Manager profile and Communication Manager profile are removed.

Note:

If you are using Avaya Aura® System Manager to edit an existing B5800 Branch Gateway R6.2 user and the System Manager version is R6.3.2, you must ensure that the **Local Number Length** field is configured correctly in IP Office Manager. If it is not, you will not be able to modify the extension. An error message will appear that indicates the extension length

is invalid. For information on how to configure the **Local Number Length** field in IP Office Manager, see “Setting the branch prefix and local number length for extension numbering” in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

The following assumptions apply:

- IP Office management is performed centrally by Avaya Aura® System Manager.
- All users and extensions are appropriately configured as users in a Distributed enterprise branch and operational.
- For each branch user, a user record exists in Avaya Aura® System Manager with an IP Office profile, and with no Session Manager or Communication Manager profiles.

Note:

If a user record does not exist in Avaya Aura® System Manager you must export the user data from IP Office and import the data to Avaya Aura® System Manager.

Converting an IP Office user to a Centralized user

About this task

Use this task to update the user's existing System Manager user record. You must perform this task for each user that is migrating from the Distributed enterprise branch to a Centralized enterprise branch. Repeat this procedure for each IP Office user you want to convert to a Centralized user.

Procedure

1. On the System Manager console, in **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. On the **Communication Profile** tab, scroll to the bottom of the page and select **IP Office Endpoint Profile**.
6. Click **Commit & Continue**.

   The user and extension are deleted from the IP Office.
7. In **Communication Profile Password**, enter the appropriate communication profile password.
8. In **Confirm Password**, enter the password again.
9. Accept the default values for the **Name** field and the **Default** check box.
10. Expand the **Communication Address** section, and do the following:
    a. Click **New**.
    b. In the **Type** drop-down box, select **Avaya SIP**.

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

   The extension number will typically have to be changed from a short IP Office local extension number to a longer enterprise-wide number that often includes the branch prefix as the first digits. For example, if the distributed extension number was **yyyy** and the branch prefix was **xxx**, then after migration the centralized extension number will be **xxxyyyy**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

d. In the **Extension** field, enter the same extension number you added in the **Fully Qualified Address** field in Step 10c on page 33.

Note:

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

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

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

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

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

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

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

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

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

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

m. Click **Commit & Continue**.

Note:

Be sure to click **Commit & Continue** before continuing with the Step 10 on page 32. When you click **Commit & Continue**, System Manager automatically populates the **Extension** and **Set Type** fields when you configure the IP Office Endpoint Profile.

13. Select **IP Office Endpoint Profile** , and do the following:

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

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

Note:

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

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

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

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

14. Click **Commit**.

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

Converting a Centralized user to an IP Office user

About this task

Use this task to update the user's existing System Manager user record. You must perform this task for each user that is migrating from the Distributed enterprise branch to a Centralized or Mixed enterprise branch.

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. On the **Communication Profile** tab, scroll to the bottom of the page and clear the following check boxes:
   a. **Session Manager Profile** .
   b. **CM Endpoint Profile** .
   c. **IP Office Endpoint Profile**.
6. Click **Commit & Continue**.

   The user and extension are deleted from IP Office and from System Manager.
7. 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.

      When you select a template, the **Set Type** field is automatically populated based on the template selected. The template must be an IP Office non-centralized user template.
   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. For more information, see “Creating an endpoint template” in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

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.

8. Click **Commit**.

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

9. Repeat this procedure for each Centralized user you want to convert to an IP Office user.

About converting users in bulk

The System Manager bulk export and import feature provides the capability to convert multiple users to Centralized users, rather than one at a time as described in Converting an IP Office user to a Centralized user on page 32.

Adding a Session Manager Profile and Communication Manager Endpoint Profile to IP Office users

About this task

Use this task to add a Session Manager Profile and Communication Manager Endpoint Profile to multiple users that are existing IP Office users in System Manager. This task includes the steps to export the IP Office users from System Manager to an xml file, edit the xml file, and then import the users back to System Manager. The CLI utility is used to export the IP Office users from System Manager to an xml file.

Procedure

1. Log in to System Manager using SSH as **root**.
2. Go to ***$MGMT_HOME*/bulkadministration/exportutility** where ***$MGMT_HOME*** is an environment variable that represents the System Manager HOME path.

   The CLI utility is located in this directory.

3. From the CLI utility, run the **exportUpmUsers.sh** script. For more information, see the About bulk export of users section in the *System Manager on-line help*.

   The system exports all user records to an xml file in the parent directory.

4. Open the xml file and modify the following for *each* user you want to convert to a Centralized user.

   a. Remove all user data. User data is data within the starting tag **<ns2:data>** and ending tag **</ns2:data>**.

   b. Add the xml tags for the IP Office Endpoint Profile. For more information, see the XML Schema for IP Office Communication Profiles and Sample xml for the IP Office Communication Profiles sections in the *System Manager on-line help*.

   c. Modify the **userTemplate** tag in the IP Office Endpoint Profile to specify the default Centralized SIP template. For example, **<ns2:userTemplate>Default Centralized SIP Template</ns2:userTemplate>**

      Note:

      If you do not want to use the Default Centralized SIP template, you can create a new Centralized user template and use that one instead. In that case, you would specify the name of the new Centralized user template within the **userTemplate** tags.

   d. Add the xml tags for the Session Manager Profile. For more information, see the XML Schema Definition for bulk import of Session Manager profiles and Sample XML for bulk import of Session Manager profiles sections in the *System Manager on-line help*.

   e. Add the xml tags for the Communication Manager Endpoint Profile. For more information, see the XML Schema Definition for bulk import of endpoint profiles and Sample XML for bulk import of endpoint profiles sections in the *System Manager on-line help*.

   f. Change the IP Office extension number to match the Communication Manager extension number.

5. If there are users in the xml file that you do not want to convert to a Centralized user, delete those users from the xml file.

6. Import the users back to System Manager. See Importing the users in bulk on page 29.

   Note:

   When performing this task, on the **Import users** page, click **Replace** for **If a matching record already exists**, .

7. Synchronize the IP Office system configuration and users with System Manager. For more information, see the Synchronizing the IP Office system configuration section in the *System Manager on-line help*.

Adding an IP Office Endpoint Profile to existing System Manager users

About this task

Use this task to add an IP Office Endpoint Profile for multiple users that are existing users of Session Manager and Communication Manager. Although this task may not typically be required, you may need to add the IP Office Endpoint Profile to multiple System Manager users in the following circumstances:

- There are Session Manager SIP users in the branches but without a survivable gateway. At a later time, IP Office systems are added to the branches.
- There are IP Office systems in the branches and users have been configured as Centralized users from a standalone IP Office Manager application and not from System Manager. If the solution is upgraded to include central management of the IP Office systems from System Manager, the IP Office Endpoint Profile must be added to the Centralized users in System Manager.

