IP Office
Deploying IP Office Server Edition

Release 11.0
Issue 12
March 2020

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. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

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

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

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number

indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use 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. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software 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. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: 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 G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

The deployment guide is provided primarily for the those engaged in implementing a configuration for customers. This include new installations and enhancements to existing solutions. These people are

- Implementation engineers—who work with beta and key customers to install the hardware and the software and configure the individual components.
- Field technicians—who install the hardware and the software and configure the individual components at the customer's site.
- Solution program Managers—who work with the customer, third-party vendors, and the implementation team to deploy the reference architecture.

In addition, those who design the solution would find the information valuable.

As the user of this book, you are expected to have a clear understanding of the

- Technology being deployed in this reference architecture
- Skills necessary to install and configure the various Avaya products
- General process for implementing multiple Avaya products

The book is not intended to provide all of the information about the technology; that information must come from other sources, including internal resource material and training. If you do not have sufficient knowledge or skills to deploy this reference architecture, get them before proceeding any further.

Contents

Chapter 1: Introduction

Purpose

This document provides deployment procedures for installing and configuring a solution based on a verified reference configuration. It includes installation, configuration, initial administration, troubleshooting, and basic maintenance checklists and procedures.

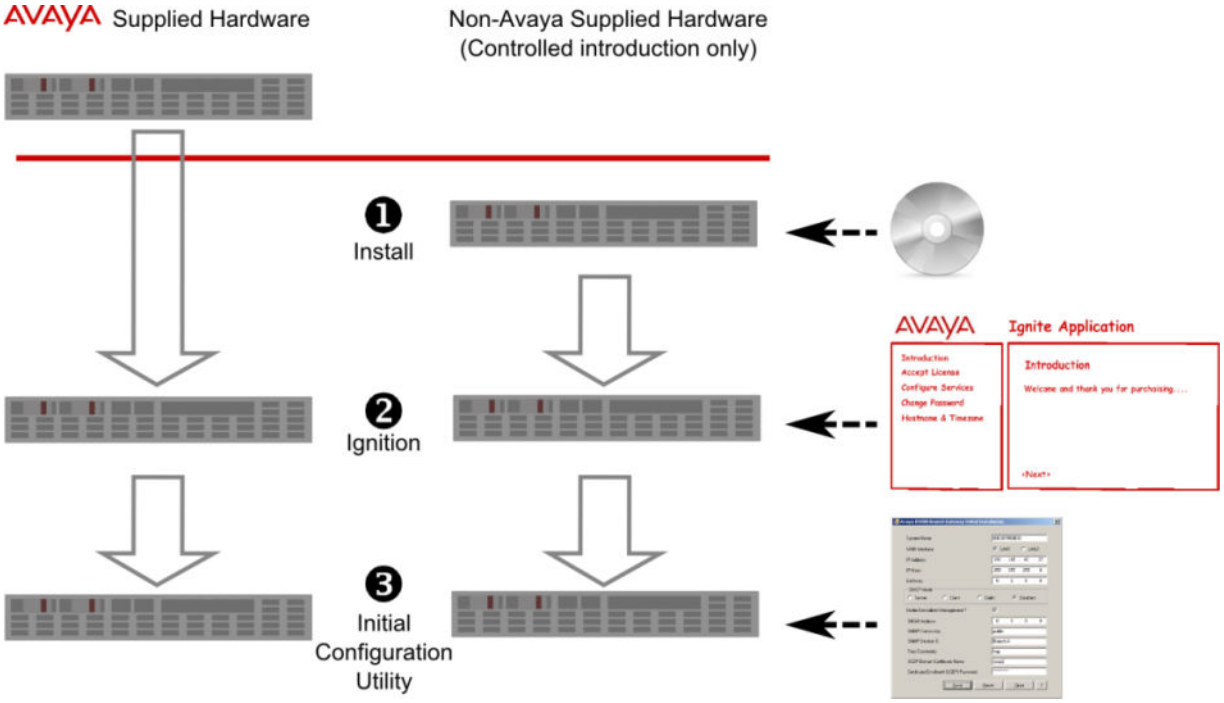
This document is intended to be used by anyone who is responsible for deploying a solution at a customer site. The checklists and procedures are based on a verified reference configuration. This document does not include optional or customized aspects of a configuration.

Document changes since last issue

- A new section about configuring IP Office systems using the Dashboard has been added. See Configuring IP Office using the Dashboard on page 18.
- Information about Avaya WebLM Release 7.1 support in IP Office Release 11.0 has been added to the Upgrade Licenses section in Server Edition Upgrade Policy on page 47 topic.
- The Upgrade Licenses section in the Server Edition Upgrade Policy on page 47 topic has been updated to inform that when IP Office Server Edition is upgraded from R10.0 to R11.0, the password is reset to default.
- The topic - Backing up an IP Office Server Edition server has been updated to remove Contact Recorder backup procedure.
- A cautionary note for backing up Contact Recorder database before starting upgrade to IP Office Release 11 has been added to the topic Upgrade Process Summary.
- References to IP Office Integrated Contact Reporter has been removed.
- References to Contact Recorder.have been removed.
- The chapter on Capacity Planning has been removed from this guide. However, all Capacity Planning related content will continue to be available in the *Capacity Planning* document.

Chapter 2: Deploying an IP Office Server Edition Solution

About this task



Note:

You can install the software for an IP Office Server Edition Solution only on the servers that Avaya supports. Avaya does not provide support for Server Edition software that you install on any other servers. For more information, about the servers that Avaya supports, see *IP Office Server Edition Reference Configuration*.

Note:

If you are deploying an IP Office Select solution, you must specify the deployment as Select in the Initial Configuration Utility. For information on Select operation, see

- *Avaya IP Office™ Platform Server Edition Reference Configuration*
- *Avaya IP Office™ Platform Solution Description*

You can install IP Office Server Edition Solution on a virtual server. For information, see *Deploying Avaya IP Office™ Platform Servers as Virtual Machines*.

To deploy an IP Office Server Edition Solutionthe key steps that you need to perform are:

Procedure

1. If you have not purchased a pre-installed server from Avaya, then install Server Edition on a supported server.
2. Configure the role of the server using the ignition process.
3. Configure the server using the Initial Configuration Utility.
4. Add the optional components such as a Server Edition Secondary server and a Server Edition Expansion System.
5. Upgrade to the latest IP Office Server Edition software release if a new version is available.
6. Add the licenses for a Server Edition Secondary and Server Edition Expansion System.
7. Administer the various components using IP Office Web Manager and IP Office Manager.

Chapter 3: Installing an IP Office Platform Server Edition server

Server Edition Primary server

The primary server is the only hardware component that you need to deploy an IP Office Server Edition Solution. In a multi-node deployment, the Primary Server manages all the components of an IP Office Server Edition Solution.

Installation and Upgrade With a USB Drive

You can install and upgrade IP Office Server Edition using a USB drive. Before creating the USB drive you must download the required software from the Avaya support site.

Related links

[Downloading the Software for USB Drive Creation](#) on page 12
[Creating a USB Drive](#) on page 13

Downloading the Software for USB Drive Creation

Creating a USB drive for installation or upgrade requires the following software from the Avaya support site:

- IP Office Server Edition ISO image
- Avaya USB Creator Tool

  This software tool is downloadable from the same page as the ISO files. After installation, you can use the tool to load an ISO image onto a USB memory key from which the server can boot and either install or upgrade.

Before you begin

You must be able to log in to the Avaya support site.

Procedure

1. In a web browser, navigate to the Avaya support site at http://support.avaya.com and log in.
2. On the menu bar, click **Support by Product** and select **Downloads**.
3. Enter IP Office Platform in the **Enter Product Name** box and select the matching option from the displayed list.
4. Use the **Choose Release** drop-down to select the required IP Office release.
5. The page lists the different sets of downloadable software for that release. Select the software for IP Office Server Edition.

   The page displayed in a new tab or windows details the software available and provides links for downloading the files.
6. Download the IP Office Server Edition ISO image and the Avaya USB Creator Tool.

   Also download the documents listed under the **RELATED DOCUMENTS** heading, if shown.

Related links

Installation and Upgrade With a USB Drive on page 12

Creating a USB Drive

Before you begin

- You need a USB drive with 8 GB storage space.
- Install the Avaya USB Creator Tool.

Procedure

1. Insert the USB drive into a USB port on the PC.
2. Start the Avaya USB Creator. From the Windows Start menu, select **All Programs** > **Avaya USB Creator** > **Avaya USB Creator** .
3. In the Avaya USB Creator, click **Browse** and select the IP Office Server Edition ISO file.
4. In the **Select Target USB Drive** field, select the USB memory key. Ensure that you select the correct USB device as this process overwrites all existing content on the device.
5. In the **Select USB Label** field, enter a name to identify the key.
6. In the **Select Installation Mode** field, select the if the USB drive will be configured for installation or upgrade.

   Note that selecting the **Attend Mode** disables automatic installation.
7. Under **Select Locals to Install / Upgrade**, select the check boxes for the Voicemail Pro prompts to install or upgrade.

   Selecting only the languages that you require significantly reduces install or upgrade time.

8. Click **Start** and then confirm.

Related links

Installation and Upgrade With a USB Drive on page 12

Starting Web Manager

You can use the Web Manager application to manage IP Office Server Edition Solution.

Web Manager is supported on the following browsers.

- Internet Explorer 9 and higher
- Firefox 16 and higher
- Chrome
- Safari 7 and higher

Do not use a mobile version of the browser to access Web Manager.

Before you begin

You must have the IP address of IP Office Server Editionserver.

Procedure

1. On a client computer, start the browser and type `https:<ip address of IP Office Server Edition>`.

   The system displays a list of links.

2. Click **IP Office Web Manager** link.

Result

The system opens the Web Manager application.

Installing IP Office Server Edition server manually

You can install or upgrade IP Office Server Edition manually using the install DVD or a USB drive.

If you have purchased a pre-installed Server Edition Server, perform this procedure to ensure you have the latest version of the software installed.

Before you begin

- You need Server Edition installation DVD or an Server Edition installation USB drive.
- Ensure that you take a backup of all user data on the server. In this installation process, the system purges everything that is already on the server including the operating system and all user data.

Procedure

1. Perform one of the following.
   - Insert the installation DVD in the DVD drive of Server Edition Primary server.
   - Insert the installation USB drive in the USB port of Server Edition Primary server.
2. Restart the Primary server.

   Note:

   To restart a Server Edition server, always use Web Manager. For more information, see Restarting a Server using Web Manager on page 87. For a new installation, power cycle the server.

   The system restarts and boots from the installation DVD or the installation USB drive.

   Note:

   If the system does not restart or boot from the installation DVD or the installation USB drive, then verify the boot order in BIOS settings.
3. Click **Change Language** to select the language for use during the installation or upgrade process.
4. Click **Next**.
5. Select the type of keyboard you would like to use for the system.
6. Click **Next**.
7. Select the language in which you would like to read the End User License Agreement (EULA).
8. Click **OK**.
9. Click **Yes, I have read, understood and accepted the terms of Avaya EULA**.
10. Click **Next**.

    The system prompts you to install or upgrade. If you are installing Server Edition on a server in which Server Edition is already installed, then the system displays the details of the applications that are already installed. The system also displays the details of the applications that the system will install.
11. Select **Install** if you want the system to replace the applications that are already installed.
12. Click **Next**.
13. Do one of the following:
    - Select **Yes** if you want to continue with the installation.
    - Select **Advanced** if you want to configure addition settings such as hardware partitioning.
14. Click **Next**.
15. Type the name of the IP Office Server Edition server in the **Hostname** field.

The system identifies IP Office Server Edition by the name that you type in the **Hostname** field. The server advertises this name in the network. Ensure that the **Hostname** is unique within the network domain. The **Hostname** can be a string of characters that is 63 characters in length. The characters can be upper-case or lower-case letters A through Z, digits 0 through 9, the minus sign (-), and the period (.).

16. Click **Configure Network**.

    The system displays the network interfaces that are connected to the IP Office Server Edition in the **Network Connections** window.

    Note:

    You cannot configure the VPN network interfaces using the **VPN** tab in IP Office Server Edition.

17. Select the network connection that the system has identified.
18. Do one of the following:.
    - To edit the configuration of the network connection, click **Edit**. You can assign the IP address for the network connection using the DHCP.
    - To delete the network connection, click **Delete**.

    The default configuration settings for the network connection for *System eth0* are as follows:

    - Connection name: System eth0
    - IP address: 192.168.42.1
    - Netmask: 255.255.255.0
    - Gateway: 0.0.0.0

    The default configuration settings for the network connection for *System eth1* are as follows:

    - Connection name: System eth1
    - IP address: 192.168.43.1
    - Netmask: 255.255.255.0
    - Gateway: 0.0.0.0
19. Click **Close** to close the **Network Connections** window.
20. Click **Next**.
21. Type the password for the root user in the **Root Password** field.
22. Retype the password in the **Confirm** field.

    The system displays a warning message if the strength of the password is weak.
23. Click **Next**.

    The system displays the location of the installation log file and kick start installation file.

24. Click **Next**.

    The system displays the progress of the applications that are installed.

25. Click **Next**.

    The system displays an option to install TTS language packs

26. Do one of the following:

    a. To install TTS language packs, insert the TTS installation DVD, click **Continue**.

    b. To skip installation of TTS language packs, click **Decline**.

27. Click **Next**.

    The system displays the progress of the installation. The installation process can take up to 30 minutes.

28. Remove the installation DVD or USB drive from the DVD or USB drive and click **Reboot**. Log in to the sever using a web browser on another computer in the network.

Installing IP Office Server Edition automatically

You can install Server Edition automatically using the installation USB drive. The system automatically configures the default parameters during the installation. For more information, see Default parameters. on page 18

Note:

In this installation process, the system purges everything that is already there on the server including the operating system and user data.

Before you begin

You need the following:

- IP Office Server Edition installation USB drive. For more information, see Installation and Upgrade with a USB Drive on page 12.

Procedure

1. Insert the installation USB drive in the USB port of the Server Edition server.
2. Restart the Server Edition server.

   Note:

   To restart Server Edition server, always use Web Manager. For more information, see Restarting a Server using Web Manager on page 87. For a new installation, turn off the power supply to the server.

   The system restarts and boots from Server Edition installation USB.

Note:

If the system does not restart or boot from the installation USB drive, then verify the boot order in BIOS settings.

Default parameters

When you install using the installation USB for automatic installation, the system configures the default parameters for various settings.

The default parameters that the system configures during an automatic installation are as follows:

Language for installation	US English
Keyboard for the system	US English
Hostname	MAC_HOSTNAME: : 00:AE:EF:00:00:00
System eth0	• Connection name: System eth0 • IP address: 192.168.42.1 • Netmask: 255.255.255.0 • Gateway: 0.0.0.0
System eth1	• Connection name: System eth1 • IP address: 192.168.43.1 • Netmask: 255.255.255.0 • Gateway: 0.0.0.0
Root Password	Administrator

Configuring IP Office Server Edition using the Dashboard

About this task

If you have installed and ignited a single-node IP Office system, a Configuration Dashboard is presented to you when you log in to the **Web Manager** interface for the first time. You can use the Dashboard to configure your IP Office system. The Dashboard comprises of widgets that contain minimum required set of configuration fields to set up the system. Clicking each widget takes you to the relevant configuration page. In the first login, you are presented with a single widget - **System** for configuring the system details. You can click on the widget to navigate to the System configuration page. Once you configure the System, the rest of the widgets become available for configuration. You can complete the rest of the configuration in your subsequent logins if you have

completed at least the System configuration. The following widgets are available for configuration using the Configuration Dashboard:

- **System**
- **VOIP**
- **Voicemail**
- **Licenses**
- **Users**
- **Group Settings**
- **Lines**
- **Incoming Call Routes**
- **Outgoing Call Routes**

For detailed description of the fields, see the *Administering Avaya IP Office™ Platform with Web Manager* guide.

Before you begin

Ensure that your Server Edition Primary system has been installed and ignited.

Procedure

1. Log on to **Web Manager**.
2. On a Server Edition system, select **Solution** > **Server Menu** > **Dashboard**.

   The Dashboard page appears.
3. Click the **System** widget.
4. Type appropriate information in the fields.

   For information on the fields, see the field descriptions for each of the pages.
5. Click **Apply** to save the page.

   The System page can be updated in **Offline Mode** only. You must **Save to IP Office** to enable the configuration.
6. Click **Back** to go back to the Dashboard.
7. Follow steps 3 to 5 for each widget you want to configure.

Configuring IP Office Server Edition using the ignition process

The system displays the Ignition menu the first time that you log in to Web Manager of the Linux based IP Office Server Edition server. You can set and confirm various key settings such as the role of the server. For example, you can set the role of the server as Primary, Secondary, Expansion, or Application Server.

Note:

You can run the Ignition process only once and you cannot rerun the Ignition process unless you reinstall the server completely.

If the Ignition process is not completed. For example, if you click the **Cancel** button. The system displays the Ignition menu when you login the next time.

Note:

The default configuration settings for an Avaya server on which Server Edition is already installed is as follows:

- DHCP Mode: Off
- IP address (eth0/LAN1): 192.168.42.1
- IP address (eth1/LAN2): 192.168.43.1
- Netmask: 255.255.255.0
- Gateway: 0.0.0.0
- Hostname: The eth0 MAC address of the server
- DNS1: Blank
- DNS2: Blank
- Root Password: Administrator

The default configuration settings for the server on which you install Server Edition manually are the values that you set during the installation process.

About this task

To start the ignition process:

Procedure

1. On a client computer, start the browser and type *https://<IP address of IP Office Server Edition> : 7070*

   The system displays the SID of the Server Edition server only when you have not completed the Ignition process. You can also select the language in which you want to proceed with the Ignition process.

