Administering an IP Office Enterprise Branch

Issue 2
December 2021

© 2014-2021, Avaya Inc.
All Rights Reserved.

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).

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: IP Office Element Manager

IP Office Element Manager

You can configure and manage IP Office, Unified Communications Module (UCM) and Application Server devices from System Manager. You can backup, restore and download the IP Office device configurations.

In System Manager, use inventory management through SNMPv1, to discover IP Office devices. The discovered IP Office devices appear in **Manage Inventory** > **Discovery** in **Inventory**.

With System Manager, you can support the following IP Office configurations:

- IP Office application

  ✱ **Note:**

  You can use this interface to view or edit the configuration values.

- UCM and Application Server

However, client computers need JRE for System Manager to support the IP Office application. See JRE requirement for client computers on page 9.

Use the administrative capabilities of IP Office in System Manager to:

- Edit and view system configuration data in **System Configuration**.
- Edit and view security configuration data in **Security Configuration**.
- Perform the backup and restore tasks of IP Office, UCM and Application Server device configuration that includes system configuration data and user data.
- Synchronize the IP Office, UCM and Application Server devices through the **Inventory** tab.

✱ **Note:**

When you use System Manager to gain access to an IP Office device, System Manager locks the device you have selected. You cannot go to that IP Office device externally. To unlock the device, edit the security settings in System Manager. Edit the security settings only in critical scenarios.

To create and apply system configuration and endpoint templates for IP Office devices, use **IP Office Endpoint** and **IP Office System Configuration** pages. Use the **IP Office Endpoint** and **IP Office System Configuration** menus in template management to:

- Create, edit, view, duplicate, and delete the Endpoint Templates for IP Office, UCM and Application Server devices.
- Create, edit, view, duplicate, and delete the System Configuration Templates for IP Office, UCM and Application Server devices.

- Upload and convert audio files from a .WAV to a .C11 format.
- Apply IP Office System Configuration templates to IP Office, UCM and Application Server devices.

Related links

JRE requirement for client computers on page 9

JRE requirement for client computers

When launching IP Office Manager, client computers need Java Runtime Environment (JRE). JRE is required to open IP Office Manager through the Java Applet.

As an System Manager administrator, you must install JRE 1.7+ on your client machine to manage IP Office users, system configuration, and security configuration.

If JRE 1.7+ is not installed, the system displays the following message:

```
Failed to launch IP Office Manager.
```

`IP Office Manager requires Java Runtime Environment to launch, System has detected that there is no Java Runtime Environment present or version present is below recommended Java Runtime Environment version 1.7+. Download and install latest Java Runtime Environment version for Windows operating system from the Oracle site` http://www.oracle.com/technetwork/java/javase/downloads/index.html.

You can download the latest version of JRE from http://www.oracle.com/technetwork/java/javase/downloads/index.html.

Note:

- Upgrade JRE to JRE 1.7.0_51+ and upgrade JDK plugin in the browser to JDK 7.0.510+. Because JRE 1.7 introduced security settings changes, you must clear the browser cache and temporary internet files of Java from Java Control Panel. To delete the cache of applications and applets, when you delete the temporary internet files from Java Control Panel, click **Installed Applications and Applets**.
- The Java version on the client computer must correspond to the supported browser type. For example, a 32-bit browser requires a 32-bit Java version, and a 64-bit requires a 64-bit Java version.

Related links

IP Office Element Manager on page 8

Unlocking an IP Office device

Procedure

1. On the IP Office Manager interface, in **Security Settings** pane, click **Security** > **Services**.

2. In the **Services** pane, click **Configuration**.
3. In the **Service: Configuration** pane, in the Service Details section, do the following:
    a. In **Name**, type a name for the service.
    b. In **Host System**, type a name for the host system.
    c. In **Service Port**, type a value for the service port.
    d. In **Service Security Level**, select the service security level.
    e. In **Service Access Source**, click **Unrestricted**.
4. Save and exit IP Office Manager.

    This procedure unlocks the IP Office device for external access. However, remains unlocked until the device receives a request through System Manager.

Next steps

You can lock the IP Office device:

- Using System Manager.
- When you perform any operation on the device through System Manager.

Starting the IP Office Element Manager

The IP Office application is a prerequisite for successful completion of administrative tasks on the **Security Configuration** and **System Configuration** pages in **IP Office**, **IP Office Endpoint** and **IP Office System Configuration** pages in **Templates**, and the **IP Office Endpoint Profile** section in **User Management**.

When you newly install System Manager , set up System Manager to start the IP Office application, and to upgrade the IP Office application to the latest version available in PLDS.

Setting up System Manager to start IP Office element manager

About this task

If you have already downloaded the `AdminLite-XXX.exe` file by using Solution Deployment Manager in System Manager, do not perform the procedure.

Procedure

1. Download the IP Office element manager `AdminLite-XXX.exe` file from http://plds.avaya.com.

XXX in `AdminLite-XXX.exe` specifies the version string. For example, `B5800AdminLite-6.2(38).exe`.

Using IP Office element manager, (AdminLite-XXX.exe), you can manage IP Office and B5800 devices.

2. Transfer the downloaded `AdminLite-XXX.exe` or `B5800AdminLite-XXX.exe` file to the System Manager server using SFTP or SCP to the `$ABG_HOME/tools` directory.
3. Change this file into an executable file using the command: `chmod +x <file name>`.
4. To create a soft link by using the name `ManagerSFX.exe` for the uploaded file, perform the following:
    a. To navigate to the `tools` folder, type `cd $ABG_HOME/tools`.
    b. To create the link, type `ln -sf target linkname`.

       For example, if the file that you uploaded to the `$ABG_HOME/tools` location is `B5800ManagerLite.exe`, then run the **`ln -sf B5800ManagerLite.exe ManagerSFX.exe`** command.
5. Update the `abg_b5800_mgr_version` parameter with the IP Office element manager version that you downloaded from PLDS in the `$ABG_HOME/tools/ManagerSFXVersion.properties` file.
6. If you have an IP Office administration suite already installed on your computer using the IP Office Administration Applications DVD, update the *abg_b5800_mgr_version* parameter with the manager version of your computer in the `$ABG_HOME/tools/ManagerSFXVersion.properties` file on System Manager.

   Important:

   You must update the `abg_b5800_mgr_version` parameter when you download a new version of IP Office element manager from PLDS, and transfer to System Manager. If you fail to update, an attempt to start the IP Office element manager through System Manager fails, and the system displays an error message to update the parameter.
7. To set the environment variable to match the version of the `AdminLite-XXX.exe` file, on the administration computer that is used to start IP Office, refer to the “Setting up the environment variable in Windows 7 to match the version of AdminLite” section in Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager.