Procedure

1. Follow the steps in Adding a Session Manager Profile and CM Endpoint Profile to existing IP Office users on page 36.
2. Exclude step 4 d on page 37 and e on page 37. The Session Manager Profile and Communication Manager Endpoint Profile are already included in the xml file for these users.

9600 Series phone changes for migration

Conversion from H.323 to SIP and migration from a Distributed to a Centralized IP Office configuration are supported for the 9600 Series telephones that are listed in Supported telephones on page 13.

Note:

The 9620, 9630, 9640, and 9650 phones are older versions of the 9600 Series phones while the 9601, 9608, 9611G, 9621G, and 9641G are newer versions. The steps to convert the older versions and the newer versions of the 9600 Series phones are slightly different.

About the SIG parameter and converting 9600 Series phones from H.323 to SIP

To convert the 9600 Series phones from H.323 phones to SIP phones, the SIG parameter, among other phone settings parameters, must be configured on the phones. Depending on the phone, the SIG parameter can be set as follows:

- For branches where *all* 9608, 9611, 9621, and 9641 phones need to be converted from H.323 to SIP, a NoUser Source Number string (SET_96xx_SIG=2) can be added to the IP Office system configuration which will force IP Office to add the line **SET SIG 2** to the 9608, 9611, 9621, and 9641 phone sections in the 46xxsettings.txt file. This will convert all 9608, 9611, 9621, and 9641 phones in IP Office Branch to SIP. The conversion from H.323 to SIP for these phones can be performed remotely.

- For branches where *some* 9608, 9611, 9621, and 9641 phones need to be converted from H.323 to SIP while other phones in the branch remain H.323 phones, the SIG parameter must be set locally on the phone. It cannot be set in the 46xxsettings.txt file.
- For branches where *some* except for 9608, 9611, 9621, and 9641 phones need to be converted from H.323 to SIP while other phones in the branch remain H.323 phones, and for branches where *all* except 9608, 9611, 9621 and 9641 phones need to be converted to SIP, the SIG parameter must be set locally on the phone. It cannot be set in the 46xxsettings.txt file.

DHCP and phone configuration file server

Avaya IP phones deployed in a Distributed enterprise branch get their configuration files and firmware from the local IP Office as a file server. They typically also use the local IP Office as a DHCP server.

When the supported 9600 Series SIP phones are deployed in a Centralized enterprise branch, the primary method for phone firmware download is centralized as well. In this mode the phones get their settings file and firmware file from a central HTTP server. However, if this method cannot be used, for example due to WAN bandwidth concerns, an alternative method may be used leveraging IP Office located in the branch where the phones are located.

The phone will get the address of its file server, whether it is a central server or the IP Office, in the DHCP response it receives from the DHCP server. There are multiple options available to set up DHCP servers in a Centralized branch deployment, as follows:

- A central DHCP server can be used (with scopes per branch for per-branch IP addressing).
- The IP Office can be used as a DHCP server.
- A separate local DHCP server in the branch can be used.

Whether a local DHCP server or central DHCP server (with scopes per branch) is used, the DHCP response to the phone can indicate either a per-branch configuration file server or a central file server common to all branches, depending on the model chosen for setting up the configuration file server.

When migrating from a Distributed to Centralized branch, the phone configuration files appropriate for the Centralized deployment have to be uploaded onto the file server, either the central server or the IP Office depending on the method chosen. If using a central file server, then a change is needed in the DHCP server to provide the phones with the address of the central file server.

For more information about downloading files for the 9600 Series phones, see the following guides:

- *Installing and Maintaining Avaya one-X ® SIP for 9601, 9608, 9611G, 9621G, and 9641G*, document number 16-603504
- *Administering Avaya one-X ® Deskphone SIP for 9601, 9608, 9611G, 9621G, and 9641G*, document number 16-601944
- *Avaya one-X® Deskphone Edition for 9600 Series SIP IP Telephones Installation and Maintenance Guide*, document number 16-601943

Converting 9608, 9611, 9621, and 9641 phones from H.323 to SIP

About this task

This task can be performed remotely. The changes required to convert 9608, 9611, 9621, and 9641 H.323 phones to SIP phones are made by first adding a NoUser Source Number to the IP

Office system configuration which will convert 9608, 9611, 9621, and 9641 H.323 phones in IP Office Branch to SIP phones. Then changes are made to the upgrade file and settings file that can be remotely loaded onto the IP Office System SD card.

In this task, IP Office is used as the file server for the phones.

Note:

The SIG parameter on the phones that are to be upgraded to SIP should remain set with the default value, **default**. A SIG parameter setting of **default** allows the phones to be converted to SIP based on the value of the SIG parameter in the settings file. If there are 9608, 9611, 9621, and 9641 phones you want to convert to SIP and their SIG parameter was manually changed to **H.323**, you must set it back to **default** to allow it to be converted.

Procedure

1. In the IP Office system configuration, add the NoUser Source Number string **SET_96xx_SIG=2**. See Adding a NoUser Source Number to set the phone SIG parameter to SIP in the auto-generated settings file on page 42 for the instructions on how to add a NoUser Source Number to the IP Office system configuration.

   The NoUser Source Number string will force the IP Office system to add the line **SET SIG 2** to the 9608, 9611, 9621, and 9641 phone sections in the **46xxsettings.txt** file. This will convert 9608, 9611, 9621, and 9641 phones in the IP Office Branch to SIP.

2. Download the following files from the Avaya Support website at http://support.avaya.com/:

   - **Avaya one-X ® Deskphone SIP 6.2.2 Software for the 9601/9608/9611G/9621G/ 9641G IP Deskphones** – this is the SIP software distribution package that comes as a zip file. It contains the upgrade and firmware files required to upgrade the Centralized SIP phones from one release to the next and to convert phones from H.323 to SIP.
   - **46xxsettings.txt file** – this file contains option settings that you are able to customize for your enterprise.

3. Prepare the files as follows:

   a. Unzip the SIP software distribution package and have its entire content ready to be loaded.

   b. Rename the **46xxsettings.txt** file to **96xxSIPsettings.txt**.