2. Log in as *root*.

   The system displays the **Accept License** page.

3. In the **Accept License** page, read all of the Avaya Global Software Licensing Terms, if these are acceptable, select **I Agree**.

4. Click **Next**.

   The system displays the **Server Type** page.

5. In the **Server Type** page, select the role of the server.

Note:

You cannot reset the type of server that you select after the ignition process is complete.

6. Click **Next**.

   The system displays information for additional hardware. The page is populated when an additional hard disk is added to be used when running Media Manager on the server.

   Accept the default settings. Note that the **Name** is needed later by the Media Manager application. It is used to configure where to store the call recordings it collects from the Voicemail Pro server.

7. Click **Next**.

   The system displays the default network configurations. Ensure that the network configuration details match that of the server for which a role is assigned. Otherwise, update the network configuration details.

   The system identifies IP Office Server Edition by the name that you type in the **Hostname** field. The server advertises this name in the network. Ensure that the **Hostname** is unique within the network domain. The **Hostname** can be a string of characters that is 63 characters in length. The characters can be upper-case or lower-case letters A through Z, digits 0 through 9, the minus sign (-), and the period (.).

8. In the **Configure Network** page, click **Next**.
9. In the **Time & Companding** page:
   a. Select **Use NTP**.

      Note:

      The system displays the **Use NTP** option in the Time & Companding page only when you assign the role of a server as **Application Server** or **Primary** server. Ensure that you select **Use NTP** for the primary server.

   b. Select the type of **Companding**.

      Note:

      The system does not display the **Companding** option in the Time & Companding page when you assign the role of a server as **Application Server**.

      Typically µ-law is for North America and Japan, A-law for Europe and other parts of the world. If you are not sure about the option that you need to select, consult your service provider.

   c. Click **Next**.
10. In the **Change Password** page, you must change the **root and security** account password, the **Administrator** account password, and the **System** account password to ensure that the system is secure.

Note:

The following account passwords are synchronized.

- Setting the IP Office security account password also sets the same password for the Linux root user account.
- Setting the IP Office Administrator account password also sets the same password for the Linux Administrator user account.

- To change the existing passwords:

a. Type a password in the **New Password** field.

b. Retype a password in the **New Password (verify)** field.

Ensure that the password you type conforms to the requirements that are specified under **Password complexity requirements**.

Note:

You can also change the password and the password complexity requirements anytime after the Ignition process using Linux Platform settings.

c. Click **Next**.

On Secondary and Expansion systems, the system displays the details of the Server Edition server.

11. In the **Security** page, you can automatically generate a signing certificate for the internal Certificate Authority or import a third party signing certificate. For more information on Certificate Authority operation, see *Avaya IP Office™ Platform Security Guidelines*.

Note:

The system does not display the **Certificate Authority** option when you assign the role of a server as Secondary Server or Expansion System.

- To automatically generate a certificate, select **Generate CA automatically** and then click **Next**.
- To import a certificate, perform the following.

a. Select **Import CA**.

b. Click **Browse**, navigate to the certificate location and select the file.

c. Click **Upload**.

d. In the **Password** field, enter the password for the certificate.

12. Click **Next**.

You receive a prompt that you must import the certificate into the browser. Click **OK**.

On a Primary or Application server, the system displays the details of the Server Edition server.

13. In the **Certified Authority** field, there two links for downloading the certificate. Click on both links and download the files to the PC.

Note:

The system does not display the **Certificate Authority** option when you assign the role of a server as Secondary Server or Expansion System.

14. You can review the settings that you selected during the ignition process. To print the details of the Server Edition server, click **Print**.

    Avaya recommends that you save a copy of the ignition settings for future reference in case of server re-installation.

15. Click **Apply**.

    The system applies the changes. The ignition process can take up to eight minutes.

16. The system displays the Web Manager login page. The first time you log in, you receive a prompt regarding background synchronization. Click **Yes**.

Next steps

Start IP Office Manager.

Starting IP Office Manager

You can start IP Office Manager using Web Manager. When a Server Edition Secondary server is present, you cannot launch Manager using Web Manager from the Server Edition Secondary server, unless the Server Edition Primary server is down.

You can start Manager without using Web Manager if you installed Manager on your computer. To install Manager, use the IP Office Admin DVD or **AppCenter** page of the Server Edition Primary server. For more information, see *Administering Avaya IP Office™ Platform with Manager*.

Note:

When you start Manager using Web Manager for the Server Edition Secondary server, you can manage only the systems that are online. After the Server Edition Primary server is up, you must synchronize the offline and online configurations.

Before you begin

- Start Web Manager.
- Log in as *Administrator*.
- To start Manager using Web Manager, install the latest Java Runtime Environment (JRE) Oracle version.

Procedure

In the Web Manager menu bar, click **Applications** and then **IP Office Manager**.

The system automatically loads the IP Office configuration file from the primary server. To load an alternate IP Office configuration file, select the appropriate server.

Result

The system checks if Manager is installed. The system also checks for the version of Manager that is installed.

The system prompts you to download and install the latest version of Manager in the following situations:

- If the version of Manager is not the latest.
- If Manager is not installed.

Next steps

Do one of the following:

- Click **OK**, to open the current version of Manager that the system has detected.
- Download and install the latest version of Manager. Then restart your browser.
- Select **Start** > **Programs** > **IP Office** > **Manager** to open Manager directly from the computer.

Configuring the IP Office Server Edition server using IP Office Manager

This procedure is the third and final stage in commissioning IP Office Server Edition using the Initial Configuration Utility (ICU) in IP Office Manager.

Before you begin

Start Manager.

Procedure

1. Start Manager and log on as **Administrator**.

   The Initial Configuration Utility appears.

2. Make changes as required, and click **OK**.

   The system displays the following warning message: `The system configuration will be extensively modified and converted as per ICU option section.`

3. Set the configuration of Server Edition server in the Avaya IP Office Initial Configuration window.

   a. Verify that the **System Type** is set as **Server Edition Primary**, **Server Edition Secondary**, or **Server Edition Expansion** as per the selection you made during the ignition process.

   b. In the **System Name** field, set the name to identify the system.

      The Gatekeeper feature uses this name to identify the system. The name must be unique within the network. You cannot use the characters <, >, |, \0, :, *, ?, . or /.

c. For Select deployments, click the **Select System** check box.

   Do not select Hosted Deployment for non-hosted systems.

d. If the system type is **Server Edition Secondary**, or **Server Edition Expansion**, you must enter and confirm the **WebSocket Password**.

e. Set the default telephony and language settings for the system in the **Locale** field.

f. Set the device IP of the system in the **Services Device ID** field.

   The system displays this ID for the system in the Server Edition and System Inventory pages.

g. Select the LAN interface for the system in the **LAN Interface** section. In the LAN Interface field, select the LAN interface for the system.

h. Set the IP address of the server in the **IP Address** field.

i. Set the IP mask address of the server in the **IP Mask** field.

j. Set the gateway address of the server in the **Gateway** field.

k. Set **DHCP Mode**. In the DHCP Mode area, select the appropriate option.

l. (Optional) Type the IP address of the Server Edition Secondary server in the **Server Edition Secondary** field.

m. Type the IP address of the DNS server in the **DNS Server** field.

n. Click **Save** to save the configuration details that you set for the system.

   The system reboots.

Chapter 4: Provisioning a Server Edition Secondary Server

Server Edition Secondary server

The Server Edition Secondary server is an optional server where you can add an additional users, IP trunking, and conference channels. The secondary server provides resilience to the users, phones, hunt groups and voicemail configured on the primary server. The secondary server also provides resilience to the users and phones configured on an expansion system. The secondary server is the management access point when the primary server is offline.

You can configure a 306961/R620, 270393/DL360, 270395/DL120 or a 302788/R210 as a Server Edition Secondary server.

Note:

You must configure both the Server Edition Primary server and Server Edition Secondary server on either HP DL360G7 or HP DL120G7/Dell R210. You cannot have a combination of HP DL120G7/Dell R210 and HP DL360G7.

For information on capacity, see the Capacity Planning document on the Avaya Support website at https://support.avaya.com/.

Adding a Secondary server

If you have purchased a pre-installed IP Office Server Edition server, then you can skip this step and proceed to Configuring using the ignition process on page 19.

Before you begin

- Install IP Office Server Edition on the server that you want to add as a Server Edition Secondary server. During the ignition process, set the role of the server as **Secondary**.
- In Web Manager for the primary server, open Manager by selecting **Applications** > **IP Office Manager**

Procedure

1. In the Server Edition Solution view, on the right side under **Add**, click **Secondary Server**.

2. In the Add Secondary Server window, enter the IP address of the Secondary server and click **OK**.
3. You are prompted to run the offline configuration tool.

   If you have not configured a Server Edition Secondary server, then you can create an offline configuration. The system saves a copy of offline configuration in Server Edition Primary server. After you configure the Server Edition Secondary server, you can select the offline configuration that you saved.
4. Select one of the following:
   - **Yes**: You are taken through the process of creating a basic offline configuration for the system. That configuration is then editable in Manager as part of the Server Edition network configuration. When the configuration is saved, a copy of it is saved on the Primary Server.
   - **No**: The new system is added to the network configuration but cannot be edited. You can right click on the system and select **Create Offline Configuration**.
   - **Discard**: The configuration is not added.

   For more information on creating an offline configuration, see *Administering Avaya IP Office™ Platform with Manager*.

Next steps

- Add the licenses for the Server Edition Secondary server.
- The addition of a secondary server or expansion system requires updates to the configuration of the one-X Portal for IP Office in order to support that system. The details of how to add the provider entries required in the one-X Portal for IP Office configuration, refer to *Administering Avaya one-X® Portal for IP Office™ Platform* .

Removing a Secondary server

Before you begin

- Ensure that there are no active calls.
- Ensure that Voicemail Pro is not active on Server Edition Secondary server.

  Use Voicemail Pro client and switch the Voicemail Pro to Server Edition Primary server.
- Ensure that phones and users are not active on Server Edition Secondary server.

  Use the System Status Application and switch the phones and users to the Server Edition Primary server.

Procedure

1. In the Server Edition Solution View, at the bottom, right-click on the secondary server.
2. Select **Remove**.

3. Click **Yes** to confirm.

   The system reboots the secondary server that you removed from IP Office Server Edition Solution.

Result

The system does not list the secondary server in the **Server Edition** window.

Next steps

Save the changes that you made to the configuration.

Note:

If you do not save the configuration, when you reopen the configuration, the system lists the secondary server in the **Server Edition** window, and the status of the *Primary Link* as *Primary to Secondary*.

Chapter 5: Provisioning a Server Edition Expansion System

Server Edition Expansion System

Server Edition Expansion System is an adjunct call system that you can add to a Server Edition network. A Server Edition Expansion System can be deployed on IP500 V2 hardware or it can be a Linux (L) based system on HP DL120G7 or Dell R210 hardware.

A Server Edition Expansion System (L) supports only IP network. A Server Edition Expansion System (V2) supports both analogue, TDM and IP networks and data features such as IP routes, NAT, Firewall, and IPsec. Added expansion systems can be any combination of Server Edition Expansion System (V2) or Server Edition Expansion System (L).

Related links

Server Edition Expansion System (V2) versus Server Edition Expansion System (L) on page 29

Server Edition Expansion System (V2) versus Server Edition Expansion System (L)

The following table compares the key features in Server Edition Expansion System (V2) and Server Edition Expansion System (L).

Feature	Expansion (V2)	Expansion (L)	Expansion (L) Comments
Operating system	IP Office OS – Multos	Linux Centos	
Endpoint Support	Maximum 384 from: Analogue Digital SIP H.323 IP DECT (max 384) Wi-Fi	Maximum 750 from: SIP H.323 IP DECT (max 384) Wi-Fi	Analogue supported through SIP ATA

Table continues…

Feature	Expansion (V2)	Expansion (L)	Expansion (L) Comments
Trunk Support	SIP (max 125) H.323 (max 125) Analogue (max 204) T1/E1 CAS (max 8) T1/E1 PRI (max 8) So/To BRI (max 16)	SIP (max 125) H.323 (max 125)	Analogue supported via SIP ATA. IP trunk capacity is registered trunks, not channels/calls.
Media Server/ Processing	Provided by additional DSP (VCM) modules. Up to 148 physical DSP channels.	Integrated media server. Up to 1400 logical media channels.	Media channels used for - 2 party calls - conferencing - transcoding
Codecs	G.711 A/mu G.729a/b G.723 G.722 T.38	G.711A/mu G.729a G.722	
Conferencing	Base platform DSP: 128 Conference channels, 64 party maximum	Integrated media server. 128 Conference channels, 128 party maximum	
Hunt Groups	200 per Expansion (V2)	500 per Expansion (L)	
Administration	IP Office Manager IP Office Web Manager	IP Office Manager IP Office Web Manager	Common management application
Licensing ID	SD Card FK S/N Can be moved	System ID Fixed to hardware	Separate mechanism for OVA.
IPSec/L2TP/PPP	Supported	Not supported	
CTI WAV	Supported	Not supported	CTI Pro is supported
LAN 1/LAN 2	For information on LAN support, see *Deploying Avaya IP Office™ Platform Server Edition*.		
PKI trust domains	Supported	Supported	
Music On Hold	Analogue extn input Audio jack Wav file (common)	USB audio jack input Wav file (restart or common) Wav directory (restart or common)	Wav directory up to 255 files. USB audio not supported on OVA.

Table continues…

Feature	Expansion (V2)	Expansion (L)	Expansion (L) Comments
	Streamed from the Primary/Secondary Beep	Streamed from the Primary/Secondary Beep	
Rated performance			
Call processing (BHCC)	7200	7200	Not increased with R620 Expansion server.
Maximum concurrent direct media calls	384	750	
Maximum concurrent RTP Relay calls	120	128	
Maximum concurrent SRTP indirect media calls	40	60	
Maximum concurrent TDM<> IP calls	120	n/a	
Maximum concurrent transcoding calls	74 (148/2)	64	

Related links

Server Edition Expansion System on page 29

Adding a Server Edition Expansion System

Use this procedure to add a Server Edition Expansion System (V2) or Server Edition Expansion System (L).

- If you have purchased a pre-installed Server Edition server, perform this procedure to ensure you have the latest version of the software installed.
- If you are converting an existing IP500 V2 system, see Converting an IP500 V2 System on page 34.

Before you begin

- Install IP Office Server Edition on the server that you want to add as a Server Edition Expansion System. During the ignition process, set the role of the server as **Expansion**.
- In Web Manager for the Server Edition Primary, open Manager by selecting **Applications** > **IP Office Manager**

Procedure

1. In the Server Edition Solution view, on the right side under **Add**, click **Expansion System**.
2. In the Add Expansion System window, enter the IP address of the Expansion system and click **OK**.

3. If you have opted for an offline configuration tool for the server edition expansion system, you are prompted to run the offline configuration tool.

   If you have not configured a Server Edition Expansion System, then you can create an offline configuration. The system saves a copy of offline configuration in Server Edition Primary server. After you configure the Server Edition Expansion System, you can select the offline configuration that you saved. The SE Central Access on nodes will be added offline in primary and in the actual node (expansion). IP Office line needs to be created manually to connect to the primary server. Once both the end lines are up and running, primary server can detect the added node. The SE Central Access check box is located at **Manager** > **File** > **Preferences**

4. Select one of the following:

   - **Yes**: You are taken through the process of creating a basic offline configuration for the system. That configuration is then editable in Manager as part of the Server Edition network configuration. When the configuration is saved, a copy of it is saved on the Primary Server.
   - **No**: The new system is added to the network configuration but cannot be edited. You can right click on the system and select **Create Offline Configuration**.
   - **Discard**: The configuration is not added.

   For more information on creating an offline configuration, see *Administering Avaya IP Office™ Platform with Manager*.

Result

The system displays the details of the new Server Edition Expansion System in the **Server Edition** window.

Note:

When you configure the Server Edition Expansion System server online, the system displays the status of the device as green in the **Server Edition** window. For more information on device and link status, see the *IP Office Manager* document.

When you add a Server Edition Secondary or a Server Edition Expansion System you must administer Avaya one-X® Portal for IP Office to connect to the new system. For more information, see the *Configuring IP Office Server Edition systems in Avaya one-X® Portal for IP Office* section of this document.

Next steps

- Add the licenses for the Server Edition Expansion System.
- The addition of a secondary server or expansion system requires updates to the configuration of the one-X Portal for IP Office in order to support that system. The details of how to add the provider entries required in the one-X Portal for IP Office configuration, refer to *Administering Avaya one-X® Portal for IP Office™ Platform* .

Removing an expansion system

Before you begin

Ensure that there are no active calls in the expansion system.

Procedure

1. In the Manager **Solution** view, right-click the expansion system that you want to remove.
2. Select **Remove**.
3. Click **Yes** to confirm.

   The system reboots the expansion system that you removed from IP Office Server Edition Solution.

Result

The system does not list the expansion system that you removed in the **Server Edition** window.

Next steps

Save the changes that you made to the configuration.

Note:

If you do not save the configuration, when you reopen the configuration, the system lists the expansion system in the **Server Edition** window, and the status of the *Primary Link* as *Primary to System*.

Note:

Before you use the expansion system in another deployment, default the expansion system that you removed. In Manager, select **File** > **Advanced** > **Erase Configuration (Default)**.