Default login password for day one configuration of an IP Office device

For day one configuration for an IP Office device in **Manage Elements** in System Manager, use the default service login and password to gain access to an IP Office device through System Manager. On the Attributes tab of the New IP Office page, the following are the default values:

- **Service Login**: SMGRB5800Admin
- **Service Password**: SMGRB5800Admin

Note:

For IP Office 9.1 and later, the default values set in **Service Login** and **Service Password** are BranchAdmin.

To navigate to the New IP Office page in **Manage Elements** from the web console, click **Inventory** > **Manage Elements** > **New**.

You can use the service password only once. After you commit the service login and password, the system changes this default password internally and generates a random password. The system does not display the new password. To reset the login password, connect to the IP Office device locally by using IP Office Manager.

Important:

After you change the password, the system schedules a default Sync system configuration and a system configuration backup job everyday.

IP Office system configuration

System Configuration

Use the **System Configuration** pages to view and edit system configuration of IP Office, IP Office Application Server, and UCM devices through System Manager. However, client computers need JRE for System Manager to support the IP Office application. See JRE requirement for client computers on page 9.

To view or edit system configuration values, start the IP Office element manager in the offline mode through System Manager. System Manager uses web services to obtain the latest system configuration and passes the configuration to the IP Office element manager. After you save the IP Office element manager configuration, System Manager retrieves the modified system configuration file and pushes the file to the IP Office configuration.

Downloading the IP Office system configuration

About this task

Use the procedure to copy the configuration of an IP Office device to the local machine.

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **IP Office** > **System Configuration**.
3. On the IP Office System Configuration page, select the device whose security configuration you want to download.
4. Click **Download**.
5. Do one of the following:
   - For Firefox, click **Save File** and click **OK**.

     The system saves the saves the configuration file with the device name to the default location.
   - For Internet Explorer, provide the file name and location, and click **Save**.

     The system saves the configuration file to the default location.

IP Office security configuration

Security Configuration

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

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

Viewing a security configuration

About this task

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

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

Procedure

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

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

Related links

IP Office security configuration field descriptions on page 15

Editing a security configuration

About this task

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

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

Procedure

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

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

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

Related links

IP Office security configuration field descriptions on page 15

IP Office security configuration field descriptions

Device list

Name	Description
Device Name	The name of the IP Office device.
IP Address	The IP address associated with the IP Office device.

Table continues…

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

Buttons

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

Backup and restore of the IP Office devices

IP Office device configuration backup

Use the **Backup** feature on the **IP Office Backup** page 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.

Use the **IP Office Backup** page to create a local backup in the local storage attached to the IP Office device. The IP Office device stores only one copy of the backup file in the local storage. If you are backing up on a remote server, you can create five backup files for every device.

You can perform the backup task immediately or at a scheduled time. Use the **Scheduler** service in System Manager to set the time. You can view the logs of the backup task on the Log Harvesting pages in System Manager.

IP Office device configuration restoration

Use the **Restore** feature on the **IP Office Restore** page to restore the IP Office device configuration. The IP Office device configuration contains the system configuration data and the user data. You can perform the restore operation from a local storage or a remote server.

You can perform the restore task immediately or at a scheduled time. Use the **Scheduler** service in System Manager to set the time. You can view the logs of the restore tasks on the Log Harvesting pages in System Manager.

Configuring the http or https protocol for a remote server

About this task

Use this procedure to configure the remote server for using the HTTP or HTTPS protocol.

Procedure

1. On the remote server, install and activate the HTTPS and PHP packages.
2. On the System Manager server, do the following:
    a. Navigate to the `$ABG_HOME/httpfiles/` location.
    b. Copy the files with the `.php` extension to the backup location on the remote server.
3. On the remote server, grant full access permissions to the files that you copied in Step 2.
4. Start a browser and test the accessibility of the remote server in the network.

Creating a backup of the IP Office device configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation page, click **Backup**.
3. On the IP Office Backup page, select the IP Office device from the Device List for which you want to create a backup.
4. In the **Backup Options** field, click **Backup On Device** or **Backup On Remote Server**.
5. Click **Backup**.

    The system displays the IP Office device that you selected in the **Device List**.
6. Do one of the following:

Choice Option	Sub Steps
Backup On device	a. Click **Now** to perform the backup task immediately. b. Click **Schedule** to perform the backup task at a specified time.
Backup On Remote Server	a. In the **Select Remote Server** field, select a remote server where you want to save the backup. Alternatively, click **Add Server** to add a remote server. b. In the **Backup Label** field, type a name for the backup. c. Click **Now** or **Schedule**.

7. To view the status of the backup task for the selected device, click **Status**.

Related links

IP Office Backup field descriptions on page 19
IP Office Restore field descriptions on page 21

Restoring the IP Office device configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **Restore**.
3. On the IP Office Restore page, select the IP Office device or devices from the Device List whose backed up configuration you want to restore.
4. In the **Restore Options** field, click **Restore Backup Stored On Devices** or **Restore Backup Stored On Remote Server**.
5. Click **Restore**.
6. In the **Restore Options** field, do one of the following:

Choice Option	Choice Description
For Restore Backup Stored on Device(s), select one of the following :	• System Configuration • User • System Configuration and User • Restore Backup Stored on Devices
For Restore Backup Stored on Remote Server, do the following:	a. In the **Select Remote Server** field, select a remote server. Alternatively, click **Add Server** to add a remote server. b. Click **Get Restore Point**. c. Select **Restore Point** from the list.

7. Click **Now** to perform the restore activity immediately.
8. **(Optional)** Click **Schedule** to perform the restore activity at a specified time.

Result

You can view the status of the restore job in the **Scheduler** service.

Related links

IP Office Backup field descriptions on page 19
IP Office Restore field descriptions on page 21

IP Office Backup field descriptions

Backup Options

Name	Description
Backup Options	The options are: • Backup On Device • Backup On Remote Server **Note:** The Backup On Remote Server option is available for IP Office Manager Release 9.1 and later.

Backup On Device field descriptions

Name	Description
Device Name	The name of the IP Office device.
IP Address	The IP address associated with the IP Office device.
System Type	The type of system associated with the IP Office device. The options are: • **IP Office**: For the IP Office core unit • **B5800 device**: For the B5800 device
Last Operation on Device	The name of the last operation performed on the IP Office device.
Status	The status of the operation.
System Configuration Template	The current IP Office System Configuration template that exists on the IP Office device.
Last Modified Time of System Configuration	The last time that the system configuration was modified.
Last Backup Time	The last time that a backup was taken.