      Important:

      You must rename **46xxsettings.txt** file to **96xxSIPsettings.txt**. Do not make a copy of the file and name it **96xxSIPsettings.txt**

   c. Edit the new **96xxSIPsettings.txt** file as appropriate for the centralized deployment.

      For information about the parameters that must be configured for centralized deployments, see the Centralized phone settings section in *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*.

   d. Edit the upgrade file to point to the new SIP settings file as follows:

      a. Using a text editor, open the **96x1Supgrade.txt** file that is included in the SIP software distribution package.

b. Change the name of the settings file to **96xxSIPsettings.txt**.

The new **96xxSIPsettings. txt** file will reside on the IP Office system SD card with the existing **46xxsettings.txt** file. The **96xxSIPsettings. txt** file will provide the settings for the Centralized SIP phones after they are converted. The **46xxsettings.txt** file will continue to provide the settings for other types of phones that remain H.323 IP Office phones.

e. If the phones register using the TLS protocol, the System Manager CA root certificate and the SIP Product CA root certificate must be included in the list of files installed on the file server. These certificates must be downloaded from System Manager. For more information about downloading the System Manager CA root certificate and downloading the SIP Product CA root certificate, see *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*.

The System Manager CA root certificate must be installed on the file server in order for the phones to trust the System Manager CA root certificate so they can verify the IP Office Identity Certificate that is signed by the System Manager CA. The TRUSTCERTS setting must also be configured in the **96xxSIPsettings.txt** file that is described in Step 3 c on page 40. When the TRUSTCERTS parameter is included in the phone settings file, the SIP Product CA root certificate must be included in the list of files installed on the file server.

Note:

If the phones register using the TCP protocol, they do not need certificates.

4. Load the files listed in Step 3 on page 40 onto the IP Office System SD card in the System or Primary folder.

   These files include the files in the SIP software distribution package and the new settings file you created in Step 3 on page 40.

   You are able to remotely load these files onto the IP Office System SD card from System Manager using the System Manager file transfer mechanism. This mechanism allows you to push the files to multiple IP Office systems in bulk. For more information about using the System Manager File Transfer feature to load files to the IP Office, see *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

5. Do not change the DHCP server setting. This ensures that the HTTP server address provided in the DHCP responses to the phones is the address of the IP Office.
6. If the IP Office itself is used as the DHCP server for the phones, ensure that the **Phone File Server Type** in the IP Office system configuration **System** tab is set to **Memory Card**.
7. Reboot the phones as follows:

Note:

At this point, the phones are still operating with H.323 firmware as IP Office phones so they can be forced to reboot from the IP Office.

- To reregister the phones using the System Status application, perform the following steps:
  a. Open the System Status application for the IP Office.
  b. Select **System > H323 Extensions > Avaya IP Phones**. A list of all registered phones is displayed.
  c. Select 9608, 9611, 9621 and 9641 H.323 phones.
  d. Click **Reregister**.
- To reset the phones using the System Monitor application, perform the following steps:
  a. Open the System Monitor application for the IP Office.
  b. Select **Status > H323 Phone Status**.
  c. Select 9608, 9611, 9621, and 9641 H.323 phones.

  Note:

  You can use **Shift** + click or **Ctrl** + click to select more than one phone.

  d. Click **Reset Phones**.

Adding a NoUser Source Number to set the phone SIG parameter to SIP in the auto-generated settings file

About this task

Use this task to set the SIG parameter for the 9608, 9611, 9621, and 9641 phones in the 46xxsettings.txt file to SIP (2). This task sets the SIG parameter in the 46xxsettings.txt file that is auto-generated by the IP Office system. This task does not set the SIG parameter directly on the phones. This task is a system configuration task performed from IP Office Manager. Repeat this procedure for adding a NoUser Source Number to another IP Officesystem.

Note:

This task applies only when converting *all* 9608, 9611, 9621, and 9641 H.323 phones in an IP Office Branch to SIP.

Procedure

1. Disable the System Manager administration feature for IP Office. See the About disabling the System Manager administration feature for an IP Office section in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*, document number 18-603853.
2. Start IP Office Manager and connect directly to the branch.
3. In the left navigation pane, click **User**.

4. In the middle **User** pane, click **NoUser**.
5. Click the **Source Numbers** tab and click **Add**.
6. In the **Source Number** field, enter `SET_96xx_SIG=2`.
7. Click **OK**.
8. Select **File > Save Configuration**.

Converting 9608, 9611, 9621, and 9641 phones with SIG parameter from H.323 to SIP

About this task

This task cannot be performed remotely. On phones that are being converted to SIP, the phone SIG parameter must be set to SIP and this must be performed directly on the phones.

In this task, IP Office is used as the file server for the phones.

Procedure

1. Download the following files from the Avaya Support website at http://support.avaya.com/:
   - **Avaya one-X ® Deskphone SIP 6.2.2 Software for the 9601/9608/9611G/9621G/ 9641G IP Deskphones** – this is the SIP software distribution package that comes as a zip file. It contains the upgrade and firmware files required to upgrade the Centralized SIP phones from one release to the next and to convert phones from H.323 to SIP.
   - **46xxsettings.txt file** – this file contains option settings that you are able to customize for your enterprise.
2. Prepare the files as follows:
   a. Unzip the SIP software distribution package and have its entire content ready to be loaded.
   b. Rename the **46xxsettings.txt** file to **96xxSIPsettings.txt**.

      Important:

      Be sure to *rename* the **46xxsettings.txt** file to **96xxSIPsettings.txt**. Do not make a copy of the file and name it **96xxSIPsettings.txt**

   c. Edit the new **96xxSIPsettings.txt** file as appropriate for the centralized deployment.

      See the Centralized phone settings section in *Administering Centralized Users for an IP Office™ Platform Enterprise Branch* for information on the parameters that must be configured for centralized deployments.

   d. Edit the upgrade file to point to the new SIP settings file as follows:
      a. Using a text editor, open the **96x1Supgrade.txt** file that is included in the SIP software distribution package.
      b. Change the name of the settings file to **96xxSIPsettings.txt**.

      The new **96xxSIPsettings. txt** file will reside on the IP Office System SD card with the existing **46xxsettings.txt** file. The **96xxSIPsettings. txt** file will provide the

settings for the Centralized SIP phones after they are converted. The **46xxsettings.txt** file will continue to provide the settings for the phones that remain H.323 IP Office phones.

e. If the phones register using the TLS protocol, the System Manager CA root certificate and the SIP Product CA root certificate must be included in the list of files installed on the file server. These certificates must be downloaded from System Manager. For more information, see the Downloading the System Manager CA root certificate and Downloading the SIP Product CA root certificate sections in *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*.