Chapter 6: Converting a Standard Mode IP500 V2 System to Server Edition

Related links

Converting an IP500 V2 System Using the ICU on page 34
Configuring an IP500 V2 as a Server Edition Expansion System (V2) on page 36
Moving Elements of an existing IP500 V2 configuration to a Linux based Server Edition Server on page 37
Manually migrating a full IP500 V2 configuration on page 38

Converting an IP500 V2 System Using the ICU

When an existing IP500 V2 system is added to a Server Edition solution as a Expansion System (V2), those parts of its configuration that do not match the default settings for an expansion system are overwritten. Settings are only retained where they don't conflict with the default settings.

The Initial Configuration Utility (ICU) is a necessary step in the initial configuration of all Server Edition systems. Once the initial configuration phase is complete, the result is a system that can be managed from the Server Edition Primary server as an integral part of a IP Office Server Edition Solution. The ICU setting **Retain Configuration Data** can be selected to support converting an existing IP500 V2 system to a Server Edition Expansion System. The following table lists what is retained, deleted or modified by the ICU.

Configuration Area	Retain Configuration Data	
	Off	**On**
System	Numerous changes to: • Licensing • LAN1/2 • DHCP • DNS • Directory • Voicemail • Auto user/ extn. • Time • Server Edition Flag • Syslog	Numerous changes, same as default
Line	• All IP trunks removed • IP Office trunks added	All previous IP Office trunks removed IP Office trunks added
Control Unit	No	No
Extension	• IP extensions deleted • Analog/digital extensions un-numbered	No changes
User	All users deleted	No changes
Group	All groups deleted	No changes
Short codes	All feature short codes deleted except on Primary	No changes
Service	No changes	No changes
RAS	No changes	No changes
ICR	Delete all	No changes
WAN Port	No changes	No changes
Directory	Delete all except on Primary	No changes
Time Profile	All time profiles deleted	No changes
Firewall Profile	No changes	No changes
IP Route	Add gateway route	Add gateway route
Account Code	Delete all	No changes
License	Delete all	No changes
Tunnel	No changes	No changes
User Rights	All user rights deleted	No changes
E911	E911 extension list deleted	No changes

Table continues…

Configuration Area	Retain Configuration Data	
	Off	On
ARS	Add default entry for primary/secondary	Add default entry for primary/secondary
Location	Delete all	No changes
Authorization Code	No changes	No changes
Security Settings	Configuration, Security and Web Services security level Medium	Configuration, Security and Web Services security level Medium
Call log	No changes	No changes
DHCP allocation	No changes	No changes

Related links

Converting a Standard Mode IP500 V2 System to Server Edition on page 34

Configuring an IP500 V2 as a Server Edition Expansion System (V2)

The supported conversion areas are:

- All configuration except
  - some system attributes
  - Directory
  - Embedded voicemail
- All security settings
- Call logs
- DHCP allocations

Before you begin

You must have:

- the correct target software version installed
- valid configuration data

Procedure

1. Back up the configuration before making any changes.
2. Run the ICU with **Retain Existing Configuration** checked.
3. Review and test the resulting configuration.
4. Back up the configuration.

Related links

Converting a Standard Mode IP500 V2 System to Server Edition on page 34

Moving Elements of an existing IP500 V2 configuration to a Linux based Server Edition Server

The supported Configuration conversion areas are:

- Directory
- Users
- Groups, except non-advertised
- Short Code

Before you begin

You must have:

- the correct target software version installed
- valid configuration data

Procedure

1. Using IP Office Manager, select **File** > **Offline** > **Receive Configuration** to save a copy of the existing IP500 V2 system configuration onto your Computer.
2. Select **File** > **Offline** > **Open File** to open that configuration in IP Office Manager.
3. Use IP Office Manager to delete analogue/digital trunks/extensions and any other entries not required.
4. Convert any hunt groups to network advertised.
5. Save as offline file in case of errors.
6. Use CSV or binary export to extract required areas of configuration to local files. Do not use the whole configuration option.
7. Use IP Office Manager to read the Server Edition server configuration.
8. Use CSV or binary import to include required areas.
9. Manually update any System attributes required.
10. Resolve all warnings and errors before saving to the Server Edition server.
11. Save to the Server Edition server.
12. Review and test the resulting configuration.
13. Back up the configuration.

Related links

Converting a Standard Mode IP500 V2 System to Server Edition on page 34

Manually migrating a full IP500 V2 configuration

You can migrate a Server Edition Expansion System (V2) manually using CSV import and export.

Note:

Only experienced technicians should attempt to convert configuration settings using CSV import and export. Avaya recommends you use the ICU for all conversions.

The following table lists what the system retains and modifies when manually converting a configuration using CSV import and export.

Configuration Area	Migration allowed	Potential migration issues	Manager Detect/ Correct?	Comments
System	Partial	• Server Edition mode is reset. • Removes many ICU changes resulting in solution integration issues.	• No • Some	Do not attempt to migrate whole system settings.
Line	Yes	• Line numbering duplication • No Analog/Digital support on Linux	• Yes • Yes	• Manager line renumbering is not solution wide and must be done individually. • Only if V2 to Linux conversion is considered.
Control Unit	No	None – unit entries are regenerated.	No	Unnecessary migration data. All control unit entries are regenerated at platform start-up.
Extension	Yes	• Duplicate extension numbers. • Duplicate extension IDs. • No Analog/Digital support on Linux	• Yes • Yes	• Resolvable in Manager • Resolvable in Manager • Only if V2 to Linux conversion is considered.
User	Yes	• Duplicate user names. • Duplicate user extensions. • CCR Agent settings	• Yes • Yes • Yes	• Resolvable in Manager • Resolvable in Manager • Resolvable in Manager

Table continues…

Configuration Area	Migration allowed	Potential migration issues	Manager Detect/ Correct?	Comments
Group	Yes	Non network advertised groups not supported	Yes	Non network advertised groups cannot be resolved.
Short codes	Yes	• Existing global short codes are no longer global. • Existing Call routing	• Varies • Yes	• Any common feature short code that is not part of the migrated configuration will disappear from the top level but is resolvable in SE manager. If Manager is in Consolidated mode, a prompt to harmonize to the Primary common items is offered. • Resolvable in Manager.
Service	Yes V2 Expansion only	Linux only supports the SSLVPN service	Yes	Only for IP500 V2 to V2 Expansion System migrations.
RAS	Yes V2 Expansion only			Only for IP500 V2 to V2 Expansion System migrations. No Linux support
ICR	Yes	Existing global ICRs are no longer global.	Varies	Any common feature short code that is not part of the migrated configuration will disappear from the top level but is resolvable in SE manager. If Manager is in Consolidated mode, a prompt to harmonize to the Primary common items is offered.
WAN Port	Yes V2 Expansion only	No Linux support.		Only for IP500 V2 to V2 Expansion System migrations.
Directory	Yes	Expansion directory entries cannot be deleted.	Yes	Use CSV export/import to migrate to Primary. Use non Server Edition Manager to delete entries.

Table continues…

Configuration Area	Migration allowed	Potential migration issues	Manager Detect/ Correct?	Comments
Time Profile	Yes	Existing global Time Profiles are no longer global.	Varies	Manager allows per system Time Profiles. Any that do not map to common Time Profiles will make that Time Profile disappear from the top level but it is resolvable in Manager. If Manager in Consolidated mode, a prompt to harmonize to the Primary common items is offered.
Firewall Profile	Yes V2 Expansion only	No Linux support.	No	Only for IP500 V2 to V2 Expansion System migrations.
IP Route	Yes V2 Expansion only	No Linux support.	No	Only for IP500 V2 to V2 Expansion System migrations.
Account Code	Yes	Existing global account codes stop being global.	Varies	
License	Yes V2 Expansion only	Some will not be supported.	Yes	Once saved and loaded from IP Office, marked as invalid/obsolete Resolvable in Manager
Tunnel	Yes V2 Expansion only	No Linux support.	Yes	
User Rights	Yes	Existing global user rights are no longer global.	Varies	Manager allows per system user rights. Any that map to common user rights will make that user right disappear from the top level but it is resolvable in Manager. If Manager in Consolidated mode, a prompt to harmonize to the Primary common items is offered.
E911	No	No support.	No	Enhanced 911 not supported.

Table continues…

Configuration Area	Migration allowed	Potential migration issues	Manager Detect/ Correct?	Comments
ARS	Yes	Existing Call routing	No	Resolvable in Manager
Location	Yes	Existing global locations stop being global.	Varies	Manager allows per system locations. Any that map to common locations will make that user right disappear from the top level but it is resolvable in Manager. If Manager in Consolidated mode, a prompt to harmonize to the Primary common items is offered.
Authorization Code	Yes			
Security Settings	Yes V2 Expansion only	Can only migrate using SD card. ICU may not work if PKI trust domain active.	Yes	PC running ICU must be in PKI trust domain. May have to be changed manually if security settings extensively modified.
Call log	Yes V2 Expansion only		No	Internal configuration file on SD Card mapped to users. Not deleted on upgrade or change of mode from Standard to Server Edition.
DHCP allocation	Yes V2 Expansion only		No	Internal configuration file on SD Card containing DHCP allocations. Not deleted on upgrade or change of mode from Standard to Server Edition.

Related links

Converting a Standard Mode IP500 V2 System to Server Edition on page 34

Chapter 7: IP Office Platform Server Edition LAN support

Warning:

You must ensure the IP Office Line network links between Server Edition systems are either all LAN1, or all LAN2. Failure to adhere to this can reduce efficiency and limit some functionality. The recommended configuration is to use the Server Edition Linux LAN1 for all Ethernet traffic with LAN2 disconnected, and all nodes connected via LAN 1.

Additionally, full application and telephony functionality is available through LAN1 for all Linux servers. There is limited access through LAN2 for one-X Portal client voicemail playing.

There are some differences between the functionality of the LAN interfaces of the Server Edition Expansion System (L) and IP500 V2 based Server Edition Expansion System (V2) platforms. Some of the differences are:

- No IPsec, PPP, NAT or NAPT support on Server Edition Linux.
- No IP routing support on Linux.
- Configuration of a Linux Firewall is limited. No traffic is routed between LAN1 and LAN2, except VoIP media (RTP).

The LAN2 interface of the Server Edition Linux platform has fewer capabilities than LAN1.

- A one-X Portal client cannot listen to voicemail messages.
- You cannot launch the Server Edition Manager and other clients from Web Control.
- External MAPI and SMTP voicemail servers cannot be accessed via LAN2.

The following table details the LAN supported features for Server Edition Expansion System (V2) and Server Edition Expansion System (L) platforms.

Feature	IP500 V2 LAN1	IP500 V2 LAN2	Linux LAN1	Linux LAN2	Notes
Interface Layer1 - Layer4					
Interface Support	Yes	Yes	Yes	Yes	
Physical<>logical interface mapping	Fixed: ‘LAN’	Fixed: ‘WAN’	Yes	Yes	
Speed	10/100	10/100	10/100/ 1000	10/100/ 1000	
Duplex	Full/half	Full/half	Full/half	Full/half	

Table continues…

Feature	IP500 V2 LAN1	IP500 V2 LAN2	Linux LAN1	Linux LAN2	Notes
802.1Q VLAN support	No	No	Yes	Yes	Static o/g VLAN assignment via administration IP500 V2 strips any received VLAN tag, all o/g packets have no VLAN tag
DSCP/ToS	Yes	Yes	Yes	Yes	Linux LAN2 uses LAN1 DSCP settings – any LAN2 settings are ignored
Default gateway/route	Yes	Yes	Yes	Yes	Linux via ignition or Web Control
Proxy ARP	Yes	Yes	No	No	IP500 V2 acts as an L3 router
IP Multicast	Yes	Yes	No	No	
Inter LAN					
Firewall	Yes	Yes	Yes	Yes	A Linux ingress/egress firewall can be activated, with further controls for specific unsecure ports such as TFTP and HTTP. No differentiation between LAN1 and LAN2
IP Routes	Yes	Yes	No	No	No configurable IP routing between Linux LAN interfaces All received Linux LAN traffic that is not destined for the node is discarded except VoIP media which is allowed to traverse with NAT
NAT/NAPT	Yes	Yes	No	No	
PPP	Yes	Yes	Yes	No	
Clients					
1XP client – basic	n/a	n/a	Yes	Yes	
1XP client – VM listen	n/a	n/a	Yes	No	
One-X Mobile Preferred	n/a	n/a	Yes	Yes	
One-X Mobile Preferred – VM listen	n/a	n/a	Yes	No	
Avaya Communicator	Yes	Yes	Yes	Yes	
One-X Plugins	n/a	n/a	Yes	Yes	
SoftConsole	Yes	Yes	Yes	Yes	

Table continues…

Feature	IP500 V2 LAN1	IP500 V2 LAN2	Linux LAN1	Linux LAN2	Notes
VMPro – MAPI Link	n/a	n/a	Yes	Yes	Two way MS Exchange VM Integration via MAPI or EWS
VMPro – SMTP	n/a	n/a	Yes	No	One way IMAP/Exchange VM integration
Administration					
IP Office Manager	Yes	Yes	Yes	Yes	Also accessible via IPOSS remote tunnel (SSLVPN)
Server Edition Manager	Yes	Yes	Yes	Yes	Access should be the same LAN1/2 interface as the inter-node connections Also accessible via IPOSS remote tunnel (SSLVPN)
SSA	Yes	Yes	Yes	Yes	Also accessible via IPOSS remote tunnel (SSLVPN)
SysMon	Yes	Yes	Yes	Yes	Also accessible via IPOSS remote tunnel (SSLVPN)
Web Manager	Yes	Yes	Yes	Yes	Cannot launch other clients (including Manager and Linux Platform Management) when not accessed via LAN 1 Also accessible via IPOSS remote tunnel (SSLVPN)
VMPro Client	n/a	n/a	Yes	Yes	Also accessible via IPOSS remote tunnel (SSLVPN)
Linux Platform Management	n/a	n/a	Yes	Yes	Was Web Control in Server Edition Release 8.1 Also accessible via IPOSS remote tunnel (SSLVPN)
Admin launch from Web Manager	n/a	n/a	Yes	Yes	Launch of IP Office Manager, SSA, Voicemail Pro client, Linux platform management from Web Manager. Not supported via IPOSS remote tunnel (SSLVPN).
Protocols					
DHCP	Yes	Yes	Yes	Yes	Client and server
BOOTP	Yes	Yes	Yes	No	
TFTP	Yes	Yes	Yes	Yes	

Table continues…

Feature	IP500 V2 LAN1	IP500 V2 LAN2	Linux LAN1	Linux LAN2	Notes
HTTP/S	Yes	Yes	Yes	Yes	Client and server, including embedded file management, web services, phone files Backup/restore
SCP	No	No	Yes	Yes	Backup/restore
FTP	No	No	Yes	Yes	Backup/restore
SFTP	No	No	Yes	Yes	Backup/restore
PPP	Yes	Yes	No	No	
IPsec	Yes	Yes	No	No	
VPN (L2TP/PPTP)	Yes	Yes	No	No	
RIPv2	Yes	Yes	No	No	
SSLVPN	Yes	Yes	Yes	Yes	
NTP	Yes	Yes	Yes	Yes	Client and server SNTP operation
TIME	Yes	Yes	No	No	RFC 868
TSPI	Yes	Yes	Yes	Yes	CTI interface for TAPI and one-X Portal
SNMP	Yes	Yes	Yes	Yes	Traps and MIBs, v1 only
SMDR	Yes	Yes	Yes	Yes	Emission and collection
DNS	Yes	Yes	Yes		
Syslog (UDP+TCP +TLS)	Yes	Yes	Yes	Yes	Alarms, audit trail, debug
Telephony					
H.323 trunks (including SCN)	Yes	Yes	Yes	Yes	LAN1 and LAN2 should not be mixed for SCN. Should be all LAN1 or all LAN2. This also includes SE Manager access
H.323 phones	Yes	Yes	Yes	Yes	Phones must be configured with ‘local’ registrar IP address – e.g. not possible to access LAN2 registrar via LAN1
H.323 Remote worker phone	Yes	Yes	Yes	Yes	
IP DECT	Yes	Yes	Yes	Yes	
SIP trunks	Yes	Yes	Yes	Yes	
SIP phones	Yes	Yes	Yes	Yes	

Table continues…

Feature	IP500 V2 LAN1	IP500 V2 LAN2	Linux LAN1	Linux LAN2	Notes
STUN	Yes	Yes	Yes	Yes	
IP Office Softphone	Yes	Yes	Yes	Yes	
Avaya Communicator Essential	Yes	Yes	Yes	Yes	

Chapter 8: Upgrading

Server Edition upgrade policy

Both *Minor* and *Major* Server Edition upgrades are supported.

Minor Upgrades

- *Minor* Server Edition upgrade is an upgrade from one release to another minor release in that series including Service Packs (SP). For example: 10.0 GA to an 10.0 SP or 10.0 SP to another 10.0 SP
- *Minor* upgrade does not require a manual pre or post upgrade activities such as database exporting/import, configuration resets.
- *Minor* upgrade does not result in the loss of configuration, logs or other stored data.

Major Upgrades

- *Major* Server Edition upgrade is an upgrade from one major release series to another release series, including Feature Packs (FP).For example, 8.1 GA to 8.1 FP or 8.1 FP to 9.0 SP or 9.1 FP to 10.0 GA
- *Major* does not require a manual pre or post upgrade activities such as database exporting/import, configuration resets, however this cannot be guaranteed.
- *Major* upgrade does not result in the loss of configuration, logs or other stored data, however this cannot be guaranteed

Upgrades with Patches Present

Major or Minor Upgrades to systems that are patched are supported. However, depending upon the patched component, the process may differ from the standard case.