Button descriptions

Name	Description
Backup	Displays the IP Office Backup page.
Status	Displays the status of the last operation.
Stop	Stops the operation.

Backup On Device button descriptions

Button	Description
Now	Performs the backup operation, as applicable, immediately.
Schedule	Displays the IP Office Job Scheduler page to schedule a backup.
Cancel	Cancels the backup job and returns to the IP Office Backup page.

Backup On Remote Server field descriptions

Name	Description
Select Remote Server	The Remote Server location to store the backup. The options are: • **Select**: To select a remote server. • **Add Server**: To add a remote server.
Add Server	The configuration for a remote server: • **Backup Label**: The name of the backup • **New Server Name**: The name of the new server • **New Server IP**: The IP address of the new server • **Port**: The port number of the new server • **Backup Path**: The backup path of the new server • **Selected Protocol**: The protocol of the new server • **User Name**: The name of the user • **Password**: The password of the user
Selected Protocol	The protocol of the new server. The options are: • **http** • **https**

Backup On Remote Server button descriptions

Button	Description
Save	Saves the remote server and backup configuration.
Edit	Modifies the remote server and backup configuration.
Delete	Deletes the remote server and backup configuration.

IP Office Restore field descriptions

Restore Options

Name	Description
Restore Options	The options are: • Restore Backup Stored on Devices • Restore Backup Stored on Remote Server

Restore field descriptions

Name	Description
Device Name	The name of the IP Office device.
IP Address	The IP address associated with the IP Office device.
Last Operation on Device	The name of the last operation performed on the IP Office device.
Status	The status of the operation.
System Configuration Template	The current IP Office System Configuration template that exists on the IP Office device.
Last Modified Time of System Configuration	The date and time of the last system configuration operation.
Last Backup Time	The date when you last performed the Backup operation on the device.

Restore Backup Stored On Devices field descriptions

Name	Description
System Type	The type of system associated with the IP Office device. The option: • **IP Office and B5800 device**

Table continues…

Name	Description
Restore Backup Stored On Devices	The options are: • **System Configuration**: For restoring the system configuration • **User**: For restoring the user • **System Configuration and User**: For restoring the system configuration and the user • **Restore Backup Stored on Devices**: For restoring the backup stored on the devices

Button descriptions

Name	Description
Restore	Opens the IP Office Restore page.
Status	Displays the status of the operation that is currently running or was last run.
Stop	Stops the operation that is currently running.

Restore Backup Stored on Remote Server field descriptions

Name	Description
System Type	The type of system associated with the IP Office device. The option is: • **IP Office**: only for IP Office Manager version 9.1
Remote Server	The Remote Server location where the last backup was stored. Do one of the following: • **Select**: Select a remote server. • **Add Server**: Add a remote server.
Add Server	The configuration for a remote server: • **New Server Name**: The name of the new server • **New Server IP**: The IP address of the new server • **Port**: The port number of the new server • **Backup Path**: The backup path of the new server • **Selected Protocol**: The protocol of the new server • **User Name**: The name of the user • **Password**: The password of the user

Table continues…

Name	Description
Selected Protocol	The protocol of the new server. The options are: • **http** • **https**
Restore Point(s)	The restore point from where you want to restore the last backup

Restore Backup Stored on Remote Server Button descriptions

Name	Description
Get Restore Point	Creates a Restore Point from where you can restore the last backup.
Save	Saves the new remote server configuration.
Edit	Edits the new remote server configuration.
Delete	Deletes the new remote server configuration.

UCM or IP Office Application Server

UCM and Application Server device configuration backup

Use the **Backup** feature on the UCM and Application Server Backup to back up the UCM and Application Server device configuration. The UCM and Application Server device configuration contains the following data:

- Voice mail— related configuration
- Messages
- Recordings
- One-X portal— related configuration

Use the UCM and Application Server Backup page to create a remote backup, where the system stores the backup in the selected remote server location. The UCM and Application Server device can store five copies of the backup file in the remote storage.

You can perform the backup task immediately or at a scheduled time. Use the **Scheduler** service in System Manager to set the time. You can view the logs of the backup tasks on the Log Harvesting pages in System Manager.

Note:

For additional steps, see *Deploying Avaya Aura® System Manager*.

UCM and Application Server device configuration restoration

Use the Restore feature on the UCM and Application Server Restore page to restore the UCM and Application Server device configuration. The UCM and Application Server device configuration contains the following data:

- Voice mail-related configuration
- Messages
- Recordings
- One-X portal-related configuration

Use the UCM and Application Server Restore page to restore the data from a remote server. The UCM and Application Server device stores five copies of the backup file in the remote storage.

You can perform the restore task immediately or at a scheduled time. Use the **Scheduler** service in System Manager to set the time. You can view the logs of the restore tasks on the Log Harvesting pages in System Manager.

Note:

For additional steps, see *Deploying Avaya Aura® System Manager*.

Creating a backup of the UCM and Application Server device configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **UCM and Application Server** > **Backup**.
3. On the UCM and Application Server Backup page, in Device List, click the UCM and Application Server device for which you want to create a backup.
4. Click **Backup**.

   The system displays the UCM and Application Server device that you selected in **Device List**.
5. Select a remote server from the **Remote Server** field. Alternatively, click **Add Server** to add a remote server.
6. Configure the settings for **Backup Configuration** using the following parameters:
   - In the **Select Voicemail Pro Sets** field, choose voice mail pro sets.
   - In the **Select One-x Portal Sets** field, choose one-x portal sets.
   - In the **Select Contact Recorder Sets** field, choose contact recorder sets.
   - In the **Backup Label** field, type the backup file name.

7. Do one of the following:
    - Click **Now** to perform the backup task immediately.
    - Click **Schedule** to perform the backup task at a specified time.
8. To view the status of the backup task for the selected device, click **Status**.

Restoring the UCM and Application Server device configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation page, click **UCM and Application Server** > **Restore**.
3. On the UCM and Application Server Backup page, select the UCM and Application Server device whose backed— up configuration you want to restore.
4. Click **Restore**.

    The system displays the UCM and Application Server device that you selected in **Device List**.
5. Do the following:
    a. In the **Remote Server** field, click a Remote Server . Alternatively, click **Add Server** to add a remote server.