The System Manager CA root certificate must be installed on the file server in order for the phones to trust the System Manager CA root certificate so they can verify the IP Office Identity Certificate that is signed by the System Manager CA. The TRUSTCERTS setting must also be configured in the **96xxSIPsettings.txt** file that is described in Step 3c. When the TRUSTCERTS parameter is included in the phone settings file, the SIP Product CA root certificate must be included in the list of files installed on the file server.

Note:

If the phones register using the TCP protocol, they do not need certificates.

3. Load the files listed in Step 2 onto the IP Office System SD card in the System or Primary folder.

   These files include the files in the SIP software distribution package and the new settings file you created in Step 2.

   You are able to remotely load these files onto the IP Office System SD card from System Manager using the System Manager file transfer mechanism. This mechanism allows you to push the files to multiple IP Officesystems in bulk. For more information, see the Using the System Manager File Transfer feature to load files to the IP Office system section in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

4. Do not change the DHCP server setting. This ensures that the HTTP server address provided in the DHCP responses to the phones is the address of the IP Office.
5. If the IP Office itself is used as the DHCP server for the phones, ensure that the **Phone File Server Type** in the IP Office system configuration **System** tab is set to **Memory Card**.
6. For each phone that should be converted to SIP, change the SIG parameter on the phone to SIP as follows:
   a. Enter the setup menu on the phone.
   b. Enter the appropriate password. The default is `<MUTE>CRAFT#`
   c. Scroll down to and select **SIG**.
   d. Select **SIP**.
   e. Perform steps a through d for each phone that is being converted from H.323 to SIP.

Note:

The phones automatically reboot when the SIG parameter is changed.

Converting 9600 series phones from H.323 to SIP

About this task

This task cannot be performed remotely. For phones that are to be converted to SIP, the phone SIG parameter must be set to SIP directly on the phones.

In this task, IP Office is used as the file server for the phones.

Procedure

1. Download the following files from the Avaya Support website at http://support.avaya.com/:
   - **Avaya one-X® Deskphone SIP 2.6.10 Software for 9600 IP Deskphones** – this is the SIP software distribution package for the 9620, 9630, 9640, and 9650 phones. It comes as a zip file and contains the upgrade and firmware files required to upgrade the Centralized SIP phones from one release to the next and to convert phones from H.323 to SIP.
   - **46xxsettings.txt file** – this file contains option settings that you are able to customize for your enterprise.
2. Prepare the files as follows:
   a. Unzip the SIP software distribution package and have its entire content ready to be loaded.
   b. Rename the **46xxsettings.txt** file to **96xxSIPsettings.txt**.

      Important:

      Be sure to *rename* the **46xxsettings.txt** file to **96xxSIPsettings.txt**. Do not make a copy of the file and name it **96xxSIPsettings.txt**
   c. Edit the new **96xxSIPsettings.txt** file as appropriate for the centralized deployment.

      For more information about the parameters that must be configured for centralized deployments, see the Centralized phone settings section in *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*.
   d. Rename the **96xxupgrade.txt** file that came in the SIP software distribution package to **96xxupgradeSIP.txt**.

      Important:

      Be sure to *rename* the **96xxupgrade.txt** file to **96xxupgradeSIP.txt**. Do not make a copy of the file and name it **96xxupgradeSIP.txt**.
   e. Edit the new **96xxupgradeSIP.txt** file to point to the new SIP settings file as follows:
      a. Using a text editor, open the **96xxupgradeSIP.txt** file.
      b. Change the name of the settings file to **96xxSIPsettings.txt**.

      The new **96xxSIPsettings. txt** file will reside on the IP Office System SD card with the existing **46xxsettings.txt** file. The **96xxSIPsettings. txt** file will provide the

settings for the Centralized SIP phones after they are converted. The **46xxsettings.txt** file will continue to provide the settings for the phones that remain H.323 IP Office phones.

f. If the phones register using the TLS protocol, the System Manager CA root certificate and the SIP Product CA root certificate must be included in the list of files installed on the file server. These certificates must be downloaded from System Manager. For more information, see the Downloading the System Manager CA root certificate and Downloading the SIP Product CA root certificate sections in *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*.

The System Manager CA root certificate must be installed on the file server in order for the phones to trust the System Manager CA root certificate so they can verify the IP Office Identity Certificate that is signed by the System Manager CA. The TRUSTCERTS setting must also be configured in the **96xxSIPsettings.txt** file that is described in Step 3c. When the TRUSTCERTS parameter is included in the phone settings file, the SIP Product CA root certificate must be included in the list of files installed on the file server.

Note:

If the phones register using the TCP protocol, they do not need certificates.

3. Load the files listed in Step 2 onto the IP Office System SD card in the System or Primary folder.

   These files include the files in the SIP software distribution package and the new settings file and upgrade file you created in Step 2.

   The original **96xxupgrade.txt** file included in the SIP software distribution package has been renamed to **96xxupgradeSIP.txt** so that when it is loaded onto the IP Office System SD card, it will not override the auto-generated **96xxupgrade.txt** file. The new **96xxupgradeSIP.txt** file and the IP Office auto-generated **96xxupgrade.txt** file will co-reside on the IP Office System SD card. The **96xxupgradeSIP.txt** file will be used for except 9608, 9611, 9621, and 9641 phones SIP phones while the IP Office auto-generated **96xxupgrade.txt** file will be used for the phones that remain as H.323 phones.

   You are able to remotely load these files onto the IP Office System SD card from System Manager using the System Manager file transfer mechanism. This mechanism allows you to push the files to multiple IP Office systems in bulk. For more information, see the Using the System Manager File Transfer feature to load files to the IP Office system section in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

4. Do not change the DHCP server setting. This ensures that the HTTP server address provided in the DHCP responses to the phones is the address of the IP Office.
5. If the IP Office itself is used as the DHCP server for the phones, ensure that the **Phone File Server Type** in the IP Office system configuration **System** tab is set to **Memory Card**.

6. For each phone that should be converted to SIP, change the SIG parameter on the phone to SIP as follows:
   a. Enter the setup menu on the phone.
   b. Enter the appropriate password. The default is `<MUTE>CRAFT#`
   c. Scroll down to and select **SIG**.
   d. Select **SIP**.
   e. Scroll to and select **Restart Phone** to reboot the phone.
   f. Perform steps a through e for each phone that is being converted from H.323 to SIP.