- Before any activity, please check with the group that issued the patch and review any patch notes.
- Any patch should be reverted prior to upgrade. This must be done if the Server Edition Primary server is patched, or else the solution upgrade will fail.
- The normal upgrade process can then be followed, including taking a backup before reapplying any patches.
- After upgrade, if the original or an updated patch must be reapplied, apply the patch manually to every component as per the patching instructions.
- Perform a backup after applying the patch.

Upgrade Licenses

- To upgrade from one Server Edition release to another, for example, from 9.1 to 10.0 , you need to add Server Edition Software Upgrade license(s) to Server Edition Primary for correct telephony operation. You can add the upgrade license before or after an upgrade.
- To upgrade to a Feature Pack release, for example, from 8.1 to 8.1 FP, you do not need a Server Edition Software Upgrade license.
- From Release 10.0 onwards, use PLDS licenses only. ADI licenses are not supported in R10.
- The prior releases of IP Office used to support Avaya WebLM Release 7 that had 12–digit Host ID. IP Office Release 11 supports Avaya WebLM R7.1 that has 14–digit Host ID, the old Host ID with a suffix – “03”. Customers upgrading IP Office from previous releases, must apply for the upgrade license based on the 12–digit Host Id prior to upgrading.
- When you upgrade IP Office Server Edition from Release 10 to Release 11, the WebLM password is automatically reset to default password, that is, `weblmadmin`.

Upgrade Configuration Data

IP Office component configuration data is upgraded automatically when the new version is initially executed for both major and minor upgrades. Typically new attributes are set to a default value although this is overridden in some instances. Consult the release notes of the prospective version.

Upgrading IP500 V2 Expansion Systems to Release 9.1

Existing IP500 V2 expansion systems running a release lower than 8.1.1.0 must first upgrade to 8.1 (8.1.1.0 or higher) or 9.0 (any) before being upgraded to 9.1. The upgrade licenses for 9.1 are also valid for the lower releases.

Viewing Application Servers in Web Manager After Upgrade to Release 10

After upgrading to release 10, Application Servers are not visible on the Web Manager **Solution** page. They must be manually added.

To add an Application Server,

1. On the Web Manager **Solution** page, click **Solution Settings** > **Application Server** > **Add**.
2. In the Add Application Server window, enter the **Application Server IP Address**.

Server Edition downgrade policy

Both *Minor* and *Major* Server Edition downgrades are supported, however for a major downgrade you need to install Server Edition again:

1. Review the release notes of the current version before you downgrade.
2. Take a backup of the solution backup from Web Manager of Server Edition Primary before you downgrade. The backup should include all systems, components and configuration data sets.
3. Perform downgrade when there is no traffic on the system because it affects the service of the system.

4. *Minor* downgrade is a downgrade from one previously installed minor release to another in the same series. For example: 8.1 SP to 8.1 SP or 8.1 SP to 8.1 GA
5. *Minor* Linux server downgrade can be performed using the Web Manager package manager by qualified personnel only for the following IP Office components: IP Office, Jade Media Server, Avaya one-X® Portal for IP Office, Voicemail Pro Server or client, Web Control and Web Manager. You cannot downgrade any other component.
6. You can perform a *Minor* Linux server downgrade by performing a complete reinstallation and re-ignition.
7. You can perform a *Major* Linux server downgrade, for example, a downgrade from 9.0 to 8.1 or from 9.1 to 9.0 GA only by reinstallation and re-ignition. Do not attempt to downgrade a component through the Web Manager. In addition, all servers require downgrade because IP Office Server Edition Solution does not support mixed versioning.
8. You can downgrade Server Edition Expansion System through the IP Office Manager memory card Restore command.

   After you downgrade, to restore the corresponding backup, use Web Manager.

   Note:

   For Release 8.1 when you restore the system through Web Control, the system does not restore IP Office Security settings for any device other than Server Edition Primary . To restore the IP Office configurations, use the configuration synchronization feature of IP Office Manager .
9. Ensure that all components of a Server Edition deployment have the same software version.
10. Subsequent upgrade of a *Minor* or *Major* downgrade are supported

    Note:

    Avaya reserves the right to change Server Edition downgrade policy at some time in the future.

Downgrade configuration data

When you downgrade, the system does not downgrade the configuration data of the component automatically when the new version is initially executed. You need to restore the correct configuration version or administer new configuration data.

To achieve IP Office configuration reuse where no corresponding backup data is available, use the CSV export/import feature of IP Office Manager:

- Read the latest configuration into IP Office Manager offline. IP Office Manager supports all configuration versions up to its own version.
- Export configuration using File | Import/Export | Export, CSV, All of the configuration
- Default the configuration on the target system and read into IP Office Manager.
- Import each configuration using the File | Import/Export | Import, CSV, All of the configuration.
- Check/correct errors and warnings.
- Check configuration settings are as expected.
- Send to system and check operation

- For a IP Office Server Edition Solution , the process should start with the Primary, then secondary then expansion systems. Each should be done individually using Manager in ‘standard’ not IP Office Server Edition Solution mode.

Upgrade Process Summary

- Consult relevant release notes prior to any upgrade or downgrade
- Backup before and after any upgrade or downgrade

Note:

You must take a backup of the Contact Recorder database before upgrading your IP Office to Release 11. Once you upgrade IP Office to Release 11, you will not be able to access or back up Contact Recorder database.

- *Minor* Linux upgrades can be downgraded to a previously installed release, IP Office components only.
- *Major* Linux upgrades cannot be downgraded – reinstall is required
- *Minor* Linux upgrades does not cause loss of configuration, logs or other stored data; Major Linux upgrade may.
- Downgrades require application/restore of correct version configuration data
- Ensure that all components of a Server Edition deployment have the same software version.
- This is policy not an absolute guarantee; if for example Avaya fix a bug in a Service Pack that corrects an upgrade or configuration error, the policy may not apply, and would be highlighted in the release notes

Note:

Avaya reserves the right to change Server Edition upgrade or downgrade policy at some time in the future.

Upgrade Procedures

You can upgrade IP Office Server Edition Solution using the following methods:

- Burn the ISO image to a DVD or create a USB drive. Reboot the server with the DVD or USB as the first boot device.
- Transfer the ISO image to the Primary Server and upgrade using Web Manager.

Note:

Ensure that you use only one method to upgrade at a time. You cannot upgrade using more than method at the same time.

Downloading ISO using Web Manager

To upgrade IP Office Server Edition systems you can download the ISO file from a remote server, DVD, primary server path, or a client machine to the primary server. The system creates the repository data required for upgrade on Server Edition Primary server. The system uses the repository data on Server Edition Primary server, to upgrade all the components of IP Office Server Edition Solution.

Before you begin

If you want to download the ISO from a remote server or set the proxy, set the remote server and proxy settings by selecting **Solution Settings** > **Remote Server**. For more information about setting the remote server and proxy settings, see *Administering IP Office Platform with Web Manager*.

About this task

When you download ISO the system mounts the ISO, creates a repository data, and extracts the zip file.

Procedure

1. Log in to Web Manager.
2. In Solution window, click **Actions** and select **Transfer ISO**.
3. In the Transfer ISO window, do one of the following:
   - Download from a remote server.
     a. In **Transfer from** field, select **Remote Location**.
     b. In **File path** field, type the path where the ISO file is located on the remote server.
     c. In **Select Remote Server**, choose the remote server where the latest ISO is located.

     If you want to set a proxy server, enable **Use Proxy** and select the proxy server in **Select Proxy** field.
   - Download from primary server path.
     a. In **Download from** field, select **Primary Server Path**.
     b. In **File path** field, type the path where the ISO file is located in the primary server.
   - Download from the client machine.
     a. In **Download from** field, select **Client Machine**.
     b. In **Select ISO** field, browse to the location where the ISO file is located on the client machine.
   - Download from DVD of Primary server.
     a. Insert the installation DVD in the DVD drive of the Primary server.
     b. In **Download from** field, select **DVD Primary Server**.

4. Click **OK**.

Result

The system displays the progress of ISO download in the Download ISO window. When the download is complete, the servers in the server list display the **Upgrade Available** notification.

Upgrading using Web Manager

After you download the latest ISO in the primary server, the system displays the  Update Available icon in the Solution window for the servers.

Note:

Ensure that the version of the software on all the components of IP Office Server Edition Solution such as Server Edition Primary, Server Edition Secondary, Server Edition Expansion System , and the separate Avaya one-X® Portal for IP Office are the same.

Before you begin

Download the latest ISO using Web Manager.

It is recommended that you install upgrade licenses prior to the upgrade.

About this task

You can upgrade a single component or multiple components of IP Office Server Edition Solution using Web Manager.

Note:

You cannot upgrade IP Office Server Edition systems directly from a remote server. You must upgrade primary server first as the primary server cannot be upgraded with other systems.

Procedure

1. Log in to Web Manager.
2. In the server list on the Solution page, select the Primary Server.

   Click **Actions** and then select **Upgrade**.
3. In the Upgrade window, ensure that the Primary server is selected and click **OK**.

   Note that you can opt to schedule the upgrade at a later time by selecting **Use Schedule** and defining a scheduled time.
4. Select the **Restart IP Phones** check box if you want all the connected IP Phones to restart after the upgrade is complete.
5. You receive a prompt regarding upgrade licenses. Click **Yes**.
6. You receive a prompt for the License Agreement. Click **Accept** and then **Next**.
7. Click **Close** to close the Upgrade window.

8. You receive a prompt to confirm the upgrade. Click **OK**.

   The upgrade process begins.

9. After 30 minutes, log in to Web Manager.
10. You receive a prompt regarding background synchronization. Click **Yes**

    The upgrade continues and the server is rebooted. The server can take up to 20 minutes to completely restart.

11. Log in to Web Manager and upgrade the remaining systems. On the Solution page, in the server list, select all the remaining servers.
12. Click **Actions** and select **Upgrade**.
13. You receive a prompt regarding upgrade licenses. Click **Yes**.
14. You receive a prompt for the License Agreement. Click **Accept** and then **Next**.

    The upgrade process begins.

    During the upgrade process, the Secondary Server and all Linux expansion systems are rebooted. The server can take up to 20 minutes to completely restart.

Upgrading the system using an installation DVD or USB drive

Before you begin

It is recommended that you install upgrade licenses prior to the upgrade.

Procedure

1. Perform one of the following.
   - Insert the installation DVD in the DVD drive of Server Edition Primary server.
   - Insert the installation USB drive in the USB port of Server Edition Primary server.
2. Restart the Primary server.

   Note:

   To restart a Server Edition server, always use Web Manager. For more information, see Restarting a Server using Web Manager on page 87. For a new installation, power cycle the server.

   The system restarts and boots from the installation DVD or the installation USB drive.

   Note:

   If the system does not restart or boot from the installation DVD or the installation USB drive, then verify the boot order in BIOS settings.

3. Click **Change Language** to select the language for use during the installation or upgrade process.
4. Click **Next**.
5. Select the type of keyboard you would like to use for the system.
6. Click **Next**.
7. Select the language in which you would like to read the End User License Agreement (EULA).
8. Click **OK**.
9. Click **Yes, I have read, understood and accepted the terms of Avaya EULA**.
10. Click **Next**.

    The system prompts you to install or upgrade. If you are installing Server Edition on a server in which Server Edition is already installed, then the system displays the details of the applications that are already installed. The system also displays the details of the applications that the system will install.
11. Select **Upgrade** and then click **Next**.
12. You receive a prompt regarding licenses. Click **Next**.
13. Click **Next** to start the upgrade. The upgrade process can take up to one hour to complete.
14. You receive a prompt that the system has been successfully upgraded. Click **Next**.
15. You receive a prompt to install additional TTS languages. Click **Next**.
16. Remove the installation DVD or the installation USB drive and click **Reboot**.

    The upgrade continues and the server is rebooted. The server can take up to 20 minutes to completely restart.
17. Log in to Web Manager.
18. You receive a prompt regarding background synchronization. Click **Yes**.

Next steps

If a Secondary server or expansion systems are part of the Server Edition Solution, upgrade these systems. You can use Web Manager to upgrade the remaining systems or use the DVD or USB and reboot each server.

Upgrading the system automatically

You can upgrade IP Office Server Edition automatically using the installation USB drive.

- After you upgrade, you will not be able to downgrade to an older Release. You will have to reinstall IP Office Server Edition server.
- Upgrade standalone Application Server separately.

Before you begin

Server Edition installation USB drive. For more information, see Installation and Upgrade with a USB Drive on page 12.

Procedure

1. Insert the installation USB drive in the USB port of Server Edition server.
2. Restart Server Edition server.

   Note:

   To restart Server Edition server, always use Web Manager. For more information, see Restarting a Server using Web Manager on page 87. For a new installation, turn off the power supply to the server.

   The system restarts and boots from Server Edition installation USB drive.

   Note:

   If the system does not restart or boot from Server Edition installation USB drive, then verify the boot order in BIOS settings.

Result

The system upgrades Server Edition and shuts down Server Edition server.

Note:

When you upgrade Server Edition to 9.1, the system upgrades the version of CentOS to 6.4. For more information, see Checking the version of CentOS on page 103.

Next steps

Remove the installation USB drive from the USB port of Server Edition server.

Note:

To ensure service continuity take a complete solution backup using Web Manager.

Upgrading or changing the version of an application on a local server using Linux Platform settings

You can upgrade the application services hosted on IP Office Server Edition server without having to reinstall or upgrade the whole server. This is done using files either uploaded to the local server or in the repository server for update files. When a new .rpm file is available, the system lists the available versions.

Before you begin

Ensure that you have read the appropriate Avaya Technical Bulletins for the software release. The Technical Bulletins detail supported versions of software and known issues or additional actions required for upgrading.

About this task

You can upgrade only a local server using this procedure.

Procedure

1. On a client computer, start the browser and type `https://` *<IP address of the Server> :<port number>*.

   The default port number is *7071*.

2. Logon as *Administrator*.
3. Select **Updates**.

   In the **Services section**, the system displays current version and latest available version of each application service.

   Note:

   You cannot upgrade or change the version of some applications such as Avaya one-X® Portal for IP Office. The **Change Version** and **Update** buttons are disabled for such applications even if there are updates available in the application file repository. You must first uninstall the application to enable the **Change Version** and **Update** buttons.

4. Do one of the following:
   - To update an application to the latest version available, click **Update**.
   - To update all applications to the latest version available, click **Update All**.
   - To change the current version of an application, click **Change Version**. Select the version required and click **Apply**.

Chapter 9: Backup and Restore

This chapter looks at how the web manager menus can be used to configure backup and restore operation between servers.

- If the sever's own hard disk has sufficient capacity it can be used as its own backup. However, this is not a suitable solution for a backup that could be used to restore data in the case of a major failure. The recommendation its that backup should ideally be to another IP Office server.
- Within a primary/secondary server pair, reciprocal backup can be configured as an option.
- The preferred option is a separate backup server. This can be done by installing an IP Office Application server with a sufficiently large hard disk (see Disk space required for backups on page 60) and no services (Voicemail Pro and one-X Portal) enabled.

Warning:

- Backup/restore is not supported between different server software release levels. Any exceptions are specifically documented in software release notes and migration documents.
- You cannot restore data to a server unless either the IP Address or the system id (LAN1 MAC address) match the server from which it was backed up.
- Backup and restore action must only be performed using servers inside a secure, trusted network.

Related links

Backup and restore policy

It is essential to implement a comprehensive, robust and secure backup policy as part of a Business Continuity plan before any failure or other data restoration requirement. It is not possible to define a single approach that would meet all possible customer needs. Each installation should be assessed and an backup policy implemented. .

Backup Key Information

The backup process supported by web manager only includes specific data, see Backup data sets on page 61. There is key information which, though included in the backup data, should also be recorded separately in case it is necessary to rebuild a failed sever:

- The ignition settings for each server should be recorded. For example, IP address and host name settings, server role, etc. These details may be required if a full reinstallation of the server becomes necessary before any data restoration operation.

In addition, the following are not included in the web manager backup processes and so must be backed up using other manual processes.

- Copies of any PLDS license key files used by the system.
- If using web manager to load custom voicemail prompts, copies of those prompt files.
- Copies of any custom phone settings files plus phone screen saver and background images.

Backup Schedule

In addition to performing backups before major system changes such as an software upgrade, you must consider having a regular backup schedule.

- Periodic configuration backup for every IP Office.
- Periodic configuration backup for one X Portal – Server Edition Primary server and Application Server only
- Periodic configuration backup for Voicemail Pro – Server Edition Primary server only
- Periodic voice mailbox and recording data backup – Server Edition Primary server only
- The period and number of unique instances selected should reflect the frequency of change, the consequence due to data loss, and the storage capacity of the backup data server. It should also be bourne in mind that the backup server used will only retain up to 14 backups, after which any further backup will cause the automatic deletion of the oldest previous backup.
- The timing of backup operation: This should be done when little or no traffic is present on the target system(s), but the backup process itself is not service-affecting.

Additional Backup Options

This documentation only looks at the backup/restore process provided through the server's own web manager menus. The IP Office Manager and Voicemail Pro client application also provide methods for backing up the current IP Office service configuration and the voicemail configuration/ mailbox contents respectively. Therefore also consider:

- Manual backup of the IP Office service configurations before major configuration changes.
- Manual backup of the Voicemail Pro before major configuration changes.

Related links

Backup and Restore on page 57

Backup and restore protocols

Backup and restore is only supported using another IP Office server as the backup server. If necessary, an IP Office Application Server can be installed without enabling the Voicemail Pro and one-X Portal for IP Office services on that server.

Warning:

- Backup and restore action must only be performed using servers inside a secure, trusted network.

The server being backed up requires a remote server connection to the backup server. That connection is configured with the settings below (see Creating a remote server connection on page 63). For a set of networked servers, the connection from the primary server is used for all the servers.