        The system activates the **Get Restore Point** button.

    b. Click **Get Restore Point**.

        The system displays the **Restore Points** list with the restore point that you added:

Field name	Field description
Restore Point	Displays the name of the restore point.
IP Address	Displays the IP address associated with the restore point.
Version	Displays the version of the restore point.
Set	Displays the set of the restore point.
Time Stamp	Displays the time stamp associated with the restore point.

6. Do one of the following:
    - Click **Now** to perform the restore task immediately.
    - Click **Schedule** to perform the restore task at a specified time.

        To view the status of the restoration task for the selected device, click **Status**.

UCM and Application Server Backup field descriptions

Remote Server

Name	Description
Select Remote Server	The Remote server location to store the backup.

Backup On Remote Server

Name	Description
Select Remote Server	The Remote Server location to store the backup. The options are: • **Select**: To select a remote server. • **Add Server**: To add a remote server.
Add Server	The configuration parameters for adding a remote server. The parameters are: • **Backup Label**: The name of the backup • **New Server Name**: The name of the new server • **New Server IP**: The IP address of the new server • **Port**: The port number of the new server • **Backup Path**: The backup path of the new server • **Selected Protocol**: The protocol of the new server • **User Name**: The name of the user • **Password**: The password of the user
Selected Protocol	The protocol P of the new server. The options are: • **http** • **https** • **scp** • **sftp** • **ftp**

Backup Configuration

Name	Description
Select voice mail Pro Sets	The voice mail pro sets.
Select one-X Portal Sets	The one-X Portal sets.
Select Contact Recorder Sets	The contact recorder sets.
Backup Label	The name of the backup file.

Buttons

Button	Description
Backup	Opens the UCM and Application Server Backup page.
Status	Displays the status of the last operation.
Save	Saves the remote server and backup configuration.
Edit	Modifies the remote server and backup configuration.
Delete	Deletes the remote server and backup configuration.
Now	Performs the backup job, as applicable, immediately.
Schedule	Schedules the backup at a later time and opens the UCM and Application Server Backup page.
Cancel	Cancels the backup job and opens the UCM and Application Server Backup page.
Stop	Stops the backup job.

UCM and Application Server Restore field descriptions

Remote Server

Name	Description
Select Remote Server	The list of available remote servers
New Server Name	The name of the new server
New Server IP	The IP address of the new server
Port	The port address
Backup Path	The path of the latest backup
Selected Protocol	The protocol for the new server
User Name	The user name for the new server
Password	The password for the new server

Button	Description
Restore	Opens the **UCM and Application Server Restore** page. Use this page to restore the backed up system configuration and the messages, the recording and the one-X configuration to a UCM and Application Server device.
Status	Displays the status of the operation that is currently running or was last run.
Save	Saves the remote server and backup configuration.
Now	Performs the restore operation immediately.

Table continues…

Button	Description
Schedule	Displays the **IP Office Job Scheduler** page. Use this page to schedule a Restore operation.
Cancel	Cancels the restore job, as applicable, and directs you to the **Restore** landing page.
Get Restore Point	Creates a restore point on the selected remote server.

Restore Backup stored on Remote Server

Name	Description
Remote Server	The Remote Server location where the last backup was stored. Do one of the following: • **Select**: Select a remote server. • **Add Server**: Add a remote server.
Add Server	The configuration for a remote server • **New Server Name**: Name of the new server • **New Server IP**: IP address of the new server • **Port**: Port number of the new server • **Backup Path**: Backup path of the new server • **Selected Protocol**: Protocol of the new server • **User Name**: Name of the user • **Password**: Password of the user
Selected Protocol	Protocol of the new server. Select a protocol from the following: • **http**: for the http protocol • **https**: for the https protocol • **scp**: for the scp protocol • **sftp**: for the sftp protocol • **ftp**: for the ftp protocol
Restore Point(s)	The restore point from where you want to restore the last backup

UCM or Application Server file transfer

Transferring custom prompt files to a UCM or Application Server device

Procedure

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

2. In the left navigation pane, click **UCM and Application Server** > **File Transfer**.
3. In **Select File Type**, click **Custom Prompts**.
4. In **Select Files to Upload**, click the audio file that you want to upload.

   List Audio Files displays the list of audio files that you have uploaded by using **Manage Custom Prompts** in the UCM or Application Server system configuration templates.

   In the **Enter Destination Folder Location to Push Files** field, the system displays the default location where you want to transfer the file.
5. In **Devices List**, select the IP Office Application Server or UCM device where you want to upload the audio file.
6. Click **Commit**.
7. On the File Transfer page, perform one of the following:
   - Click **Now** to upload the audio file to the IP Office Application Server or UCM device.
   - Click **Schedule** to upload the audio file at the scheduled time.

   Note:

   After you schedule a file transfer do not delete the file till the transfer is complete. The file transfer operation fails if you delete the file you want to transfer.

   Using the file transfer capability you cannot upload PLDS license files. See Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager to view details on uploading a PLDS license file to the IP Office device, if applicable.

   For uploading files to System Manager, see Uploading files to the System Manager repository on page 42. To delete a file, see Deleting an uploaded file on page 43.
8. To check the status of the file transfer, click **Services** > **Scheduler**.

Voice Mail Pro Call Flow and System Configuration

Viewing the Voice Mail Pro call flow

Procedure

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

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

5. To exit Voicemail Pro Client , click **File** > **Exit**.

   The system displays the VMPro Call Flow page.

Editing the Voice Mail Pro call flow

Procedure

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

   The system starts the Voicemail Pro Client application in Offline and Editable mode.
6. Do one of the following:
   - To exit Voicemail Pro Client without saving, click **File** > **Exit**.
   - To return to the Voicemail Pro Client page after saving, click **File** > **Save and Make Live**.

   The system displays the VMPro Call Flow page.

Downloading the Voice Mail Pro call flow

Procedure

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

     The system saves the configuration file with the device name to the default location.
   - For Internet Explorer, provide the file name and location, and click **Save**.

     The system saves the configuration file to the default location.

Viewing the status of a Voice Mail Pro call flow

Procedure

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

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

Saving Voice Mail Pro call flow as a template

Procedure

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

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

VMPro Call Flow field descriptions

Device List

Name	Description
Device Name	The name of the IP Office device.

Table continues…

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

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

Viewing the Voice Mail Pro system configuration

Procedure

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

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

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

Next steps

For Voice Mail Pro system preferences, see Administering IP Office Voicemail Pro.