Licensing changes for migration

Migrating IP Office users to Centralized users involves the following licensing changes:

- IP Office Avaya IP endpoint licenses are uplifted to Aura licenses in PLDS. Investment credit is provided and Aura licenses are priced as an upgrade. Avaya IP endpoint licenses are decremented in same quantity as purchased quantity of Aura licenses. The endpoint license conversion is managed as follows:
  - If the endpoint licenses are ADI licenses, the conversion to Aura licenses in PLDS is performed manually by Avaya Products Ops.
  - If the endpoint licenses are IP Office PLDS licenses, the conversion to Aura licenses is an uplift process in PLDS.
- Centralized Endpoint licenses available in PLDS must be acquired. See the Activating license entitlements section in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.
- SIP Trunk Channel licenses available in PLDS must be acquired if SIP trunks are going to be configured. See the Activating license entitlements section in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.
- WebLM mode license may have to be acquired if the migration triggers a change to WebLM centralized licensing.
- If WebLM centralized licensing is used, the central license file must be generated and installed on the WebLM server. The IP Office systems must be configured to work with the WebLM server.

IP Office configuration changes for migration

The following IP Office configuration changes may be required for migration:

- Changing the type of voice mail system configured for the system if the migration involves a change from a local voice mail option to a central voice mail solution.

- Modifying Incoming Call Routes that are specific to extension numbers that have changed.
- Changing hunt groups from Local to Centralized.

Session Manager configuration changes for migration

The following Session Manager configuration changes may be required for migration:

- Changing the Session Manager call routing configuration through Routing Policies and Dial Patterns.
- Defining the Session Manager location for the Centralized branch and defining IP address maps on Session Manager to map the Centralized users' endpoints in that branch to that location.
- Adding emergency calling rules so Session Manager can send emergency calls originating from the Centralized users in the given branch location to the IP Office in that branch.

Communication Manager configuration changes required for migration

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 the Configuring direct media on Communication Manager section in *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*.

Chapter 4: Upgrading a B5800 Branch Gateway to IP Office

The areas listed below are involved when upgrading from a B5800 Branch Gateway Distributed branch deployment to an IP Office Distributed enterprise branch deployment. Once the B5800 Branch Gateway is upgraded to an IP Office Distributed enterprise branch, the tasks required to implement the branch as a Centralized enterprise branch are the same as described in Checklist to migrate IP Office standalone or Distributed branch to IP Office Centralized branch on page 16 .

- **Software upgrade to IP Office** — a software upgrade to later version of IP Office can be performed on the existing platform and SD card of the B5800 Branch Gateway system. New hardware or a different SD card are not required. The software upgrade can be performed remotely. For B5800 Branch Gateway R6.2 systems, Avaya Aura® System Manager is used to perform the upgrade.
- **Configuration data** — B5800 Branch Gateway configuration data is automatically transferred and applied to IP Office.
- **Security settings** — to support IP Office, move to a more secure environment. When the Initial Configuration utility is run, new security settings are applied. During an upgrade, if the security settings are set to default, the Initial Configuration utility applies the new security settings. If the security settings are not set to default, the Initial Configuration utility does not apply the new security settings. All existing security settings remain, and the new configuration items are disabled. When the Initial Configuration utility is run, the Avaya SIP CA certificate automatically gets installed. This CA certificate is required for IP Office to trust the Session Manager identity certificate when connecting to Session Manager as well as the identity certificates of the WebLM server and of centralized 9600 Series SIP phones if applicable.
- **Licensing**:
  - B5800 Branch Gateway PLDS licenses must be replaced by IP Office PLDS licenses. This license migration must be performed manually.
  - To implement WebLM centralized licensing, the WebLM Mode license must be installed on the WebLM server and WebLM licensing must be enabled on IP Office.

  Management — The method used to manage the B5800 Branch Gateway – that is, IP Office Manager or Avaya Aura® System Manager – can continue to be used after the system is upgraded to the later version of IP Office.

Note:

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

- **Services** — The Secure Access Link (SAL) gateway can continue to be used for remote delivery of service to the IP Office system.

Related links

Checklist to upgrade B5800 Branch Gateway to IP Office on page 50
Replacing B5800 Branch Gateway PLDS licenses with IP Office PLDS licenses on page 51
Reverting an IP Office system to a B5800 Branch Gateway system on page 52

Checklist to upgrade B5800 Branch Gateway to IP Office

Use this checklist to monitor your progress as you upgrade a B5800 Branch Gateway Distributed branch to later version of IP Office. When the B5800 Branch Gateway is upgraded to an IP Office Distributed enterprise branch, the tasks required to implement the branch as a Centralized enterprise branch are the same as described in Checklist to migrate IP Office standalone or Distributed branch to IP Office Centralized branch on page 16 beginning with Step 7.

#	Description	Section	✔
1	Confirm that your version of Avaya Aura® System Manageris R6.3.	—	
2	Turn the Automatic Backup setting off.	See Turning off the automatic backup feature on page 18.	
3	Create a backup of the system configuration.	See one of the following: • Creating a backup of the system configuration using IP Office Manager on page 19 • Creating a backup of the system configuration using System Manager on page 20	
4	Upgrade IP Office. The upgrade wizard upgrades all of the IP Office components including the modules, cards, and phone firmware.	See one of the following: • Using the upgrade wizard on page 21 • Upgrading the IP Office using System Manager on page 23	

Table continues…

#	Description	Section	✔
5	Upgrade the administration applications.	See Upgrading the administration applications on page 25	
6	Replace the B5800 Branch Gateway PLDS licenses with IP Office PLDS licenses.	See Replacing B5800 Branch Gateway PLDS licenses with IP Office 9.0 PLDS licenses on page 51	
7	Migrate the branch to a Centralized enterprise branch which includes: • Implementing centralized management • Implementing centralized licensing • Implementing centralized voicemail • Migrating IP Office users to Centralized users	Go to Step 7 in the Checklist to migrate IP Office standalone or Distributed branch to IP Office Centralized branch on page 16 and follow the remaining steps in that checklist.	

Related links

Upgrading a B5800 Branch Gateway to IP Office on page 49

Replacing B5800 Branch Gateway PLDS licenses with IP Office PLDS licenses

Procedure

1. Send email to http://PRODUCTOPS@avaya.com/ and ask to have your B5800 Branch Gateway licenses converted to IP Office. You will need to provide your **SOLDTO** information. Product Ops will ask you if you use WebLM and a single, shared PLDS license, or nodal license files. If WebLM, you will need to provide the WebLM Host-ID. If individual nodal license files, you will need to provide the Host-ID of each IP Office.
   - Product Ops team will manually convert your B5800 Branch Gateway licenses to IP Office licenses. There is no charge for this conversion. You may update locations incrementally or all at once.
   - If you have Native station licenses, Product Ops will ask if you have 3rd-party SIP phones. These licenses must be purchased separately because IP Office uses a different license model than B5800 Branch Gateway.
   - Product Ops will create the nodal file for each branch.
2. Activate the new IP Office licenses in PLDS and generate the appropriate license file for your deployment, as follows:
   - If you are using centralized licensing with WebLM, generate an IP Office license for the WebLM server.

