



IP Office 9.0 Deploying IP Office Server Edition Solution

Release 9.0.3
15-604134
November 2015

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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: <http://support.avaya.com> 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) 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 Avaya's computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed, or remotely accessed on hardware products, and any upgrades, updates, 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.

Licence types

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 an 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 the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use 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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at <http://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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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.

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 Documentation or on Avaya’s website at: <http://support.avaya.com/Copyright> or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Note to Service Provider

The Product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

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: <http://support.avaya.com> or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: <http://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: <http://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

© 2013-2015, Avaya Inc.
All Rights Reserved.

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	9
Purpose.....	9
Intended audience.....	9
Document changes since last issue.....	9
Related documents.....	10
Support.....	10
Deploying an IP Office Server Edition Solution.....	11
Chapter 2: Installing IP Office Server Edition server	12
Server Edition Primary server.....	12
Creating an installation USB drive.....	12
Creating an installation USB drive for manual installation or upgrade.....	13
Creating an installation USB drive for automatic installation.....	14
Creating an installation USB drive for automatic upgrade.....	14
Installing or upgrading IP Office Server Edition server manually.....	15
Installing IP Office Server Edition server.....	19
Installing IP Office Server Edition automatically	23
Default parameters.....	23
Configuring IP Office Server Edition using the ignition process.....	24
Starting Web Manager.....	32
Starting IP Office Server Edition Manager.....	33
Configuring IP Office Server Edition server using IP Office Server Edition Manager.....	34
Chapter 3: Provisioning Server Edition Secondary server	37
Server Edition Secondary server.....	37
Adding a Secondary server.....	37
Removing a Secondary server.....	39
Chapter 4: Provisioning a Server Edition Expansion System	40
Server Edition Expansion System.....	40
Adding a Server Edition Expansion System (V2).....	40
Adding a Server Edition Expansion System (L).....	42
Removing an expansion system.....	43
Server Edition Expansion System (V2) versus Server Edition Expansion System (L).....	44
Configuration data.....	46
Chapter 5: Configuring IP Office Server Edition Solution	52
IP Office Server Edition Solution.....	52
Web Manager.....	52
IP Office Server Edition Manager.....	53
Operating system support.....	53
Adding a license.....	54
Activating resilience.....	55

Adding an extension.....	56
Adding a hunt group.....	57
Creating a template.....	57
Applying a template.....	58
Configuring alarms.....	58
Linux Platform settings.....	59
Configuring VLAN.....	60
Viewing system information.....	65
Configuring warning banner, alarms, and log files.....	67
On boarding.....	70
Adding a user.....	72
Starting Applications.....	73
Starting Avaya one-X® Portal for IP Office	73
Starting Voicemail Pro client	73
Starting SSA.....	74
Chapter 6: Configuring Avaya one-X® Portal for IP Office.....	76
Configuring Avaya one-X® Portal for IP Office users.....	76
Configuring IP Office Server Edition systems in Avaya one-X® Portal for IP Office	76
Configuring administration access for Avaya one-X® Portal for IP Office	77
Initializing AFA login for Avaya one-X® Portal for IP Office	78
Backing up and restoring one-X Portal.....	79
Backing up Avaya one-X® Portal for IP Office.....	79
Restoring Avaya one-X® Portal for IP Office.....	79
Administering a separate Avaya one-X® Portal for IP Office.....	80
Chapter 7: Configuring Voicemail Pro.....	82
Configuring Voicemail Pro.....	82
Installing Voicemail Pro client.....	82
Logging into Voicemail Pro server.....	83
Backing up and restoring voicemail.....	84
Backing up Voicemail Pro.....	84
Restoring Voicemail Pro stored on IP Office Server Edition server.....	85
Migrating Voicemail Pro to IP Office Server Edition.....	85
Chapter 8: Configuring passwords.....	89
Changing the Administrator password using Web Manager	89
Changing the Administrator password using Linux Platform settings.....	90
Changing root user password.....	90
Changing the Security Administrator password for Server Edition server.....	91
Changing the passwords of common configuration Administrator	92
Chapter 9: Backing up and restoring.....	94
Backing up and restoring the primary server.....	94
Backing up IP Office Server Edition server.....	94
Restoring IP Office Server Edition server.....	98
Restoring a failed IP Office Server Edition server.....	99