Editing the Voice Mail Pro system configuration

Procedure

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

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

Next steps

For Voice Mail Pro system preferences, see Administering IP Office Voicemail Pro.

Saving Voice Mail Pro system configuration as a template

Procedure

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

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

VMPro system configuration field descriptions

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

UCM or IP Office Application Server security configuration

Viewing UCM and Application Server security configuration

Procedure

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

   The system starts the UCM and Application Server Manager application.
5. In the right pane of the UCM and Application Server Manager window, you can view the details of the selected UCM and Application Server Security Configuration. All the fields are read-only.
6. Click **File** > **Exit** to exit the UCM and Application Server Manager application and return to the UCM and Application Server Security Configuration landing page.

Editing UCM and Application Server security configuration

Procedure

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

4. Click **Edit**.

   The system starts the UCM and Application Server Manager application.

5. The system starts the UCM and Application Server Manager window, edit the required fields on the right pane.

6. Click **File** > **Save Security Settings and Exit** to save the modifications and exit the UCM and Application Server Manager application.

   The system directs you to the IP Office Security Configuration landing page.

   After you save the configuration, System Manager retrieves the edited security configuration file from the UCM and Application Server Manager application and pushes the file to the UCM and Application Server device.

UCM and Application Server security configuration field descriptions

Device list

Name	Description
Device Name	The name of the UCM and Application Server device.
IP Address	The IP address of the UCM and Application Server device.
System Type	The type of system associated with the UCM and Application Server device.
Last Operation on Device	The last operation that you performed on the device.
Status	The status of the operation that is currently running or was last run.
System Configuration Template	The current system configuration template that exists on the UCM and Application Server device.
Last Modified Time of System Configuration	The date and time of the last system configuration operation.
Last Backup Time	The date and time when you last performed the backup activity on the UCM and Application Server device.

Buttons

Name	Description
View	Click to view the UCM and Application Server security configuration field descriptions.

Table continues…

Name	Description
Edit	Click to edit the UCM and Application Server security configuration field descriptions.

UCM or IP Office Application Server system configuration

Viewing a UCM and Application Server system configuration

Procedure

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

   In the right pane of the UCM and Application Server window, you can view the details of the selected UCM and Application Server system configuration.

   > **Note:**
   >
   > All the fields are view only.

   The system starts the UCM and Application Server Manager application.
5. Click **File** > **Exit** to exit the UCM and Application Server Manager application.

   The UCM and Application Server System Configuration landing page opens.

Editing a UCM and Application Server system configuration

Procedure

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

   The system starts the UCM and Application Server Manager application.
5. On the UCM and Application Server Manager window, edit the required fields on the right pane.

6. Click **File** > **Save Configuration and Exit** to save the modifications and exit the UCM and Application Server Manager application.

   On the UCM and Application Server System Configuration Edit page, the system displays selected UCM and Application Server device in the device list. Perform one of the following:

   - Click **Commit** to apply the changes immediately.
   - Click **Schedule** to apply the changes at a specified time.

UCM and Application Server system configuration field descriptions

Name	Description
Device Name	The name of the UCM and Application Server device.
IP Address	The IP address associated with the UCM and Application Server device.
System Type	The type of system associated with the UCM and Application Server device.
Last Operation on Device	The operation that has been performed last on the device.
Status	The status of the operation that is currently running or was last run.
System Configuration Template	The current UCM and Application Server System Configuration template that exists on the UCM and Application Server device.
Last Modified Time of System Configuration	The date and time you last modified the system configuration.
Last Backup Time	The date and time when you last performed a backup.

Button

Name	Description
View	Click to view the UCM and Application Server system configuration field descriptions.
Edit	Click to edit the UCM and Application Server system configuration field descriptions.
Download	Click to download the UCM and Application Server system configuration field descriptions.

Chapter 2: IP Office configuration

Add IP Office field descriptions

General

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

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

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

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

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

SNMP

Name	Description
Version	The SNMP protocol type. The options are None and V1.

Table continues…

Name	Description
Read Community	The read community of the device.
Write Community	The write community of the device.
Retries	The number of times that an application polls a device without receiving a response before timing out.
Timeout (ms)	The number of milliseconds that an application polls a device without receiving a response before timing out.

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

IP Office configuration

IP Office elements are GR-unaware. During failover, split network, or failback, perform the procedures from this section to ensure data integrity and proper administration of IP Office from System Manager. As the System Manager certificates contain an entry of the secondary System Manager in the **SAN** field, the same trust continues to work between the secondary System Manager and the IP Office element.

Important:

- The System Manager lock is maintained on the IP Office device to ensure that changes are not provisioned on the device outside System Manager. You can only make configuration changes on IP Office after removing the System Manager lock. For more information, see Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager.
- If IP Office has been added to any System Manager previously, then before reusing it, you must erase the IP Office security settings using the **File** > **Advanced** > **Erase Security Settings** page on the IP Office Manager window.

IP Office configuration when the primary System Manager is nonfunctional

If the primary System Manager server is nonfunctional, the secondary System Manager server can administer and manage the IP Office device without any additional steps on the secondary System Manager.

IP Office configuration in the Active-Active scenario

If the primary System Manager server is nonfunctional, the secondary System Manager server can administer and manage the IP Office device without any additional steps on the secondary System Manager.

If the IP Office element can communicate with both System Manager servers, you can administer IP Office from both System Manager servers. The data from the two servers conflict. During recovery, you must select the database of only one System Manager, and the changes in the other database are lost.

Manage the IP Office elements from only one System Manager even in the Active-Active scenario so that you can select this database for recovery when the communication between the two System Manager servers is reestablished. For more information about managing IP Office from System Manager, see Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager.

Note:

For configuring the trap destination, SCEP details, and WebLM server in a single step, run the Initial Installation Utility of Native B5800 Manager.

You can also use the installation utility to change the configuration on IP Office for the System Manager failover scenarios. As the System Manager certificates contain an entry of the secondary System Manager in the **SAN** field, the same trust continues to work between the secondary System Manager and IP Office.

Chapter 3: IP Office file transfer

Transferring audio files to an IP Office device

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. Click **File Transfer**.
3. In **Select File Type**, click **Audio**.
4. In **Select Files to Upload**, click the audio file that you want to upload.

   List Audio Files displays the list of audio files that you have uploaded using Manage Audio in IP Office System Configuration Templates.

   In the **IP Office Destination Folder Location** field, the system displays the default location where you want to transfer the file.
5. In **Devices List**, select the IP Office device where you want to upload the audio file.
6. Click **Commit**.
7. On the IP Office File Transfer page, perform one of the following actions:
   - Click **Now** to upload the audio file to the IP Office device.
   - Click **Schedule** to upload the audio file at the scheduled time.