- If you are using PLDS nodal license files, generate an IP Office nodal license file for each IP Office.

  See the Activating license entitlements section in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

3. Install the new license file(s) as follows:
   - If you are using centralized licensing with WebLM, install the new license file on the WebLM server. See the Installing the shared PLDS license file on the System Manager WebLM server section in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.
   - If you are using PLDS nodal license files, install the new license files on each IP Office. See the Support for individual license files section in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager* and determine the method you want to use to install the licenses.

Related links

Upgrading a B5800 Branch Gateway to IP Office on page 49

Reverting an IP Office system to a B5800 Branch Gateway system

About this task

If an unexpected problem occurs with the system after it has been upgraded, you are able to revert the system back to a B5800 Branch Gateway system. It is not expected that this will be required frequently, but can be done in order to avoid business disruption.

Note the following:

- Reverting an IP Office system to a B5800 Branch Gateway system is possible only for systems that were B5800 Branch Gateway systems before being upgraded IP Office
- The system must have a B5800 Branch Gateway System SD card (not an IP Office system SD card).
- The B5800 Branch Gateway System SD card must be available for use.
- You will need to install the version of Manager available on the B5800 Branch Gateway Administrator Applications DVD. Depending on the B5800 Branch Gateway release you are reverting to, you will need either the R6.1 or R6.2 Administrator Applications DVD.
- This task cannot be performed remotely. You must be physically located at the branch.

Procedure

1. Create a backup of the IP Office system configuration. See Creating a backup of the system configuration using IP Office Manager on page 19.

Note:

Be sure not to override the backup of the B5800 Branch Gateway system configuration you created before you upgraded IP Office.

2. Install Manager from the B5800 Branch Gateway Administrator Applications DVD. See the Installing the administration applications section in *Implementing the Avaya B5800 Branch Gateway for an Avaya Aura Configuration*, document number 18-603853.

   Depending on the B5800 Branch Gateway release you are reverting to, use either the R6.1 or R6.2 Administrator Applications DVD.

3. Shut down the IP Office system and remove the System SD card. See the Shutting down the system using Manager section in *Implementing the Avaya B5800 Branch Gateway for an Avaya Aura Configuration*.
4. Insert the System SD card into a card reader on the IP Office Manager PC.
5. Recreate the System SD card as **Avaya Branch Gateway**. See the Upgrading the card firmware section in *Implementing the Avaya B5800 Branch Gateway for an Avaya Aura Configuration*.
6. While the System SD card is still in the card reader, place the B5800 Branch Gateway system configuration backup file onto the System SD card.

   Note:

   If you do not have a backup of the B5800 Branch Gateway configuration, you will have to reconfigure the system when it comes back as a B5800 Branch Gateway.

   You will also have to administer the IP Office users but can use the existing user records in System Manager and reapply the IP Office user template to the users. For more information, see Reapplying the IP Office user template to existing IP Office users in System Manager on page 54.

7. Remove the System SD card from the card reader and install it in the IP Office system.
8. Replace the IP Office licenses with the B5800 Branch Gateway licenses. Contact Avaya Product Ops to obtain the required licenses as described for the reverse case in Replacing B5800 Branch Gateway PLDS licenses with IP Office 9.0 PLDS licenses on page 51.

   Note:

   If you are not able to obtain the B5800 Branch Gateway licenses promptly, the system will still operate immediately once the downgrade to B5800 Branch Gateway is completed. The B5800 Branch Gateway system will operate in License Error mode without any licenses for up to 30 days.

9. **For B5800 Branch Gateway R6.2 systems only:** Refer to “Chapter 8: Initial branch configuration” in *Implementing the Avaya B5800 Branch Gateway for an Avaya Aura Configuration* and do the following:
   a. Re-create the identity certificate. See “Generating a certificate on System Manager.”
   b. Run the Initial Installation Utility. See “Using the Initial Installation Utility.”

10. **For B5800 Branch Gateway R6.2 systems only:** If the B5800 Branch Gateway was centrally managed from System Manager before it was upgraded to later version of IP Office, to restore centralized management of the system, do the following:
    a. From the System Manager console, in **Services**, click **Inventory.**
    b. In the left navigation pane, click **Manage Elements**.
    c. On the **Manage Elements** page, click the check box for the system you are reverting to a B5800 Branch Gateway.
    d. Click **Edit**.
    e. In the **Device Type** drop-down box, select **B5800**.

       When **B5800** is selected, **6.2** automatically appears in the **Device Version** field.
    f. Click **Commit**.

Related links

Upgrading a B5800 Branch Gateway to IP Office on page 49
Reapplying the IP Office user template to existing IP Office users in System Manager on page 54

Reapplying the IP Office user template to existing IP Office users in System Manager

About this task

If you revert an IP Office system to a B5800 Branch Gateway system and you do not have a B5800 Branch Gateway system configuration backup file, you must reconfigure the system. For more information, see “Chapter 8: Initial branch configuration” in *Implementing the Avaya B5800 Branch Gateway for an Avaya Aura Configuration*. You must also administer the IP Office users on System Manager. You can use the existing user records in System Manager and reapply the IP Office user template to the users as described in this task. Repeat this procedure for each user.

Procedure

1. On the System Manager console, in **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. Click the **IP Office Endpoint Profile** check box to uncheck the box.
8. Click **Commit**.
9. 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. 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.

10. Click **Commit**.

Related links

Reverting an IP Office system to a B5800 Branch Gateway system on page 52

Chapter 5: Upgrading an IP Office with a service pack

Avaya periodically releases service packs to provide updates that fix existing problems or provide enhancements. This chapter describes how to perform an upgrade using Avaya Aura® System Manager. Avaya Aura® System Manager must be used on IP Office systems when multiple branches require upgrades.

Two other methods which require using IP Office Manager that is connected directly to the IP Office system are available to perform an upgrade. You can perform an upgrade using the IP Office Manager upgrade wizard or using the System SD card. For more information, see *Deploying Avaya IP Office™ Platform IP500/IP500 V2*, document number 15-601042.