Protocol	Port	Path	User Name/ Password	Notes
HTTPS	5443	/avaya/backup	none	HTTPS backup is enabled by default.
HTTP	8000	/avaya/backup	none	HTTP backup is disabled by default. To enable it on the backup server, see Enabling HTTP backup support on page 59.

Related links

Backup and Restore on page 57

Enabling HTTP backup support

By default, HTTP support for backup/restore is disabled. You can enable it using the following process on the backup server.

Security alert:

- Backup and restore action must only be performed using servers inside a secure, trusted network.

Enabling HTTP Backup Support on the Backup Server

1. Login to the web manager menus of the backup server.
2. Select the servers **Platform View** option.
3. Within the platform view menus, select **Settings** > **System** > **HTTP Server**.
4. Select the **Enable HTTP file store for backup/restore** option and click **Save**.

Related links

Backup and Restore on page 57

Disk space required for backups

The space required for a backup is highly variable. It depends on the number of servers includes in the backup and the data sets selected. However, the largest and most significant backup is that required for voicemail.

The following tables show the potential space required for a worst case full backup. That is, one that assumes all the users have used their voicemail mailbox and other facilities to their maximum capacity.

The minimum disk size column indicates the disk hard disk size required to have a sufficiently large backup quota (see above) for at least one maximum full backup.

Backup for a Sever Edition Network

Users	Maximum Full backup	Minimum Backup Server Disk Size
100	35GB	160GB
750	78GB	214GB
1500	127GB	275GB
2000	158GB	320GB
2500	189GB	360GB

Backup for an IP Office Application Server/Unified Communications Module

Users	Maximum Full backup	Minimum Backup Server Disk Size
20	30GB	160GB
50	32GB	160GB
100	34GB	160GB
150	37GB	165GB

Related links

Backup and Restore on page 57

Checking the backup server’s backup quota

Backup is supported to a server with a hard disk of 160GB or larger. The actual portion of that space, the backup quota, available for backup usage can be checked using the process below. On servers with a smaller hard disk, no backup quota is supported.

Estimating the Backup Quota

The approximate space that will be allocated for the backup quota can be calculated as follows:

- Backup Quota = (0.8 x Hard Disk Capacity) – 92GB if the Hard Disk Capacity is greater than 160GB, otherwise zero.
  - The capacities are all approximate. The quoted disk capacity from a disk manufacturer or a virtual server platform will differ from the capacity reported by the operating system.
  - For example, for a 500GB hard disk, the backup quota is approximately 308GB.

Checking the Backup Server's Backup Quota

Once a server is installed, the actual space allocated for backups can be checked as follows:

1. Login to the backup server's web manager menus.
2. Click and select **Platform View**.
3. On the **System** tab, note the **Quota available for backup data** value. Note this is the total space usable for backups, it does not account for the space already used by any existing backups.
4. Click **Solution** to exit the platform view.

Related links

Backup and Restore on page 57

Backup data sets

Each backup can include multiple selected servers. Within that backup a number of different data sets can be selected for inclusion in the backup.

The table summarizes the data included in the different backup data sets. Some data sets are greyed out if the related service is not running on one of the servers included in the backup.

When performing a restore it is also possible to select which servers and which data sets are included in the restore operation.

Data Set	Options	Contents
IP Office Sets	**IP Office Configuration**	When selected for Linux-based IP Office servers: • Server Settings • Web Management Settings • IP Office Service Configuration • IP Office Security Settings • DHCP Allocations • Call logs When selected for IP500 V2 Expansion systems: • IP Office Configuration • IP Office Security Settings • DHCP Allocations • Call logs
one-X Portal Sets	**one-X Portal Configuration**	one-X Portal server settings
Voicemail Pro Set	**Voicemail Pro Configuration**	• Voicemail Pro server preferences • Call flows
	Messages & Recordings	• Voicemail mailbox contents
	Voicemail Pro Full	• Voicemail Pro server preferences • Call flows • Mailbox contents including greetings, announcements and name prompts. Note: This does not include any custom prompts from the Web Manager customer prompts folder. Separate manual copies of those prompts must be kept.
	Selective Voicemail Users	This option backups a group of preselected mailboxes. The mailbox group is specified through **Applications** > **Voicemail pro — System Preferences** > **User Group**|.
WebLM Sets	**WebLM Configuration**	Note that this data set does not include the license file being used by the server. A separate manual copy of any license file uploaded to the system should be retained.
WebRTC Sets	**WebRTC Configuration**	
Media Manager Sets	**Media Manager Configuration**	This is the configuration of the Media Manager service only. It does not include the call recordings and other data stored on the additional hard drive used for Media Manager.

Related links

Backup and Restore on page 57

Creating a remote server connection

Once the backup server has been configured, a remote server connection is required on the server to be backed up. In a network of servers, the remote connection s defined on the primary server.

Procedure

1. In the Web Manager menu bar, click **Solution**.
2. Click **Solution Settings** and select **Remote Server**.
3. Click **Add Remote Server**.
4. Enter a name that identifies the connections use.
5. Set the **Protocol** to either **HTTPS** or **HTTP**.
   - These are the only protocols supported for backup/restore operations.
   - **HTTP** is only supported if the backup server has had HTTP enabled. See Enabling HTTP backup support on page 59.
6. Set the **Port** to match the selected protocol. The default ports are not correct.
   - For **HTTPS**, set the port to 5443.
   - For **HTTP**, set the port to 8000.
7. Set the **Remote Path** to `/avaya/backup`.
8. No **User Name** or **Password** details are required.
9. Click **Save**.
10. The new remote server connection is now shown in the list of remote servers. It can now be selected for backup and restore actions.

Related links

Backup and Restore on page 57

Backing up a server/servers

The system backs up the configuration of the server, application and user data in a single file set. You can use this backup file to restore the server or a failed server upgrade. The system backs up the configuration of the application to a local drive, in a predefined directory. You can take a backup of the primary server on a remote file server, which can optionally be the secondary server.

Before you begin

- Create a remote server connection for the backup server. See Creating a remote server connection on page 63.

About this task

You can take a back up of the primary server on a remote file server using Web Manager:

Procedure

1. In the Web Manager menu bar, click **Solution**.
2. In the Solution page, select the servers that you want to backup.
3. Click **Actions** and select **Backup**.
4. Select which data sets you want to include in the backup. See Backup data sets on page 61 for details of the different sets contents.
5. In the **Backup Label** field, type a label for the backup.
6. In **Select Remote Server** drop down list, select the remote server that you have set.
7.
8. To back up at a scheduled time:
    a. In **Select Remote Server** drop down list, select the remote server that you have set.
    b. Under **Schedule Options**, enable **Use Schedule**.
    c. In the **Select Schedule** list, select the schedule option that you created.
    d. Set a **Start Date** and a **Start Time**.
    e. To configure a recurring backup, set **Recurring Schedule** to **Yes** and then set the **Frequency** and **Day of Week**.
9. Click **OK**.
10. The progress of the backup process is shown on the **Solution** menu.

Related links

Backup and Restore on page 57

Restoring from the backup server

The following process is used to restore previously backed up data.

Warning:

- Backup/restore is not supported between different server software release levels. Any exceptions are specifically documented in software release notes and migration documents.
- You cannot restore data to a server unless either the IP Address or the system id (LAN1 MAC address) match the server from which it was backed up.

- Close any Voicemail Pro client before attempting a restore. The restore process requires the voicemail service to restart. That will not occur if the Voicemail Pro client is connected to the service and will lead to incorrect restoration of data.
- During the restore process, the services being restored are restarted. This will end any calls using those services.

Procedure

1. In the Web Manager menu bar, click **Solution**.
2. Select the servers onto which you want to restore data sets.
3. Click **Actions** and select **Restore**.
4. Select the **Remote Server** connection that points to the backup server.
5. Click **Get Restore Points**.
6. The system displays the backup data sets that it has for the selected servers.
7. Highlight the data sets that you want to restore.
8. Click **OK**.
9. The progress of the backup process is shown on the **Solution** menu.

Related links

Backup and Restore on page 57

Restoring a failed server

The backup data can be used to attempt to restore a server that has failed.

Procedure

1. Reinstall the original server software, ensuring that the same original IP address and host name settings are used.
2. Reignite the server back to its original role. If the server includes an additional hard drive containing call recordings for Media Manager, ensure that the option to reformat the additional drive is not selected during the server ignition.
3. Login to the server and complete its initial configuration.
4. If the server was part of a network, use the options within Manager to add it back into the network and ensure that the connections between the primary, secondary and expansions are all present.
5. At this stage, use the restore process (see Restoring from the backup server on page 64) to reload the original data.

Related links

Backup and Restore on page 57

Chapter 10: Configuring the IP Office Server Edition Solution

Administration tools

After you have provisioned all the required components in an IP Office Server Edition Solution, use IP Office Manager and IP Office Web Manager to configure additional settings. Refer to

- *Administering Avaya IP Office™ Platform with Manager*
- *Administering Avaya IP Office™ Platform with Web Manager*

Warning:

Only use CLI commands only if you are Avaya support personnel. You must not install any third party applications on IP Office Server Edition components.

Setting a login warning banner

When a user logs in to IP Office Server Edition you can set a warning banner. A warning banner displays the terms and conditions to use IP Office Server Edition.

Procedure

1. Log in to Web Manager.
2. On the Solution page, for the system where you want to set a login banner, select **Server Menu** > **Platform View**.
3. Select **Settings** > **General**.
4. In the **Set Login Banner** section, type the warning message in the text area.
5. Click **Save**.

Result

The system displays the warning banner in the login page when you log in to IP Office Server Edition next time.

Managing Passwords

Changing the Administrator password using Web Manager

Before you begin

Login as *Administrator* into Web Manager

About this task

You can administer all the systems configured in IP Office Server Edition Solution using Web Manager . The components that you can administer are the Server Edition Primary, Server Edition Secondary, and Server Edition Expansion System (L).

To change the Web Manager *Administrator* password:

Procedure

1. Click **Tools**.

   The system displays the Services window.

2. Click **Preferences** .

   The system displays the Preferences dialog.

3. Type the new password in the **Password** field.

4. Retype the new password in the **Confirm Password** field.

   Note:

   Ensure that the password that you set conforms to the requirements listed in **Password complexity requirements** under **Platform** > **Settings** > **System**.

   For more information, see the *Security Mode* section of the *IP Office Manager* document.

5. Click **Save**.

Result

The system changes the password and displays the status of the password change.

Changing the Administrator password using Linux Platform settings

Procedure

1. On a client computer, start the browser and type `https://` *<IP address of the Server> :<port number>*.

The default port number is *7071*. You can change the port number after logging in as *Administrator*. To change the port number select **Settings** >**General**.

2. In the IP Office Server Edition logon page, click **Change password**.
3. Type the current password of the *Administrator* in the **Old Password** field.
4. Type the new password of the *Administrator* in the **New Password** field.

   Note:

   Ensure that the password that you set conforms to the requirements listed under **Password complexity requirements**.

   You can configure the password complexity rules for IP Office *Administrator* account using IP Office Server Edition Manager. For more information, see the *Security Mode* section of the *IP Office Manager* document.
5. Retype the new password of the *Administrator* in the **Confirm Password** field.
6. Click **Ok**.

Next steps

After you change the common configuration Administrator password for the servers using IP Office Server Edition Manager you must also update the same password for *Administrator* account of the Server Edition Primary and Server Edition Secondary servers using Web Manager.

Changing the root user password

Before you begin

In IP Office Web Manager, navigate to the Linux Platform Settings.

About this task

You can change the password of the *root user* for a Linux server using Linux Platform settings.

Procedure

1. Select **Settings** >**System**.
2. Type the new password in the **New Password** field of the **Change Root Password** section.

   Note:

   Ensure that the password that you set conforms to the requirements listed under **Password complexity requirements**.
3. Retype the password in the **Confirm New Password** field.
4. Click **Save**.

Changing the Security Administrator password for Server Edition server

Before you begin

Start IP Office Server Edition Manager.

About this task

You can administer all the components of IP Office Server Edition Solution using IP Office Server Edition Manager.

Note:

You must change the password of each IP Office Server Edition servers separately.

To change the password:

Procedure

1. Select **File** >**Advanced** > **Security Settings**.
2. In the Select IP Office window select the server for which you want to change the *Security Administrator* password.
3. Click **OK**.
4. Type the name of the *Security Administrator* in **Service User Name** field.
5. Type the password of the *Security Administrator* in **Service User Password** field.

   The default user name is *security* and password is *securitypwd*.
6. Select **General** in the navigation pane.
7. In the **Security Administrator** section, click **Change**.
8. Type the current password of the *Security Administrator* in the **Old Password** field.
9. Type the new password of the *Security Administrator* in the **New Password** field.
10. Retype the new password in the **Re-Enter Password** field.
11. Click **OK**.

    For more information on using IP Office Server Edition Manager, see the *IP Office Manager* document.

Changing the passwords of common configuration Administrator

Before you begin

Note:

Always use Web Manager to change the passwords of common configuration *Administrator*. Use this procedure only if you are not able to access Web Manager.

- Start IP Office Server Edition Manager.
- You must have the user name and password for each of the systems in IP Office Server Edition Solution to access the security configuration.

About this task

You can create a common user name and password for the multiple systems in IP Office Server Edition Solution to obtain access to the system configurations using IP Office Server EditionManager:

Procedure

1. Select **Tools** > **Server Edition Service User Management**.
2. In the **Select IP Office** window, select the systems for which you want to create a common configuration account.
3. Click **OK**.
4. Type the user name and password to access the security configuration of each of the system that you have selected.

   To use the same user name and password for the selected systems, select **Use above credentials for all remaining, selected IPOs**. The user name is *security* and password is *securitypwd*. You must change the default password later to ensure that the system is secure.

   To use different user name and password for each of the selected systems, clear **Use above credentials for all remaining, selected IPOs**.
5. The system displays the list of all the systems in IP Office Server Edition Solution and an indication if they already have an **Service User Status** account.
6. To change the password, click **Change Password**.
7. Click **Update Password**.
8. Type the common password in the **New User Password** field.
9. Retype the password in the **Re-enter New User Password** field.
10. Click **OK**.
11. Click **Close**.

Next steps

After you change the common configuration Administrator password for the servers using IP Office Server Edition Manager you must also update the same password for *Administrator* account of Server Edition Primary and Server Edition Secondary servers using the Web Manager.

Configuring log files

Viewing the Debug log files

About this task

You can view the log files of the various applications that the IP Office Server Edition supports. To view the log files:

Procedure

1. Log in to Web Manager.
2. On the Solution page, for the system which you want to view log files, select **Server Menu** > **Platform View**.
3. Select **Logs** > **Debug Logs** .

   To view the logs for a specific application, select the application from the **Application** list .

   The system displays the details of the actions performed by *Administrator* users in the **Audit Log** table.

Configuring syslog files

You can configure the server to receive and the forward the syslog records.

Note:

You cannot configure Server Edition Expansion System(L) or the Application Sever to receive and forward the syslog records.

Procedure

1. Log in to Web Manager.
2. On the Solution page, for the system on which you want to configure log files, select **Server Menu** > **Platform View**.
3. Select **Settings** > **General**.

4. In the **Syslog** section do the following:
    a. In **Log files age (days)**, set the number of the days that the server has to retain the log files.

       You can set the age of the log files for **General log files**, **Security log files**, **Audit log files**, **Operational log files** and **Debug log files**. If you select **Apply general settings to all file types** , the system sets the same age for all types of log files.

    b. In **Max log size (MB)**, set the maximum size for each type of log files.

       You can set the maximum size for **General log files**, **Security log files**, **Audit log files**, **Operational log files** and **Debug log files**. If you select **Apply general settings to all file types** , the system sets the same size for all types of log files.

    c. In **Receiver Settings**, select **Enable**.
    d. Set the protocol and the port number that the system should use to receive the syslog records.
    e. Select **Forward Destination 1**.
    f. Set the protocol that the system should use to send the syslog records. Type the address of the server and the port number in **IP Address: Port** field.

       To send the syslog records to a second server, select **Forward Destination 2**.

    g. In **Select Log Sources**, select the type of server reporting that the system should include in the syslog records.

       The different types of reporting that you can include in the syslog records are: Authentication and authorization privileges, Information stored by the Linux audit daemon (auditd), News errors of level critical or higher, and Apache web server access_log and error_log.

5. Click **Save**.

Example

Viewing the syslog records

The system displays the syslog files or records that are received by the server.

Before you begin

Configure the syslog events that the server should receive by performing the procedure Configuring syslog files on page 72.

Procedure

1. Log in to Web Manager.
2. On the Solution page, for the system which you want to view logs, select **Server Menu** > **Platform View**.
3. Select **Logs** > **Syslog Event Viewer** .

You can view the logs that are received by the server based on the **Host**, **Event Type**, **View Last**, and **Tag**.

Result

The system displays the date, name of the host server, type of the event , tag and message of the syslog events in **Syslog Events** table.

Configuring the age of the log files

About this task

The system notifies you regarding the status of the application service or the server in the event of any failure or outage. The system displays the notifications along with time stamps and records them in a log file. You can configure the number of days that these log files need to be retained in the system.

Procedure

1. Log in to Web Manager.
2. On the Solution page, for the system on which you want to configure log files, select **Server Menu** > **Platform View**.
3. Select **Settings** > **General**.
4. In the **Watchdog** section, type the number of days in the **Log files age (days)** field.

   Note:

   The system does not apply the number of days that you set in the **Log files age (days)** field to the log files that are already archived.

Downloading the log files

The system archives the log files of the applications in *.tar.gz* format in the **Debug Files** section.

Procedure

1. Log in to Web Manager.
2. On the Solution page, for the system which you want to download log files, select **Server Menu** > **Platform View**.
3. Select **Logs** > **Download** .