   Note:

   Using the file transfer capability you cannot upload PLDS license files. See Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager to view details on uploading a PLDS license file to the IP Office device, if applicable.

   After you schedule a file transfer do not delete the file till the transfer is complete. The file transfer operation fails if you delete the file you want to transfer.
8. To check the status of the file transfer, click **Services** > **Scheduler**.

Transferring files to an IP Office device

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. Click **File Transfer**.
3. In **Select File Type**, click **Other**.
4. In **Select Files to Upload**, select the file you want to upload.
5. In the **IP Office Destination Folder Location** field, enter the location of the IP Office device where you want to transfer the file.
6. From **Select IP Office(s)**, select the IP Office device where you want to upload the file.
7. Click **Commit**.
8. On the IP Office File Transfer page, perform one of the following actions:
    - Click **Now** to upload the greeting file to the IP Office device.
    - Click **Schedule** to upload the greeting file at the scheduled time.

    Note:

    After you schedule a file transfer do not delete the file till the transfer is complete. The file transfer operation fails if you delete the file you want to transfer.

    Using the file transfer capability you cannot upload PLDS license files. See Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager to view details on uploading a PLDS license file to the IP Office device, if applicable.
9. To check the status of the file transfer, click **Services** > **Scheduler**.

Uploading files to the System Manager repository

About this task

If you select **Other** as the file type, you can upload files up to 300MB in the System Manager repository.

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. Click **IP Office** > **File Transfer**.
3. In **Select Files to Upload**, select the file that you want to upload to System Manager.
4. Browse to the file in your local computer, and select the file you want to upload.
5. Click **Save**.

The system displays the uploaded file in the List Uploaded Files table. You cannot upload a file greater than 30MB.

Note:

The current versions of Firefox, Google Chrome, Safari, Opera and Android support file size validation, but Internet Explorer 9.0 does not support file size validation. Internet Explorer 10.0 is likely to support file size validation.

Deleting an uploaded file

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. Click **IP Office** > **File Transfer**.
3. In **Select File Type**, click **Other**.
4. In **List Uploaded Files**, select the files that you want to delete.
5. Click **Delete**.

IP Office file transfer field descriptions

Select File Type

Name	Description
File Type	Select the type of file you want to upload to the IP Office device. The values are: • Audio: Uploads the audio files to the IP Office device. • Other: Transfers other files such as phone settings, firmware files, and other IP Office files.

Select Files to Upload (Audio Files)

Name	Description
wav Audio File Name	The file name of the `.wav` type of audio file.
Last uploaded time of wav	The time when you last uploaded the `.wav` audio file in the system.
Recording Label	The recording label of the `.wav` file.
c11 Audio File Name	The file name of the `.C11` type of audio file.

Table continues…

Name	Description
Last converted time of wav to c11	The time when you last converted a `.wav` file to a `.C11` audio file.

Select Files to Upload (Other files)

Name	Description
File Name	The name of the file that you want to upload to the IP Office device.

Enter IP Office Destination Folder Location to Push Files

Name	Description
IP Office Destination Folder Location	The IP Office location of the auto attendant file. The default value for audio is `SYSTEM\DYNAMIC\LVMAIL\AAG\`. For other files, provide the location of the IP Office device. The default location for other files is `SYSTEM\PRIMARY\`.

Select IP Office(s)

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

Button	Description
Commit	Uploads the audio file or other file to the IP Office device.

Chapter 4: Manual failback

Failback policy

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

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

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

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

Initiating failback

Before you begin

You must configure the failback settings in the IP Office manager.

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. Click **Initiate Failback**.
3. On the IP Office Manual Failback page, select the devices for which you want to initiate manual failback.

   System Manager lists only those devices that have manual failback settings.
4. Perform one of the following actions:
   - Click **Now** to initiate manual failback.
   - Click **Schedule** to initiate manual failback at the scheduled time.

IP Office failback field descriptions

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

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

Chapter 5: Templates

Managing IP Office Endpoint template

Adding an IP Office endpoint template

Procedure

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

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

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

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

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

Related links

IP Office endpoint template field descriptions on page 50

Viewing an IP Office endpoint template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **IP Office Endpoint**.

3. Select a type of system from the list of IP Office supported templates.
4. Click **Show List**.
5. Under **IP Office Endpoint Templates**, select the template you want to view from the list of templates.
6. Click **View**.

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

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

Related links

IP Office endpoint template field descriptions on page 50

Editing an IP Office endpoint template

Procedure

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

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

   The system displays the IP Office Endpoint landing page.

Related links

IP Office endpoint template field descriptions on page 50

Duplicating an IP Office endpoint template

Procedure

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

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

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

Related links

IP Office endpoint template field descriptions on page 50

Deleting an IP Office endpoint template

Procedure

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

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

Upgrading IP Office endpoint templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **IP Office Endpoint**.
3. Select the IP Office device type.
4. Click **Show List**.
5. Select the template you want to upgrade.

6. Click **Upgrade**.
7. In the **Supported IP Office Versions** field, enter the target version for upgrade.
8. In **Template Name**, type the name of the template.

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

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

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

IP Office endpoint template field descriptions

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

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

Managing IP Office System Configuration template

Adding an IP Office System Configuration template

Procedure

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

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

   The system directs you to the IP Office System Configuration landing page where you can view the newly created system template in the IP Office System Configuration list.

Viewing an IP Office System Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **IP Office System Configuration**.
3. On the IP Office Branch Gateway Template page, from the IP Office supported templates list, select an IP Office system type.
4. Click **Show List**.
5. Select the system configuration template you want to view from the IP Office System Configuration list.
6. Click **View**.

   The system launches the IP Office Manager application.
7. On the IP Office Manager window, in the right pane, you can view the system configuration template details. All the fields are read-only.
8. Click **File** > **Exit** to exit IP Office Manager.

The system directs you to the IP Office System Configuration landing page.

Editing an IP Office system configuration template

Procedure

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

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

   The system displays the IP Office System Configuration landing page.

Deleting an IP Office system configuration template

Procedure

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

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

Applying an IP Office system configuration template on an IP Office device

Procedure

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

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

   Important:

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

IP Office System Configuration template field descriptions

Name	Description
Name	The name of the IP Office System Configuration template.
System Type	The type of system associated with the template. The options are: • **IP Office**: for IP Office core unit • **B5800**: for B5800 core unit
Version	The version number of the template.
Last Modified Time	The date and time when the IP Office System Configuration template was last modified.