Service pack installation checklist

#	Description	Section	✔
1	Create a backup of the system configuration.	See Creating a backup of the system configuration using System Manager on page 20.	
2	Synchronize the IP Office with System Manager.	See Synchronizing IP Office with System Manager on page 57.	
3	Set up an external server to act as a remote software library.	See Remote Software Library for upgrades on page 58.	
4	Get the inventory.	See Getting inventory on page 60.	
5	Configure PLDS access.	See Configuring user PLDS access on page 61.	
6	Create a software library.	See Creating a software library on page 62.	
7	Upgrade IP Office.	See Upgrading the IP Office using System Manager on page 23.	

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 57.

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.

Remote Software Library for IP Office upgrades

For the IP Office firmware upgrade files, an external server is required to act as a remote software library. This server hosts the firmware upgrade files through HTTP. The external server should have an FTP, SCP, or SFTP server to upload the firmware files from System Manager. While downloading from the PLDS web site, the firmware files are temporarily copied on System Manager. The FTP, SCP, or SFTP protocols are then used to copy the firmware files from System Manager to the external server. This file transfer from PLDS to System Manager and then to the external server is a single operation for the administrator.

Note:

The HTTPS protocol is not supported for an IP Office device to pull files from the external server.

Downloading the firmware files from PLDS to the IP Office elements through System Manager

1. Download the IP Office firmware from PLDS to the System Manager cache using the credentials provided in **User Settings** in System Manager.
2. Upload the firmware to the external server from the System Manager cache using the FTP or SCP or SFTP protocol and the configuration information in the software library.
3. After the file is on the external server, IP Office elements use this file during upgrade using HTTP protocol.

Note:

Steps 1 and 2 happen simultaneously. The file download to System Manager is transparent.

System requirements for the external server

Component	Requirement	Recommendation
Operating System	Any standalone or virtualized Windows or Linux Distribution.	
Hard Drive	20GB free space	There should be enough free space on the hard drive to store the firmware files.
Memory	2GB	As required by the operating system and the supported protocol services.
Protocols (for the IP Office elements to download files from the external server)	HTTP server	Any supported HTTP server installation. **Note:** The HTTPS protocol is not supported for a IP Office device to pull files from the external server.
Protocols (for downloading the firmware upgrade files to the external server from the PLDS web site via System Manager)	An FTP, SCP or SFTP server (running on default ports)	Use SFTP or SCP for secure file transfer.

Setting up the external server to work as a remote software library for upgrades

Procedure

1. Install the operating system.
2. Install any one of the supported servers: FTP, SFTP, or SCP.
3. Configure users for the FTP, SFTP or SCP access. These users should have read, write, and delete permissions for the directories configured to function as the storage location for the upgrade files.

   Note:

   For IP Office upgrades, Communication Manager 5.2.1, and System Platform based Communication Manager upgrades the software library should also support HTTP. Configure the HTTP server so that the location where the upgrade files are downloaded is accessible using an HTTP URL. After the file is on the external server, the IP Office devices use this file for upgrade using HTTP protocol.

Getting inventory

Before you begin

Ensure that all IP Office devices have been added to System Manager. There are several methods available to add the IP Office to System Manager. All methods require that you identify each individual IP Office. For more information, see the About adding IP Officeto System Manager section in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

The IP Office devices to be discovered for upgrades should be SNMP enabled and the corresponding SNMPv1 communities must be set correctly in System Manager. For more information, see Setting IP Office SNMP attributes on page 60.

About this task

Use this task to collect the components of an IP Office that has been added on System Manager.

Note:

This task does not automatically find the new IP Office. The IP Office must first be added to System Manager. Then this task will collect the components for the IP Office that was added to System Manager.

IP Office that are added to System Manager using the discovery method described in the Discovering IP Office section in *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager* already have their inventory details collected. You do not need to perform this task to upgrade those IP Office.

Procedure

1. On the System Manager console, in **Services**, click **Inventory**.
2. On the **Inventory** page, on the left navigation pane, click **Element Inventory Management > Collect Inventory**.
3. On the **Collect Inventory** page, do the following:
   a. In the Network Subnet(s) section, click the check box for the appropriate network subnet(s).
   b. In the Device Type(s) section, click the check box for **IP Office**.
4. Do one of the following:
   - Click **Now** to get the inventory.
   - Click **Schedule** to get the inventory at a later time.

Setting IP Office SNMP attributes

Procedure

1. On the System Manager console, in **Services**, click **Inventory**.
2. On the **Inventory** page, on the left navigation pane, click **Manage Elements**.

3. Click the check box for the appropriate element.
4. Click **Edit**.
5. On the **Edit <*system name*>** page, click the **SNMP** tab.
6. In the **SNMP** section, do the following:
    a. For the **Version**, click the radio button for **V1**.
    b. In the **Read Community** field, enter the read community of the device.
    c. In the **Write Community** field, enter the write community of the device.
    d. In the **Retries** field, select the appropriate number of times the application should poll the device without receiving a response before timing out.
    e. In the **Timeout (ms)** field, select the appropriate number of milliseconds that the application should poll the device without receiving a response before timing out.
7. Click **Commit**.

Configuring user PLDS access

About this task

Use this procedure to configure user PLDS access and define the default support site.

Procedure

1. On the System Manager console, in **Services**, click **Software Management**.
2. On the **Software Management** page, click **User Settings**.
3. On the **User Settings** page, click **Edit**.
4. For the **Use Avaya Support Site** check box, accept the default setting, checked.

    Note:

    Use **Alternate Source** only if a service technician directs you to use an alternate site for downloads.
5. In the **SSO User Name** field, enter the user's SSO user name for PLDS.
6. In the **SSO Password** field, enter the user's SSO password for PLDS.
7. Click the **Use Proxy** check box if the user has a proxy.
8. In the **Host** field, enter the host details for this proxy server.
9. In the **Port** field, enter the port number for this proxy server.
10. Click **Commit**.

Creating a software library

Procedure

1. On the System Manager console, under **Services**, select **Software Management**.
2. On the Software Management page, click **Software Library**.
3. On the **Software Library** page, click **New**.
4. On the **Add Software Library** page, in the **Library Server Details** tab, do the following:
    a. If this software library is remote, click the **Remote Library** check box.
    b. If this is a Local Survivable Processor (LSP), click the **Local Survivable Processor (LSP)** check box.
    c. In the **Name** field, enter the appropriate name.
    d. In the **IP Address** field, enter the IP address of the library server.
    e. In the **Description** field, enter a description of this library server as appropriate.
    f. In the **Server Path** field, enter the full path of the software library location.
    g. To use this software library as the default, click the **Default Library** check box.
    h. In the **Default Protocol** drop-down box, select the appropriate protocol.
    i. Depending on the default protocol you selected in step g, click on the corresponding tab (**SCP Configuration**, **SFTP Configuration**, **FTP Configuration**, or **HTTP/HTTPS Configuration**) and configure the authentication parameters as required.