   The system displays the files that you need for debugging in the **Debug Files** section and log files in the **Logs** section.
4. Click the file to download.

Note:

The process for the download and the location to which the system downloads the files depends on the browser that you use to access Linux Platform settings.

On-boarding

On-boarding refers to the configuration of an SSL VPN service in order to enable remote management services to customers, such as fault management, monitoring, and administration. You must use the Web Manager client to configure on-boarding.

For full details on how to configure and administer SSL VPN services, refer to *Deploying Avaya IP Office™ Platform SSL VPN Services*.

The procedure provided below configures IP Office for Avaya support services. Avaya partners can also use an SSL VPN to provide support services. See the chapter “Configuring an Avaya Partner SSL VPN using an SDK” in *Deploying Avaya IP Office™ Platform SSL VPN Services*.

Related links

Configuring an SSL VPN using an on-boarding file on page 75

Configuring an SSL VPN using an on-boarding file

The on-boarding XML file is available from Avaya. It contains the settings required to establish a secure tunnel between IP Office and an AVG server. When you import the on-boarding XML file, it applies the settings and installs one or multiple TLS certificates.

When you configure the SSL VPN service on a new system, you must begin by generating an inventory file of the IP Office system. When you register your IP Office system, the inventory file that you generated is uploaded to the GRT and the inventory data is populated in the Avaya Customer Support (ACS) database. After you enable remote support, you can download the XML on-boarding file from the GRT web site and upload it into your IP Office system.

The on-boarding process configures:

- SSL VPN service configuration
- short codes for enabling and disabling the SSL VPN service
- SNMP alarm traps
- one or more TLS certificates in the IP Office trusted certificate store

Perform this procedure using the Avaya IP Office Web Manager client.

Warning:

The process of 'on-boarding automatically creates an SSL VPN service in the system configuration when the on-boarding file is uploaded to the system. Care should be taken not to delete or modify such a service except when advised to by Avaya.

Before you begin

Before you begin, you must have the hardware codes and catalog description of your IP Office system. For example, “IP OFFICE 500 VERSION 2 CONTROL UNIT TAA” is a hardware code and catalog description.

Procedure

1. Select **Tools > On-boarding**.

   The On-boarding dialog box displays.

2. If the hardware code for your IP Office system ends with the letters TAA, select the checkbox next to the prompt **Are you using TAA series hardware?**
3. Click **Get Inventory File** to generate an inventory of your IP Office system.
4. Click **Register IP Office**.

   A browser opens and navigates to the GRT web site.

5. Log in to the web site and enter the required data for the IP Office system.
6. Select **Remote Support** for the IP Office system.
7. Click **Download** and save the on-boarding file.
8. Browse to the location where you saved the on-boarding file and click **Upload**.

   A message displays to confirm that the on-boarding file has installed successfully.

Related links

On-boarding on page 75

Chapter 11: Configuring Avaya one-X® Portal for IP Office

Configuring Avaya one-X® Portal for IP Office users

To ensure that the users configured in Manager are able to use Avaya one-X® Portal for IP Office you need to configure Avaya one-X® Portal for IP Office. Use this procedure to configure Avaya one-X® Portal for IP Office users

About this task

By default Avaya one-X® Portal for IP Office is installed on the Server Edition Primary server. To support additional users, you can install Avaya one-X® Portal for IP Office as a standalone server. For capacity information, see the *Capacity Planning* document at: https://support.avaya.com/.

Procedure

1. Start Manager.
2. Add the *Office Worker* or *Power User* licenses.
3. Enable Avaya one-X® Portal for IP Office services for the users configured in IP Office Server Edition.

   For more details on enabling Avaya one-X® Portal for IP Office services for the users, see *Administering Avaya IP Office™ Platform with Manager*.

Configuring IP Office Server Edition systems in Avaya one-X® Portal for IP Office

To ensure that the all users can use the services of Avaya one-X® Portal you need to configure all the Server Edition Expansion Systems and Server Edition Secondaryof the IP Office Server Edition Solution in Avaya one-X® Portal for IP Office server.

Before you begin

Install and configure the server as an Server Edition Expansion System in the ignition process.

About this task

To configure the Server Edition Expansion System in Avaya one-X® Portal for IP Office server.

Procedure

1. Login as *Administrator*.
2. In the left panel select **Configuration** > **Providers**
3. Configure the details of the Server Edition Expansion System as Telephony (CSTA) provider and Directory (IP Office) provider.

   For more information about how to configure the details of the Server Edition Expansion System as Telephony (CSTA) provider and Directory (IP Office) provider, see the *Administration* section of the *Implementing Server Edition Expansion System* document.

Configuring administration access for Avaya one-X® Portal for IP Office

Note:

The system does not prompt you to change the password when you start Avaya one-X® Portal for IP Office using Web Manager because Web Manager provides unified password management for all applications including Avaya one-X® Portal for IP Office.

Before you begin

Install and configure a server as Avaya one-X® Portal for IP Office in the ignition process.

About this task

To configure the administration access for Avaya one-X® Portal for IP Office:

Procedure

1. On a client computer, start the browser and type *https://<IP address of IP Office Server Edition>:9443/onexportal-admin.html*.
2. Login as *Administrator*. The default user name is *Administrator* and the password is *Administrator*.

   To ensure that your system is secure always change the default password.
3. Set the initial configuration of Install and configure a server as Avaya one-X® Portal for IP Office in the ignition process.

   For details about setting the initial configuration, see the *Implementing Avaya one-X® Portal for IP Office* document.

   After you set the initial configuration the system prompts you to change the *Administrator* password.
4. Type the new password in the **New Password** field of the Administrator Default Password Check dialog box
5. Retype the password in the **New Password (Typed Again)** field. n

6. Click **Change Password**.

Next steps

Initialize the AFA login.

Administering a separate Avaya one-X® Portal for IP Office

You can administer a separate Avaya one-X® Portal for IP Office on Server Edition Primary server using Linux Platform settings:

Before you begin

- Start Linux Platform settings.
- Take a backup of the existing user data.

Procedure

1. In the **Settings** tab select **General**.
2. In the **one-X Portal Settings** section clear **Use Local IP**.
3. Select **System** > **Services**.
4. Click **Stop** to stop the services of Avaya one-X® Portal for IP Officeon Server Edition Primaryserver.
5. Clear **Auto Start** for Avaya one-X® Portal for IP Office on Server Edition Primary server.

   The system disables Avaya one-X® Portal for IP Office on Server Edition Primary server.
6. Go to **Settings** > **General**.
7. In the **one-X Portal Settings** section, type the IP address of the separate Avaya one-X® Portalin the **Remote IP** field.
8. Click **Save**.
9. In the **Home** tab click **one-X Portal Administration**.

Result

The system launches the Avaya one-X® Portal for IP Office administration login page in the browser.

Next steps

Restore the user data in the separate Avaya one-X® Portal for IP Office.

Chapter 12: Configuring Voicemail Pro

Configuring Voicemail Pro

The Voicemail Pro application provides the mailbox services for all users and hunt groups created in the IP Office configuration. In a setup where there is a single IP Office and Voicemail Pro server you need not do any configuration. This section describes only the minimum steps that Avaya recommends to ensure that the Voicemail Pro server operates correctly and is secure.

For more details about IP Office and Voicemail Pro configuration, such as enabling TTS, or enabling exchange integration, see the *Implementing Voicemail Pro* and *Administering Voicemail Pro* manuals.

About this task

Add theVoicemail Pro licenses in IP Office Server Edition Manager.

Note:

A single instance of IP Office Server Edition provides only two Voicemail Pro channels. The number of Voicemail Pro channels that the system displays depends on the number of instances of IP Office Server Edition. If you have licenses for any additional channels, you must add those licenses as well.

In a resilience setup, when Server Edition Primary is not active, the system displays a voicemail failure message even though Voicemail Pro is working . The system displays a voicemail failure message for the Voicemail Pro on Server Edition Primary that is not active.

Installing Voicemail Pro client

Before you begin

1. Start Web Manager.
2. Login as an *Administrator*.
3. Start Linux Platform settings.

About this task

Note:

If you have not installed the latest version of Voicemail Pro client, the system prompts you to install the latest version when you start Voicemail Pro using Web Manager.

To download the latest version of Voicemail Pro client using Linux Platform settings:

Procedure

1. Click **AppCenter** tab.
2. In the **Download Applications** section, click the .exe file link for Voicemail Pro client.
3. Download the .exe file and run the .exe file to install Voicemail Pro client.

Next steps

Login to Voicemail Pro server using Voicemail Pro client.

Logging into Voicemail Pro server

Before you begin

To log into a Voicemail Pro server you should configure an *Administrator* user name and password on theVoicemail Pro server. The default user name for Voicemail Pro server is *Administrator* and the password is *Administrator*.

Note:

To ensure that the system is secure you must always change the default password.

About this task

To log into Voicemail Pro server using Voicemail Pro client, do the following:

Procedure

1. Click **Start**.
2. Select **Program** >**IP Office** > **Voicemail Pro Client**.

   The system displays Select Voicemail Pro Client Mode window. If you started the client before, the system attempts to start in the same mode that you used earlier. If you start the client for the first time, the system displays the Select Voicemail Pro Client Mode dialog box.
3. Select **Online**.

   The system displays VmPro Login dialog box.
4. Type *Administrator* in the **User Name** field.
5. Type the pass word in the **User Password** field.

   The default password is *Administrator*.
6. Type the IP address of the voicemail server in the **Unit Name \ IP Address** field.

   You can also click **Browse** to search for Voicemail Pro server in the local network.
7. Click **Login**.

Note:

After three unsuccessful attempts to login as an *Administrator* the system locks the *Administrator* account for an hour.

Next steps

Change the default password for Voicemail Pro *Administrator* account.

1. In the Voicemail Pro client, select **File** > **Change Password**.
2. Type the new password in the **New Password** and **Verify New Password** fields.
3. Click **OK**.

Backing up and restoring voicemail

Backing up Voicemail Pro

You can take a backup of voicemail, user settings & greetings, call flows, modules and conditions, module recordings, campaigns, and system settings on a local drive. You can take backup once everyday, every week or every month.

Note:

To perform a backup and restore always use Web Manager. For more information, see Backing up and restoring the server on page 63 . If you use Voicemail Pro to backup and restore, the system does not provide the integrations.

About this task

To take a backup of the voicemail server do the following:

Procedure

1. Launch Voicemail Pro client.
2. Log in as *Administrator*.
3. Select **Administration** > **Preferences** > **General**.
4. Click the **Housekeeping** tab.
5. Click **Backup Now**.

   The system displays the various backup options. For more information on the backup settings, see the *Administering Voicemail Pro* document.
6. Click **OK** to start backup.

Restoring Voicemail Pro stored on IP Office Server Edition server

You can restore the voicemails, user settings & greetings, call flows, modules and conditions, module recordings, campaigns, and system settings that were backed up on a local drive.

Note:

Use this procedure to restore voicemail backups for the Release 8.0, 8.1 and 8.1 FP1. To restore the voicemail backup of Release 9.0 always use Web Manager. For more information, see Restoring IP Office Server Edition server. on page 84

Before you begin

- Ensure that you shutdown all the services on the server.
- Start Linux Platform settings.
- Login as *Administrator*.

Ensure that you shutdown all the services on the server.

About this task

To restore a backup file that is stored on IP Office Server Edition server:

Procedure

1. Select **Settings** > **General**.
2. Select **Restore** in the **Backup and Restore**.

   Note:

   You can only restore the backup files for the voicemail using Linux Platform settings. You can restore a complete backup data set. You cannot select a particular item that needs to be restored.

Result

The system displays a list of backup files, select the backup file you want to restore.

Migrating Voicemail Pro to IP Office Server Edition

Related links

Backing up an existing Voicemail Pro server on page 83
Restoring Voicemail Pro not stored on IP Office Server Edition server on page 84
Backup and restore limitations on page 85

Backing up an existing Voicemail Pro server

When you replace an existing Voicemail Pro server with IP Office Server Edition server you must take a backup of all the settings, prompts and messages from the existing server. If the existing server is a Linux based server, you must use SSH file transfer to retrieve the backup files from the

server. If the existing server is a Windows based server you copy the backup files on a folder in the server and then use the SSH file transfer to migrate the back up files to IP Office Server Edition server.

About this task

To take backup of an existing Voicemail Pro server:

Procedure

1. Log in to Voicemail Pro server using Voicemail Pro client.

   You can use the **File**> **Voicemail Shutdown** > **Suspend Calls** to display the number of voicemail sessions that are active. You can stop any new sessions or end the sessions before to take a backup.
2. Select **Preferences** >**General**.
3. Click the **Housekeeping** tab.
4. Select **Backup Now**.
5. Select all the backup options for a complete backup and click **OK**.

   The time take to complete a backup varies depending on the number of mailboxes and messages that Voicemail Pro server supports.

   The system creates a backup of folder. The name of the folder includes the date and time of the backup and Immediate. For example, *VMPro_Backup_26012011124108_Immediate*.

Next steps

Shutdown the voicemail server:

1. Select **File**>**Voicemail Shutdown** > **Shutdown**.
2. Select **Shut Down Immediately**.

Related links

Migrating Voicemail Pro to IP Office Server Edition on page 83

Restoring Voicemail Pro not stored on IP Office Server Edition server

Before you begin

Ensure that you shutdown all the services on the server.

About this task

To restore a backup file that is not stored on IP Office Server Editionserver:

Procedure

1. Connect to IP Office Server Edition using an SSH File transfer tool.
   a. Type the IP address of IP Office Server Edition server in the **Host Name** field.
   b. Type the **User Name** as `Administrator`.
   c. Set the **Protocol** as **SFTP/SSH**.

d. Set the **Port** as **22**.

When you connect to IP Office Server Edition using an SSH File transfer tool for the first time the system prompts you to accept the trusted key. Accept the trusted key.

e. Type the password for the *Administrator*. The default password for the *Administrator* is `Administrator`.

2. Copy the backup folder in the `/opt/vmpro/Backup/Scheduled/OtherBackups`.
3. Login as an Administrator into IP Office Server Edition using the Web Control Panel.
4. Select **Settings** > **General**.
5. Select **Restore** in the **Backup and Restore**.

Note:

You can only restore the backup files for the voicemail using the Web Control Panel. You can restore a complete backup data set. You cannot select a particular item that needs to be restored.

Result

The system displays a list of backup files, select the backup file you want to restore.

Related links

Migrating Voicemail Pro to IP Office Server Edition on page 83

Backup and restore limitations

If you have created extra folders on the Voicemail Pro server, in IP Office Server Edition server these folders are not included in the restore process. Instead the extra folders need to be copied manually. For example, if you created a folder containing custom prompts for use in call flows in addition to the default language folders used for prompts, then the system does not backup or restore the custom folder. To resolve this, the extra folders must be backed up and restored manually. In the following example, a folder *Custom* is manual copied from an existing server to create a backup. It is then manually restored.

Before you begin

Using SSH file transfer tool copy the folder *Custom* from `/opt/vmpro` in the old server to your computer to create a backup of the folder.

About this task

To restore the *Custom* folder, using an SSH file transfer tool, copy the folder to the `/home/Administrator` folder on the IP Office Server Edition server:

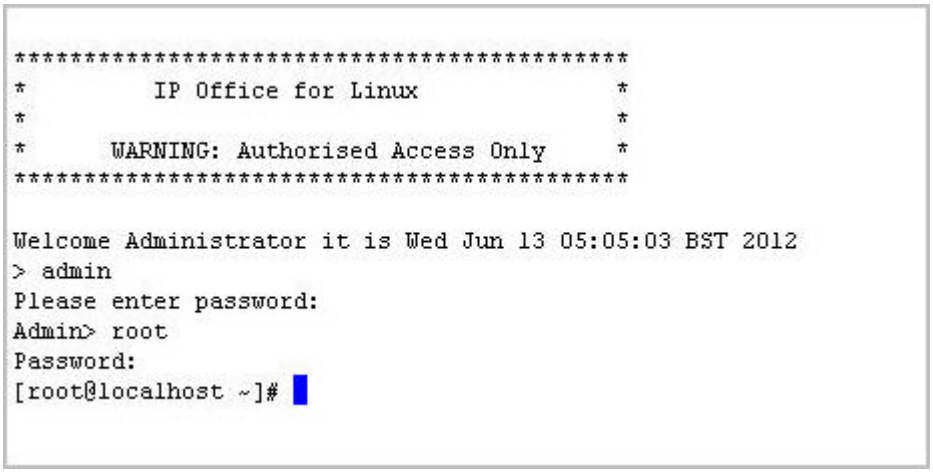
Procedure

1. Login to the command line interface of the system using the root user password. You can log in directly on the IP Office Server Edition server or remotely using an SSH File transfer tool.
   - Log in directly to the IP Office Server Edition server:
     a. At the `Command:` prompt, type `login`
     b. At the `login:` prompt, type `Administrator`
     c. At the `Password:` prompt, type the default password `Administrator`
   - Log in as `Administrator` using the SSH file transfer tool.

     . The default password is `Administrator`
2. In a new terminal window at the command prompt, type `admin`

   The system prompts for a password. The default password is `Administrator`
3. At the `Admin >` prompt, type `root`
4. Type the `root` password. The default password is `Administrator`

   The system displays the root user prompt. For example, `root@<name of the server>`



5. Type `cd /home/Administrator`
6. Type `mv Custom /opt/vmpro`

Next steps

Using the SSH file transfer tool, verify that the *Custom* folder has been copied to `/opt/vmpro`

Related links

Migrating Voicemail Pro to IP Office Server Edition on page 83

Chapter 13: Shutting down a system

Shutting down a Server Edition Expansion System (V2) using IP Office Manager

You can shut down a Server Edition Expansion System (V2) using the IP Office Server Edition Manager.