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

Manage audio files

Audio files in .WAV and .C11 formats are used in auto attendant configuration in the Auto Attendant feature in IP Office. In System Manager, you can manage .WAV and .C11 audio files from the Manage Audio page in IP Office System Configuration in Template Management. The .C11 audio file is for use in IP Office IP500V2 or the B5800 Core Unit.

To push an auto attendant file to an IP Office System Configuration template through System Manager, you must first upload the .WAV audio files using the **Upload** button in the Manage Audio page. When you upload the .WAV audio files, the corresponding .C11 audio files are automatically created. If you need to convert any .WAV audio file which does not have a corresponding .C11 audio file, or if the corresponding .C11 audio file is deleted, click the **Convert** button in the Manage Audio page.

Use the **Manage Audio** page in **IP Office System Configuration** to:

- Upload .WAV and .C11 audio files.
- Convert .WAV to .C11 audio file format.
- Delete .WAV and .C11 audio files.

Uploading an audio file

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **IP Office System Configuration**.
3. Click **More Options** > **Manage Audio**.
4. On the Manage Audio page, enter the complete path of the audio file in the **Select an Audio File** text box. You can also click **Browse** to locate and select the audio file you want to upload.

   The system displays the audio file you selected for uploading in a table.

   Note:

   System Manager filters uploaded files based on mime type or bytes in the file. If a file type does not match, System Manager shows up an error message.
5. If you want to remove the audio file from your selection, click the **Remove** link in the **Action** column.
6. Click **Upload**.

You can view the newly uploaded audio files listed in the **List of Audio Files** table.

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

Procedure

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

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

Deleting an audio file

About this task

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

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **IP Office System Configuration**.
3. Click **More Options** > **Manage Audio**.
4. On the Manage Audio page, select the audio file you want to delete from the list of audio files.
5. Click **Delete**.
6. On the Delete Audio File Confirmation page, you can view the audio files you selected in Step 4 for deletion. From the **Select the type of deletion** field perform one of the following:
   - Select the type of audio file extension you want to delete.
   - Select **Both** if you want to delete both the file extension types.

Sample scenario: Suppose you have ABC.wav and ABC.c11 audio files in the **List of Audio Files**. If you want to delete only the ABC.wav audio file, then select **Wave** from **Select the type of deletion**. If you want to delete both the audio files in a single step, then select **Both** from the **Select the type of deletion** field.

7. Click **Delete**.
8. Click **Done** to return to the IP Office System Configuration landing page.

Manage Audio field descriptions

Name	Description
wav Audio File Name	The file name of the .WAV type of audio file.
Last uploaded time of wav	The time when you last uploaded the .WAV audio file in the system.
Recording Label	The recording label of the .wav file.
C11 Audio File Name	The file name of the .C11 type of audio file.
Last converted time of wav to C11	The time when you last converted a .wav file to a .C11 audio file.
Select an Audio File	Displays the complete path of the audio file.
Select the type of deletion on the Delete Audio File Confirmation page	Provides the option to select the type of deletion of audio files. The valid options are: • **Wave**: Select to delete only the .WAV type of file for the selected audio file. • **C11**: Select to delete only the .C11 type of file for the selected audio file. • **Both**: Select to delete both, .WAV and .C11, types of files for the selected audio file.

Button	Description
Delete	Click to delete the selected audio file.
Convert	Click to convert an audio file of type .WAV to .C11.
Done	Click to exits the **Manage Audio** page and return to the IP Office Template List page.
Browse	Click to locate and select an audio file.
Upload	Click to upload an audio file to System Manager.
Delete on the Delete Audio File Confirmation page	Click to confirm the delete action for the selected audio file.
Cancel on the Delete Audio File Confirmation page	Click to cancel the delete operation and return to the **Manage Audio** page.

Managing UCM and Application Server system configuration templates

Adding a UCM and Application Server Configuration template

Procedure

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

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

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

Related links

UCM and Application Server Templates field descriptions on page 60

Viewing a UCM and Application Server Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **UCM and Application Server Configuration**.
3. On the UCM and Application Server Templates page, in the **Supported System Types** section, select one of the following system types:
   - IP Office Application Server
   - Unified Communications Module
4. Click **Show List**.

5. Select the system configuration template you want to view from the **UCM and Application Server Templates** list.
6. Click **View**.

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

   The system starts the IP Office Manager application.
7. Click **File** > **Exit** to exit IP Office Manager.

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

Related links

UCM and Application Server Templates field descriptions on page 60

Editing a UCM and Application Server Configuration template

Procedure

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

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

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

Related links

UCM and Application Server Templates field descriptions on page 60

Deleting a UCM and Application Server Configuration template

Procedure

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

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

Related links

UCM and Application Server Templates field descriptions on page 60

Applying a UCM and Application Server Configuration template

Procedure

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

   You will be directed to a new page where you can select a device to apply the template.

7. From the list of IP Office devices, select the IP Office device on which you want to apply the selected UCM and Application Server Configuration template.

   ❗ **Important:**

   When you apply a template on a device, the data of the template that you wish to apply may override the existing system configuration data on the device.

8. Do one of the following:
   - Click **Now** to perform apply the template immediately.
   - Click **Schedule** to apply the template at a specified time in **Scheduler**.
   - Click **Cancel** to cancel this task and return to the UCM and Application Server Templates landing page.

Related links

UCM and Application Server Templates field descriptions on page 60

UCM and Application Server Templates field descriptions

Name	Description
Name	The name of the system configuration template of UCM and Application Server.
System Type	The type of system associated with the template. The options are: • **Unified Communications Module**: For UCM core unit • **Application Server**: For Application Server core unit
Version	The version number of the template.
Last Modified Time	The date and time when the UCM and Application Server System Configuration template was last modified.

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

Managing VMPro system configuration templates

Adding a VMPro System Configuration template

Procedure

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

2. In the left navigation pane, click **VMPro System Configuration Template**.
3. Click **New**.
4. Complete the **Name** and **Version** fields.
5. Click **Details**.

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

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

Related links

VMPro System Configuration Templates field descriptions on page 64

Viewing a VMPro System Configuration template

Procedure

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

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

Related links

VMPro System Configuration Templates field descriptions on page 64

Editing a VMPro System Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro System Configuration Template**.

3. On the VMPro System Configuration Templates page, select a VoicemailPro system type.
4. Click **Show List**.
5. Select the system configuration template you want to edit from the VMPro System Configuration list.
6. Click **Edit**.