        Note:

        Configuring the authentication parameters for the default protocol is mandatory.

    j. Click **Commit**.

Chapter 6: 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.

Glossary

9600 series H.323 phones	This term describes the 9600 series IP Deskphones running H.323 firmware. When running H.323 firmware, these phones are used as IP Office phones in a Distributed enterprise branch deployment. The following 9600 series phones can run H.323 firmware and are supported for use by IP Office users: 9620, 9630, 9640, 9650, 9608, 9611G, 9621G, and 9641G.
9600 series SIP phone	This term describes the 9600 series IP Deskphones running SIP firmware. When running SIP firmware, these phones are used as Centralized phones in a Centralized enterprise branch deployment. The following 9600 series phones can run SIP firmware and are supported for use by Centralized users: 9620, 9630, 9640, 9650, 9601, 9608, 9611G, 9621G, and 9641G.
Branch office	A geographic office location for an enterprise other than the main enterprise location. A branch office is typically smaller and has fewer employees than the main office for an enterprise. A branch office is involved in business activities related to the local market's needs.
Centralized enterprise branch deployment option	This term describes deployments where all users in a branch are Centralized users. See Centralized user.
Centralized management	This term is used to describe a central management system that delivers a set of shared management services and provides a single access interface to administer multiple branch locations and multiple distributed IP Office users.
Centralized phone	This term describes a phone that is used by a Centralized user. See Centralized user.
Centralized trunking	This term describes routing outgoing external calls from the branch sites to the central site in order to utilize the central sites PSTN trunks. The same applies for distributing incoming PSTN calls from the central site to the appropriate branches.
Centralized user	This term describes a user whose call processing is controlled by Avaya Aura® Communication Manager Feature Server or Evolution Server in the enterprise core. During normal operation, the Centralized user gets their telephony features and services from core applications such as the

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

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

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

Note:

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

Distributed enterprise branch deployment option

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

Distributed trunking

This term describes the scenario where each branch retains and uses its own PSTN trunks for incoming and outgoing external calls.

E.164 format

E.164 is a numbering format recommended by the International Telecommunications Union - Telecommunications (ITU-T). E.164 can have a maximum of 15 digits and is preceded by a +.

Extension

This term describes a unique number supported within the dial-plan that is assigned to a user. An extension also has associated endpoint(s) configured, where the endpoint can be either a hard device such as a telephone or a soft client running on a computer, mobile device, or tablet.

Failback

This term is used for the situation where a centralized extension that is working with a survivability call controller detects that its normal call controller is available again. The extension will go through a process of failback to its normal call controller.

Failover

This term is used for the situations where a centralized extension's preferred call controller is no longer available. The extension will go through a process of failover to the first available of its configured

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

Sunny day	This term refers to full network connectivity from the branch to the core data center.
Survivability	This term describes centralized extensions when working after failover. The range of functions available to the phones in this state depend largely on those configured for them on the branch system and will not match those available from the headquarters system during normal operation.
Survivable extension	This term is used to describe an extension which, though physically located at a branch site, receives its' telephony services from the central or headquarters site and operates in a Centralized enterprise branch. A survivable extension is also called a centralized extension.
Tail-End-Hop-Off	Part of mixed mode trunking, this describes scenarios where certain calls at other branches or the headquarters site are routed to the PSTN of another branch.

Index

Numerics

9600 Series phone changes for migration 38

A

about converting users in bulk 36
adding an IP Office Endpoint Profile to existing System Manager users 38
adding a NoUser Source Number to set the SIG parameter to SIP in the auto-generated settings file 42
adding a Session Manager Profile and CM Endpoint Profile to IP Office users 36
application notes 66
Avaya support website 65

B

branch deployment options 11
bulk import of users 29
Bulk import of users 26

C

centralized branch 16
checklist
    migrate 16
    upgrade B5800 Branch Gateway 50
Communication Manager changes required for migration ... 48
configuring user PLDS access 61
Converting
    9608, 9611, 9621, and 9641 phones 39
    SIP 39
Converting 9608, 9611, 9621, and 9641 phones to SIP 43
converting a Centralized user to an IP Office user 35
converting an IP Office user to a Centralized user 32
Converting some or all 9600 phones to SIP 45
creating
    system configuration backup 19
creating a backup
    system configuration 20
    using System Manager 20
Creating a software library 62

D

deleting license files from the branches 30
DevConnect 66
distributed branch 16
document changes history 7
document conventions 7

E

editing the xml file containing the users 27
enabling secure communication after upgrading IP Offfice Manager 26
exporting users to an xml file 27
external server; system requirements 59

G

Getting inventory 60

I

InSite Knowledge Base 66
installing a service pack 56
IP Office configuration changes for migration 47
IP Office configuration changes syncing with System Manager 57
IP Office upgrades; remote software library 58

L

Licensing changes required for migration 47

M

migrating
    IP Office Centralized branch 14
    IP Office standalone 14
migrating individual PLDS license files to a WebLM server . 30
Migration
    Centralized users 31
    IP Office users 31

O

overview
    enterprise branch 9
    IP Office 9

R

reapplying the IP Office user template to existing IP Office users in System Manager 54
related documentation 63
remote software library 58
remote software library; setting up external server 59
remote software library for upgrades 58
removing
    scheduled backup jobs 19

replacing B5800 Branch Gateway PLDS licenses with IP Office PLDS licenses 51
resource websites 65
reverting an IP Office 9.0 system back to a B5800 Branch Gateway system 52

S

service pack installation checklist 56
Session Manager configuration changes for migration 48
Setting IP Office SNMP attributes 60
setting up the external server as remote software library 59
standalone 16
support 65
supported telephones 13
Synchronizing IP Office with System Manager 57
system requirements for the external server 59

T

topology 10
training 63
turning off
    automatic backup feature 18

U

upgrade
    IP Office 21
    options 21
upgrading
    B5800 Branch Gateway 49
    IP Office 23
    System Manager 23
upgrading the administration applications 25
User management changes for migration 31
using
    upgrade wizard 21

V

videos 64