About this task

Warning:

- Do not remove the power cords or turn off the power input to the system to shut down the system.
- All user calls and services that are in progress stop. After you shut down, you cannot use the system to make or receive any calls until you restart the system.
- To restart a system after you shut down indefinitely, or to restart a system before the timed restart, turn on the power supply to the system again.

Procedure

1. Select **File** > **Advanced** > **System Shutdown**.
2. In the **Select IP Office** window, select the system that you want to shutdown.
3. In the **System Shutdown Mode** dialog box:
   - Select **Indefinite**, to shut down the system for an indefinite time.
   - Select **Timed** and set the time to restart after the system is shut down.

   If you shut down the system for an indefinite time, you must turn off the power to the system and then turn on the power supply gain to restart the system.
4. Click **OK**.

Shutting Down a Linux Server Using Web Manager

To ensure that the system saves the configuration file always shut down the system using Web Manager.

Procedure

1. Log in to Web Manager
2. On the Solution page, click the Server Menu icon to the right of the server you want to shut down.
3. Select **Platform View** and then **System**.
4. Under **System**, click **Shutdown**.

Shutting down a Linux server using Linux Platform settings

About this task

To shut down a server using Linux Platform settings:

Procedure

1. On a client computer, start the browser and type `https://` *<IP address of the server> :<port number>*.
2. Log on as *Administrator*.
3. In the **System** section of the **Home** page, click **Shutdown**.
4. In the **Warning** dialog box, click **Yes** to confirm that you want to shut down the system.

   The system displays the login page. Do not log in again because the system is in the process of stopping the services.
5. After the server is shut down you can turn off the power to the server.

Chapter 14: Changing the IP Address of a Server Edition Server

Use these procedures to change the major IP address of a Server Edition Server. The major IP address is the address used to manage the Server Edition Primary server, typically LAN1.

Related links

[Changing the IP Address of the Primary Server](#) on page 89
[Changing the IP Address of a Secondary or Expansion Server](#) on page 90

Changing the IP Address of the Primary Server

Procedure

1. Use IP Office Manager to run the Initial Configuration Utility (ICU) on each Server Edition Secondary and Server Edition Expansion System.

   When running the ICU, ensure the **Retain Existing Configuration** setting is checked.

   a. Enter the new Server Edition Primary server IP address/Netmask. This may require a different Gateway IP Route.

   b. Save the configuration to the system. This results in the system going offline from the Server Edition Primary server and Manager.

   c. Once the ICU has been run on each system, close Manager.

2. Use IP Office Web Managerto log in to the Server Edition Primary server and change the IP address.

   a. Select **System Settings** > **System**

   b. On the System screen, click **View AutoPrimary** located at the right.

   c. Change the IP address as required and click **Update**.

3. Restart the Server Edition Primary server.
4. Use Manager to log in to the Server Edition Primary server and check that all the IP Office systems are online.
5. Review and test the configuration.
6. Perform a backup.

Related links

Changing the IP Address of a Server Edition Server on page 89

Changing the IP Address of a Secondary or Expansion Server

Procedure

1. Use IP Office Manager to run the Initial Configuration Utility (ICU) on the Server Edition Secondary or Server Edition Expansion System.

   When running the ICU, ensure the **Retain Existing Configuration** setting is checked.
2. Change the IP address.
3. Save the configuration to the system. This results in the system going offline from the Server Edition Primary server and Manager.
4. Log in to the Server Edition Primary server and remove the Server Edition Secondary or Server Edition Expansion System from the solution.
5. Run the ICU and add the Server Edition Secondary or Server Edition Expansion System to the solution.

   If requested, use the consolidate from Primary (Replace option).
6. Launch one-X Portal administration and configure the DSML and CSTA providers with the new IP address. The one-X Portal service may require a restart.
7. Review and test the configuration.
8. Perform a backup.

Related links

Changing the IP Address of a Server Edition Server on page 89

Chapter 15: Replacing the hardware of IP Office Server Edition

Replacing IP500 V2 system

At all times follow the relevant safety and static handling procedures. For further information see, *Warnings* section of *Deploying Avaya IP Office™ Platform IP500/IP500 V2*.

Before you begin

Take an SD card backup using either Manager, SSA or system phone. Do not take a backup of the current configuration or the SD card if it is suspicious.

Procedure

1. Shutdown system using Manager, SSA or system phone.
2. Remove the SD card.
3. Replace system hardware and swap all expansion modules, units and cables with similar kind.
4. Insert SD card.
5. Power on of the system with local connectivity only.
6. Check status using the locally attached IP Office Manager and SSA.
7. Reconnect to the network.
8. Check the configuration using IP Office Manager and Web Manager.

   A restore is not required since all necessary data is on the SD card. Licenses remain valid.

Replacing System SD Card

At all times follow the relevant safety and static handling procedures. For further information see, *Warnings* section of *Deploying Avaya IP Office™ Platform IP500/IP500 V2*.

Before you begin

The replacement SD card should be of same type for example, A-Law, U-Law and firmware version with no configuration data. Use the *Recreate IP Office SD Card* feature to load the correct firmware.

Procedure

1. Shutdown the SD card using IP Office Manager, SSA or system phone.

   You do not need to shutdown the system.
2. Remove SD card.
3. Insert replacement SD card in System SD slot and wait for System SD LED to be constant green.

   The systems save internal flash copy of configuration, security settings, DHCP and call log to the SD card.

   Note:

   Any local licenses will fail in 2-4 hours if not failed already. All Server Edition central licenses remain valid.
4. Using IP Office Manager, administer new local licenses and delete old.
5. Validate status and configuration with IP Office Manager, Web Manager, , and SSA.
6. Take a backup using Web Manager and an SD card backup using IP Office Manager, SSA or system phone.

   The SD card backup provides a local copy, and resilience to a multiple reboot scenario.

Replacing an IP 500 V2 Field Replacable Unit

Procedure

When another field replaceable IP500 V2 component has failed or Expansion module, Expansion Unit, or cable, replace the defective component according to section “Replacing Hardware” section of *Deploying Avaya IP Office™ Platform IP500/IP500 V2*.

Replacing a Linux server

At all times follow the relevant safety and static handling procedures. For further information see document IP Office Installation guide of the Avaya Common Server installation guides.

Before you begin

- At all times follow the relevant safety and static handling procedures.

- The HP DL360/Dell R620 hard drives and power supplies are hot swap. There is no need for chassis replacement. These items should be replaced while the system is running. For further information see document IP Office Installation guide of the Avaya Common Server installation guides.
- If viable and appropriate, take server backup using Web Manager. Take a backup of all components, all data sets, and to a remote server. Note any parameters required for the new server's ignition process
- If not down already, shut down the server using Web Manager, then power off.
- Ensure any resilient switch over of phones, hunt groups, VMPro has taken place. There is currently no force fail-over command.
- Remove and replace chassis with same variant. You can replace:
  - an HP DL120 with a Dell R210
  - an HP DL360 with a Dell R620

About this task

Use this procedure to replace all Avaya-supplied Linux servers. The procedure may differ for non-Avaya supplied, but you can use the procedure as the basis for replacement:

Procedure

1. Power on the system with local connectivity only
2. Upgrade to the latest version of IP Office Server Edition Solution using Web Manager DVD, or USB.
3. Configure the server using the ignition process, using the same settings as the original ignition.
4. Configure the server using IP Office Manager Initial Configuration Utility (ICU) to provide management connectivity and valid IP address. Use the same settings as the original ICU.
5. Using Web Manager, on the Server Edition Primary server, run node restore with override for new ID .

   The system restores all configuration and data saved in the original backup except security settings. If this is an Application Server that is not a part of Server Edition, use Web Manager to restore.
6. Reconsitute the security settings as these will be default.
   - If the system is supported through IPOSS and SSL VPN, see Restoring SSLVPN/ IPOSS on page 94
   - If you are replacing a Server Edition Primary server, set all the non-default security settings using IP Office Manager.
   - If you are replacing a Server Edition Secondary server, a Server Edition Expansion System, or an Application Server, use the **Synchronize Security** feature of Web Manager.
7. Validate status and configuration with Web Manager, Manager, and SSA.

8. Perform a backup using Web Manager.
9. Using IP Office Manager, administer new local licenses and delete old.

   Any local licenses will become invalid after 30 days. An offline license swap-out exists.

Restoring SSLVPN or IPOSS

About this task

Any system that has been registered for IP Office Support Services (IPOSS - also known as SSLVPN), retains various information within the configuration and security settings.

Procedure

To restore either the secutity settings or configuration data do one of the following:

- If the onboarding.xml file is available, import the original onborading.xml using Web Manager.
- If the onboarding.xml file is not available but the configuration data is available, restore the configuration and add the certificate at Appendix A: Certificate Text on page 106 to IP Office's Trusted Certificate Store using IP Office Manager. The certificate expires in 2020.

Chapter 16: Troubleshooting

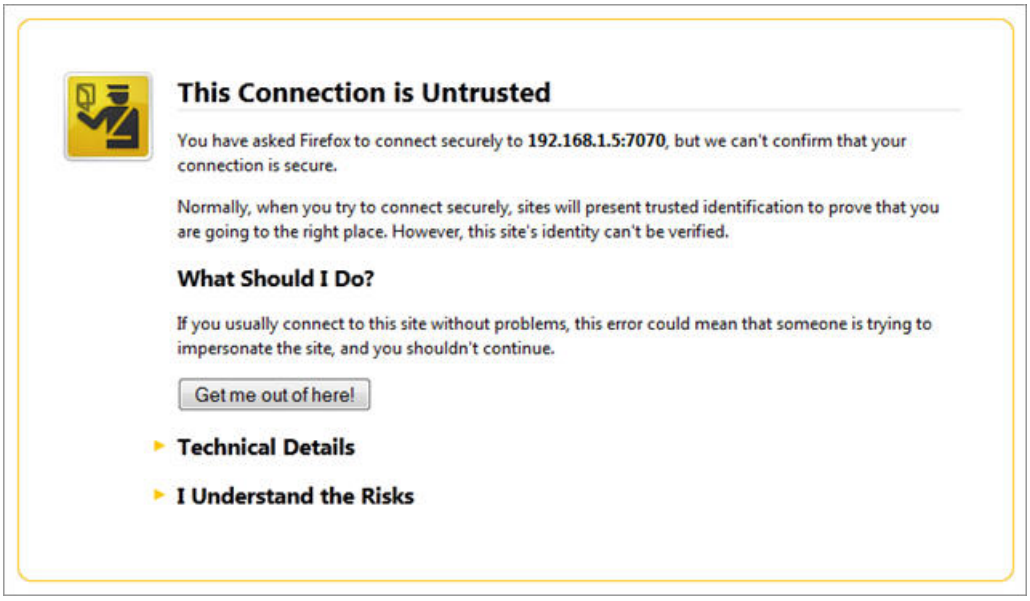
Warning message

When you open a web browser and type `https://<IP address of Server Edition server>:<port number>`, the system displays the following warning message:

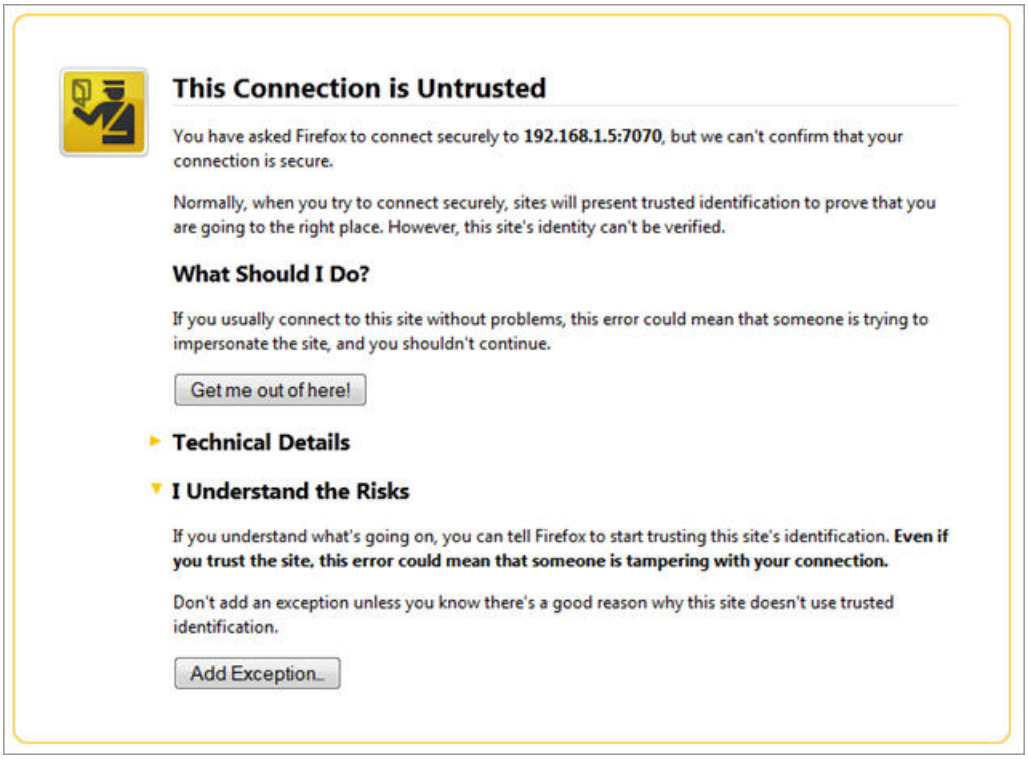
`This Connection is Untrusted`

Note:

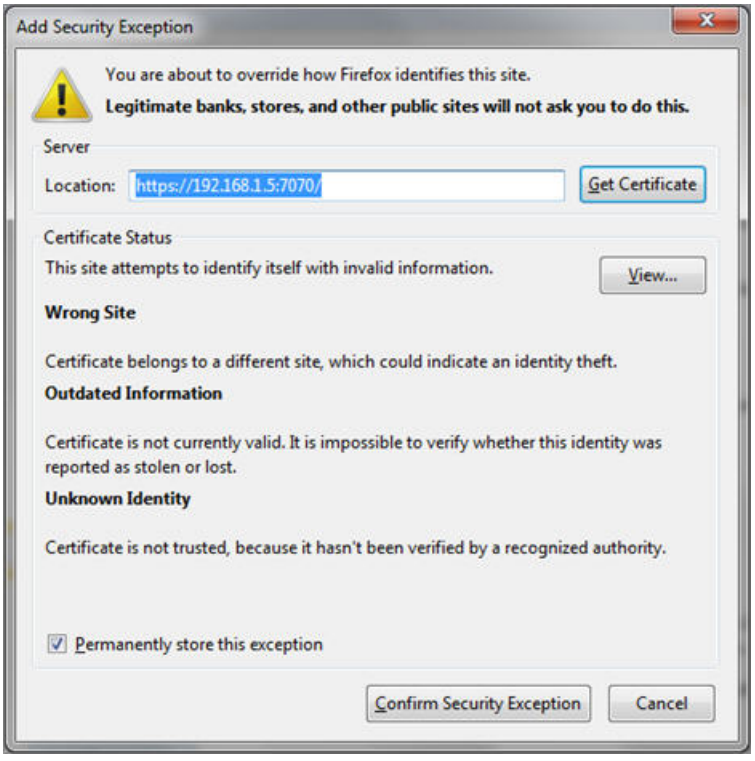
These are the images that the system displays when you open a Firefox browser.



1. Click **I Understand the Risks**.



2. Click **Add Exception**.



3. Click **Confirm Security Exception**.

.

The system displays IP Office Server Edition login page.

Unable to login. IP Office is under Server Edition Manager Administration.

When you attempt to configure an IP Office Server Edition system that is managed by an IP Office Server Edition Manager using the IP Office Standard Manager, the system displays an error message:

```
Unable to login. IP Office is under Server Edition Manager
Administration
```

1. Go to **File** >**Advanced** > **Security Settings**.
2. Select the IP Office Server Edition system, in the Select IP Office window.
3. Click **OK**.
4. Type the name of the *Security Administrator* in the **Service User Name** field.
5. Type the name of the *Security Administrator* in the **Service User Password** field.

   The default user name is *security* and password is *securitypwd*.
6. Select **Services** in the navigation pane.
7. In the Service: Configuration section, set the **Service Access Source** field as *Unrestricted*.
8. Click **OK**.
9. Select **File** > **Save Security Settings**.

   The system unlocks the access for the *Administrator*.
10. Open the configuration and log in as *Administrator*.

Resetting the security settings if all passwords are lost

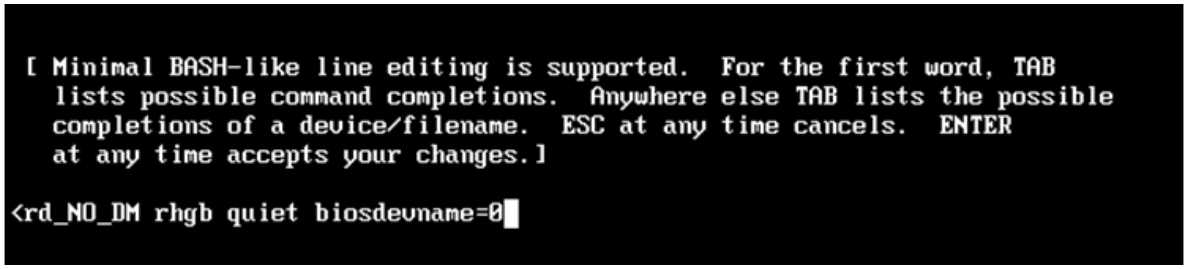
This procedure is applicable on the following environments:

- Physical Server Edition systems
- OVA – virtualized environment
- Cloud environment
- UCM
- Physical or virtualized Application Server

Procedure

1. Attach a monitor and keyboard to the system.
2. Reboot the system.
3. While the system is rebooting, press any key to display the grub menu.
4. Press “e” to edit the commands before booting.
5. Use the arrow keys to select the **kernel** line and press “e” to edit the selected command in the boot sequence.
6. Edit the kernel line.