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

   The system displays the VMPro System Configuration Template page.

Related links

VMPro System Configuration Templates field descriptions on page 64

Deleting a VMPro System Configuration template

Procedure

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

   The system displays the system template instance you selected for deletion.
7. Do one of the following:
   - Click **Delete** to delete the template.
   - Click **Cancel** to cancel the delete operation, and return to the VMPro System Configuration Template landing page.

Related links

VMPro System Configuration Templates field descriptions on page 64

Applying a VMPro System Configuration template on a device

Procedure

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

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

   ❗ **Important:**

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

Related links

VMPro System Configuration Templates field descriptions on page 64

Duplicating a VMPro System Configuration template

Procedure

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

6. Click **Duplicate**.

   The system launches the VMPro application.

7. In the **New Template Name** field, type the name of the new template.
8. Click **Commit**.

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

Related links

VMPro System Configuration Templates field descriptions on page 64

VMPro System Configuration Templates field descriptions

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

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

Managing VMPro call flow templates

Adding a VMPro Call Flow template

Procedure

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

   The system launches the **VMPro** application.

6. In the right pane, complete the call flow template by filling the required fields, and click **Update**.

7. Click **Save and Exit** to save the template specifications and exit the **VMPro** application.

Result

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

Related links

VMPro Call Flow Templates field descriptions on page 68

Viewing a VMPro Call Flow template

Procedure

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

Result

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

Related links

VMPro Call Flow Templates field descriptions on page 68

Editing a VMPro Call Flow template

Procedure

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

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

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

Result

The system displays the VMPro Call Flow Templates page.

Related links

VMPro Call Flow Templates field descriptions on page 68

Deleting a VMPro Call Flow template

Procedure

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

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

Related links

VMPro Call Flow Templates field descriptions on page 68

Applying a VMPro Call Flow template on a device

Procedure

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

The system displays the VMPro Call Flow page where you can select a device to apply the template.

7. From the list of VMPro devices, select the VMPro device on which you want to apply the VMPro call flow template.

   Important:

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

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

Related links

VMPro Call Flow Templates field descriptions on page 68

Duplicating a VMPro Call Flow template

Procedure

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

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

Result

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

Related links

VMPro Call Flow Templates field descriptions on page 68

VMPro Call Flow Templates field descriptions

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

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

Chapter 6: Upgrading IP Office

Overview of managing software

Use Manage Software from **Services** > **Solution Deployment Manager** to:

- Analyze the current software and get recommendations on the available version for the device
- Download the compatible software and upgrade the devices
- Collect the inventory and the components of a device in System Manager using **Get inventory**
- Upgrade IP Office, Unified Communications Module (UCM) and Application Server devices
- Install software patches for IP Office, Unified Communications Module (UCM) and Application Server devices

Get inventory

Before you begin

Enable SNMP so that the devices are discovered for upgrades. Set the corresponding SNMPv1 communities for the devices in System Manager through **Inventory** > **Manage Elements**.

Important:

Configure SNMP parameters on the device before you configure the same device in System Manager. You must use the same SNMP credentials for the device in System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the navigation pane, click **Manage Software**.
5. On the Manage Software page, Click **IP Office** > **Get Inventory** to obtain the inventory for the IP Office devices.

6. Perform one of the following actions:
    - Click **Now** to collect the inventory or the components of the device.
    - Click **Schedule** to get the inventory at a later time.

Analyzing the software

Before you begin

Get the inventory

Configure user settings

Ensure that the inventory is populated.

About this task

Using the analyze feature, you can identify if a new software is available for the inventory, and if you have permissions to download the software.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Manage Software**.
3. On the Manage Software page, click **IP Office** > **Analyze** > **Now** to analyze if any new IP Office software is available.

    Click **Analyze** > **Schedule** to perform the operation at a later time.

Downloading the software

About this task

You can download the software releases that you are entitled from Avaya PLDS, or from an alternate source to System Manager.

Before you begin

Refresh the elements in the inventory.

Analyze the software.

Create a software library.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Manage Software**.

3. On the Manage Software page, click **IP Office**, select a device, and click **Download**.

   The system displays the File Download Manager page where the required download files are listed.

4. To change the display settings, click one of the following:

   - **Tree View**: To view the list of elements in the tree format. The system displays each element with the list of components associated with the element that you selected.
   - **List View**: To view the list of elements in the list format. Every element is displayed individually.

5. In **Select Software/Hardware Types**, select the software or firmware that you want to download.

6. Click **Show Files**.

7. In **Select Files Download Details**, do the following:

   a. In **Source**, click the source from which you want to download the files.

      The options are Avaya PLDS/Alternate Source and My Computer.

   b. Select the files that you want to download.

   c. Click **Download**.

Result

In **File Download Status**, the system displays the file that you selected for download.

Upgrading an IP Office device

Before you begin

- Obtain the inventory.
- Analyze the software.
- Download the software.

For preupgrade tasks that you must complete, see Solution deployment and upgrade.

About this task

Use the procedure to upgrade IP Office, UCM, and Application Server devices and their components.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Manage Software**.
3. On the Manage Software page, perform one of the following:
   - To update **IP Office**, click **IP Office**.

- To upgrade UCM or Application Server, click **IP Office** > **UCM or IP Office Application Server**.

4. Select the device that you want to upgrade, and click **Upgrade**.

   Note:

   The **Upgrade** button is available only if the analyze operation is complete.

5. On the Download Manager page, in the **Release** column, select a version.

   You can configure a specific version other than the recommended version by selecting an option of your choice from the field.

6. In the **Library** field, select the software library.

   Important:

   The system lists only those software libraries with the HTTP protocol.

7. Click one of the following:

   - **Now**: To upgrade the device immediately.
   - **Schedule**: To upgrade the device at a specified time.

   Status on the IP Office page displays the status of the upgrade. Click the status of the IP Office device to view the logs and the description of the upgrade operation.

   Note:

   When you upgrade B5800 Branch Gateway to IP Office, the **Status** in the Operation Status table displays **Processing**. After the upgrade is successful, the system continues to display **Processing** in the **Status** column.

   On the IP Office page, in the second table, the system displays the **Status** as IDLE for the device that you upgraded. The **Current Version** displays the new version of the IP Office device. This information indicates that the upgrade was successful.

   You cannot downgrade an IP Office device by using Solution Deployment Manager. Use the IP Office Manager to downgrade an IP Office. For more information on downgrading an IP Office device, see the IP Office documentation.

Index