   The following screen shows the default line.



7. Modify the line by erasing `quiet` and adding `init=/bin/bash`.

8. Press Enter to display a command line prompt.
9. Enter `mount -o remount,rw /`
10. Enter `mount -o remount,rw /proc`
11. Enter `passwd` and then change the root password.
12. Enter `sync`.
13. Enter `umount /`.
14. Enter `umount /proc`.
15. Use the server power button to reboot the machine.
16. Log in using the new root password.
17. Open a console window and log in as root.
18. Reset the security settings by entering `/usr/bin/dbgclient erasesecurity`.

The Security and Administrator password are reset to the default `securitypwd` and `Administrator` respectively. When you log in through Manager, you are prompted to change the default passwords.

All systems appear online in Linux Platform settings of the primary server, but unable to upload the one or more configurations using the IP Office Server EditionManager.

All systems appear online in the Linux Platform settings of the primary server, but appear offline in theIP Office Server Edition Manager.

Solution**:**

Ensure that there is a bidirectional IP connectivity from IP Office Server EditionManager personal computer to the devices for the TCP ports 50802–50815.

All systems appear online in IP Office Server EditionManager, but appear offline on the Linux Platform settings of the primary server.

All systems appear online in IP Office Server EditionManager but appear offline on the Linux Platform settings of the primary server.

Solution**:**

- Ensure that the password of the *Administrator* account on each of the Server Edition Expansion Systemis same as the *Administrator* password of Server Edition Primary server in Linux Platform settings.
- Ensure that the *Administrator* account on each of the Server Edition Expansion Systemis the member of Administrator rights group.
- Ensure that there is a bidirectional connectivity from Server Edition Primaryserver to Server Edition Expansion Systemand Server Edition Secondary server for the TCP ports 8443 and 9080.

Debugging steps

This sections lists the key steps that you need perform to obtain information.

Warning:

You must run the CLI commands only if you are an Avaya support personnel.

About this task

The key steps are:

Procedure

1. Check and report the status of the application.

   The status of the application such as: running, stopped, stuck in starting, and stopping.

2. Check the usage of memory.

   Check for details such as: the memory that is available on the system and the amount of memory that each application uses.

3. Check for the notifications.

   When you restart an application the system displays the notification.

4. View and download the log files.

   For more information about viewing and downloading the log files, see *Chapter 10* of this guide.

Related links

Logging in as a root user on page 100
Checking memory usage on page 101
Checking the version of Linux OS on page 103

Logging in as a root user

Before you begin

Download and install SSH Secure Shell.

About this task

To login as a root user using SSH Secure Shell.

Procedure

1. Connect to the IP Office Server Edition using an SSH File transfer tool.
   a. Type the IP address of the IP Office Server Edition server in the **Host Name** field.
   b. Type the **User Name** as `Administrator`.
   c. Set the **Protocol** as **SFTP/SSH**.
   d. Set the **Port** as **22**.

      When you connect to the IP Office Server Edition using an SSH File transfer tool for the first time the system prompts you to accept the trusted key. Accept the trusted key.

e. Type the password for the *Administrator*. The default password for the *Administrator* is `Administrator`.

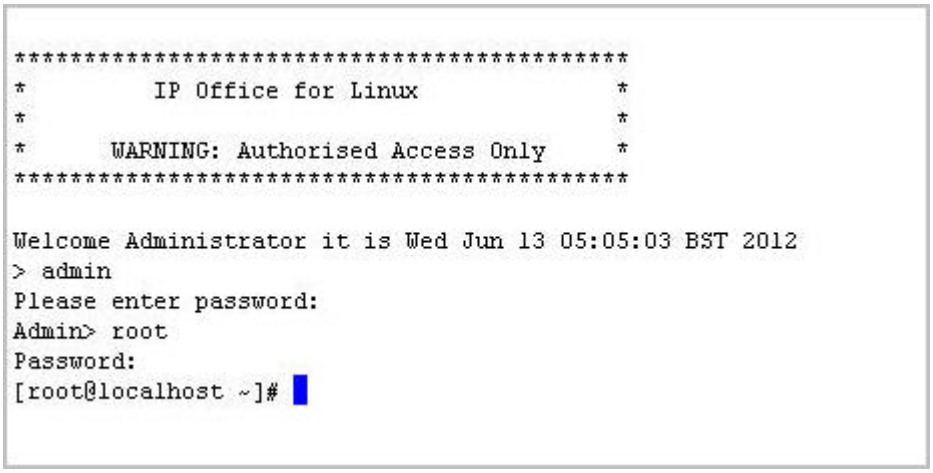
2. In a new terminal window at the command prompt, type `admin`

   The system prompts for a password. The default password is `Administrator`

3. At the `Admin >` prompt, type `root`

4. Type the `root` password. The default password is `Administrator`

   The system displays the root user prompt. For example, `root@<name of the server>`



Related links

Debugging steps on page 99

Checking memory usage

To debug a case you need to check the memory that the system uses.

Note:

You can also check the memory usage in the **Home** page of the Web Control Panel.

Before you begin

Log in as *Administrator* using SSH Secure File Transfer client

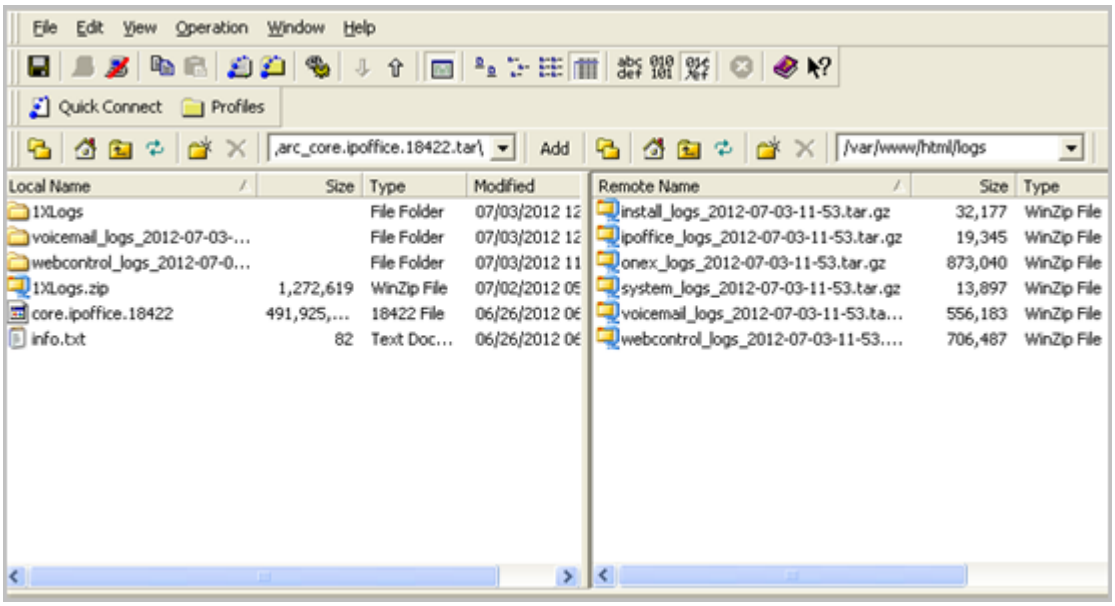
About this task

Procedure

1. Type the path of the system logs folder in the Remote View of the File Transfer window.

   The path is `/var/www/html/logs`.

The system displays the list of all the logs.



2. Move the *system_logs < time and date stamp> tar.gz* file from the Remote View to a location in the Local View of the File Transfer window.
3. In the local computer extract the *system_logs < time and date stamp> tar.gz* file.
4. Go to the `tmp` folder located in the *system_logs < time and date stamp> tar* that you extracted.
5. Open the *avayasyslog.txt* file.

Result

The system displays the details of memory usage in the table that follows the text `+ free`.

```
/dev/sda2:
+ /sbin/hdparm -I '/dev/hd*'
/dev/hd*: No such file or directory
+ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/rootvg-rootvol
                       38G   11G   26G  30% /
tmpfs                1004M     0 1004M   0% /dev/shm
/dev/sda1             512M   38M  449M   8% /boot
+ free
             total       used       free     shared    buffers
cached
Mem:       2055876    1995232      60644          0       6116
128240
-/+ buffers/cache:    1860876     195000
Swap:      1048568     101172     947396
+ ps -eo rss,cmd --sort=rss
  RSS CMD
    0 [kthreadd]
    0 [migration/0]
    0 [ksoftirqd/0]
    0 [migration/0]
```

Related links

Debugging steps on page 99

Checking the version of Linux OS

After you install or upgrade IP Office Server Edition server, you can check the version of Linux OS.

Before you begin

Log in as a root user. For more information see, Logging in as a root user on page 100.

Procedure

At the root prompt, type `cat /etc/redhat-release`

The system displays the version of Linux OS on IP Office Server Edition server.

Related links

Debugging steps on page 99

IP Office Server Edition certificates

IP Office Server Editionserver uses the following X.509 certificates to identify secure web server and administrative interfaces.

Linux Web Control identity certificate

IP Office Server Edition server uses the Linux Web Control identity certificate for:

- Browser access to Web Control.
- Secure Shell access (SSH v2).

IP Office identity certificate

IP Office Server Edition server uses the IP Office identity certificate for:

- Access IP Office Server Edition Manager.
- Browser access to Web Management for on boarding.

Avaya one-X® Portal for IP Office identity certificate

IP Office Server Edition server uses the Avaya one-X® Portal for IP Office identity certificate for:

- Browser access to Avaya one-X® Portal for IP Office when you choose to use HTTPS.

Identity certificates

Certificates are used to provide assurance of identity in a secure environment. Each IP Office component that supports a web server or TLS interface comes with a default identity certificate and a mechanism to change that certificate. For information on certificates, see *Avaya IP Office™ Platform Security Guidelines*.

After failback, the H323 phones do not automatically register back to the original server

IP Office Server Edition Solution provides resilience to some of the functions. When the Primary server is non functional the Secondary server provides resilience and vice versa. The system temporarily logs the users of the H323 phones in to the other server. However, after the original server is functional, the users of the H323 phones remain logged in to the failback server.

Solution

To manually log H323 phone users back into the original server, reset the H323 phones.

If the setting **Phone Failback** is set to **Automatic**, and the phone's primary gatekeeper has been up for more than 10 minutes, the system causes idle phones to perform a failback recovery to the original system. The setting is located at

Manager: System | Telephony | Telephony | Phone Failback

Web Manager: System Settings > **System** > **Telephony** > **Phone Failback**

Unable to export template

After you change the common configuration Administrator password for the servers using the IP Office Server Edition Manager, when you export a template from Server Edition Primary server, Server Edition Secondary, or Server Edition Expansion System (L). The system displays an error message : `HTTP request failed:401 Unauthorized`

Solution

About this task

After you change the common configuration Administrator password for the servers using the IP Office Server Edition Manager you must also update the same password for *Administrator* account of the Server Edition Primary and Server Edition Secondary servers using Web Manager.

Procedure

Change the password for *Administrator* account using Web Manager.

For more information, see Changing the Administrator password on page 68.

Users configured on Server Edition Expansion System are disconnected fromAvaya one-X® Portal for IP Office when the system starts registering SIP phones

When the users configured on Server Edition Expansion System log into Avaya one-X® Portal for IP Office of Server Edition Primary and then start registering the SIP phones on Server Edition Expansion System, the users are disconnected from Avaya one-X® Portal for IP Office.

Possible reasons

This issue appears when there are not enough third party IP Endpoint licences when a SIP extension registers on Server Edition Expansion System, the system logs the user off Avaya one-X® Portal for IP Office. The system also sends a request to Server Edition Primary to obtain the necessary licences. If the system obtains the license, then the system logs in the users, else the users remain logged out.

Work around

Enable **Reserve 3rd Party IP Endpoint licence** check box on the SIP extensions that you plan to register. This ensures that the system obtains licences from Server Edition Primary and the licenses are present in the configuration when SIP extensions register. Alternatively, ensure that there are enough third party IP endpoints licenses on Server Edition Expansion System.

Changing a System Configuration from Select to Non-Select

Condition

A Server Edition Select license has been mistakenly applied to a system or a system has been mistakenly configured as Select.

Remedy

If a Select license was applied to the system in error then it can be removed. In Manager, open the **License | License** page and remove the license.

If the system has been mistakenly configured as a Select system, then you must default the system to change it to non-Select. In Manager, select **File** > **Advanced** > **Erase Configuration (Default)**.

Chapter 17: Appendix A: Certificate Text

Use this certificate when performing the procedure SSLVPN/IPOSS Restoration on page 94.

```
-----BEGIN CERTIFICATE-----
MIIGKTCCBRGgAwIBAgIQZBvoIM4CCBPzLU0tldZ
+ZzANBgkqhkiG9w0BAQUFADCByjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQLE
xZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJpU2lnbiwgSW5jLiAtIEZvciBhdXR
ob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxWZXJpU2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljY
XRpb24gQXV0aG9yaXR5IC0gRzUwHhcNMTAwMjA4MDAwMDAwWhcNMjAwMjA3MjM1OTU5WjCBvDELMAkGA1UEBhMCVVM
xFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQLExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLE
zJUZXJtcyBvZiB1c2UgYXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYykxMDE2MDQGA1UEAxMtVmVyaVN
pZ24gQ2xhc3MgMyBJbnRlcm5hdGlvbmFsIFNlcnZlciBDQSAtIEczMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC
gKCAQEAmdacYvAV9IGaQQhZjxOdF8mfUdzasVLv/+NB3eDfxCjG4615HycQmLi7IJfBKERBD
+qpqFLPTU4bi7u1xHbZzFYG7rNVICreFY1xy1TIbxfNiQDk3P/
hwB9ocenHKS5+vDv85burJlSLZpDN9pK5MSSAvJ5s1fx+0uFLjNxC+kRLX/
gYtS4w9D0SmNNiBXNUppyiHb5SgzoHRsQ7AlYhv/JRT9Cm
mTnprqU/
iZucff5NYAclIPe712mDK4KTQzfZg0EbawurSmaET0qO3n40mY5o1so5BptMs5pITRNGtFghBMT7oE2sLktiEuP7Tf
bJUQABH/weaoEqOOC5T9YtRQIDAQABo4ICFTCCAhEwEgYDVR0TAQH/BAgwBgEB/
wIBADBwBgNVHSAEaTBnMGUGC2CGSAGG
+EUBBxcDMFYwKAYIKwYBBQUHAgEWHGh0dHBzOi8vd3d3LnZlcmlzaWduLmNvbS9jcHMwKgYIKwYBBQUHAgIwHhocaH
R0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYTAOBgNVHQ8BAf8EBAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcw
VRYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQUj
+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVyaXNpZ24uY29tL3ZzbG9nby5naWYwNAYDVR0lBC0
wKwYIKwYBBQUHAwEGCCsGAQUFBwMCBglghkgBhvhCBAEGCmCGSAGG
+EUBCAEwNAYIKwYBBQUHAQEEKDAmMCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC52ZXJpc2lnbi5jb20wNAYDVR0fBC
0wKzApoCegJYYjaHR0cDovL2NybC52ZXJpc2lnbi5jb20vcGNhMy1nNS5jcmwwKAYDVR0RBCEwH6QdMBsxGTAXBgNV
BAMTEFZlcmlTaWduTVBLSS0yLTcwHQYDVR0OBBYEFNebfNgioBX33a1fzimbWMO8RgC1MB8GA1UdIwQYMBaAFH/
TZafC3ey78DAJ80M5+gKvMzEzMA0GCSqGSIb3DQEBBQUAA4IBAQBxtX1zUkrd1000Ky6vlEalSVACT/
gvF3DyE9wfIYaqwk98NzzURniuXXhv0bpavBCrWDbFjGIVRWAXIeLVQqh3oVXY
QwRR9m66SOZdTLdE0z6k1dYzmp8N5tdOlkSVWmzWoxZTDphDzqS4w2Z6BVxiEOgbEtt9LnZQ/9/XaxvMisxx
+rNAVnwzeneUW/ULU/sOX7xo+68q7jA3eRaTJX9NEP9X+79uOzMh3nnchhdZLUNkt6Zmh
+q8lkYZGoaLb9e3SQBb26O/KZru99MzrqP0nkzKXmnUG623kHdq2FlveasB+lXwiiFm5WVu/
XzT3x7rfj8GkPsZC9MGAht4Q5mo
-----END CERTIFICATE-----
```

Chapter 18: Resources

Documentation resources

For a listing of documentation resources related to IP Office, see *Avaya IP Office™ Platform Start Here First*. Download documents from the Avaya Support website at http://support.avaya.com.

IP Office documentation is also available on the IP Office Knowledgebase at http://marketingtools.avaya.com/knowledgebase/.

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

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

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Using the Avaya InSite Knowledge Base

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

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

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

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

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

The system displays the Avaya Support page.

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

Additional IP Office resources

You can find information at the following additional resource websites.

Avaya

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

Avaya Sales & Partner Portal

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

Avaya IP Office Knowledge Base

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

Avaya maintenance, lifecycle and warranty information

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

International Avaya User Group

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

Index

R

S

U

V

W