Chapter 10: Upgrading	100
Upgrade and downgrade policy.....	100
Server Edition upgrade policy.....	100
Server Edition downgrade policy.....	101
Upgrade.....	103
Downloading ISO using Web Manager.....	103
Upgrading using Web Manager.....	104
Upgrading the system using an installation DVD or USB drive.....	106
Upgrading the system automatically.....	107
Upgrading or changing the version of an application on a local server using Linux Platform settings.....	108
Upgrading IP Office Server Edition version 8.1 to IP Office Server Edition version 9.0.....	109
Chapter 11: Shutting down a system	112
Shutting down a Server Edition Expansion System (V2) using the IP Office Server Edition Manager.....	112
Restarting the server using Web Manager.....	113
Shutting down a Linux server using Linux Platform settings.....	113
Chapter 12: Replacing the hardware of IP Office Server Edition	114
Replacing IP500 V2 system unit.....	114
Replacing System SD Card.....	114
Replacing Field Replacable Unit of IP 500 V2 component.....	115
Replacing a Linux server.....	115
Replacing Virtual Server.....	117
Restoring SSLVPN or IPOSS.....	117
Chapter 13: Capacity planning	119
Introduction	119
Planning Server Edition Expansion System (V2) capacity.....	120
Maximum extension capacity.....	121
Maximum trunk capacity.....	121
Concurrent VoIP Call Capacity.....	122
Maximum VCM Channel capacity.....	123
Call Media Type.....	124
Conference capacity.....	124
Voice recording.....	125
Voicemail.....	126
Multi-Site Network link capacities.....	126
Call media destination.....	127
IP Infrastructure, Bandwidth & VoIP QoS.....	128
Trunk utilization and call traffic profile.....	128
Resilience and Failover.....	129
Planning Server Edition Expansion System (L) capacity.....	129
Capacity planning for over 2000 users.....	131
Chapter 14: Troubleshooting	134

Warning message..... 134

Unable to login. IP Office is under Server Edition Manager Administration..... 136

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. 136

All systems appear online in IP Office Server EditionManager, but appear offline on the Linux Platform settings of the primary server. 137

Debugging steps..... 137

 Logging in as a root user..... 138

 Checking memory usage..... 139

 Checking the version of Linux OS..... 141

IP Office Server Edition certificates..... 141

Identity certificates..... 142

The H323 phones do not automatically register back to the Primary server..... 144

Unable to export template..... 144

 Solution..... 144

Users configured on Server Edition Expansion System are disconnected fromAvaya one-X[®] Portal for IP Office when the system starts registering SIP phones..... 144

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.

Intended audience

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

The following changes have been made to the document since the last issue:

- Server Edition certificate management
- Preferred / Advanced edition comparison
- Expansion system - V2 / Linux comparison
- LAN Support
- Planning capacity
- Replacement procedure
- Upgrade and downgrade policy
- Backup and Restore policy
- Installing IP Office Server Edition automatically

Related documents

	Document	Document ID
1	IP Office Manager	15-601011
2	Administering Voicemail Pro	15-601131
3	Administering one-X Portal for IP Office	15-601139
4	Installing one-X Portal for IP Office	15-601140
5	Avaya IP Office Implementing Voicemail Pro	15-601064
6	Avaya IP Office SSL VPN Solutions	—
7	IP Office Server Edition Reference Configuration	15-604135
8	IP Office Web Manager for Server Edition and Standard Mode	—
9	IP Office Server Edition Solution Overview	15-604133

Support

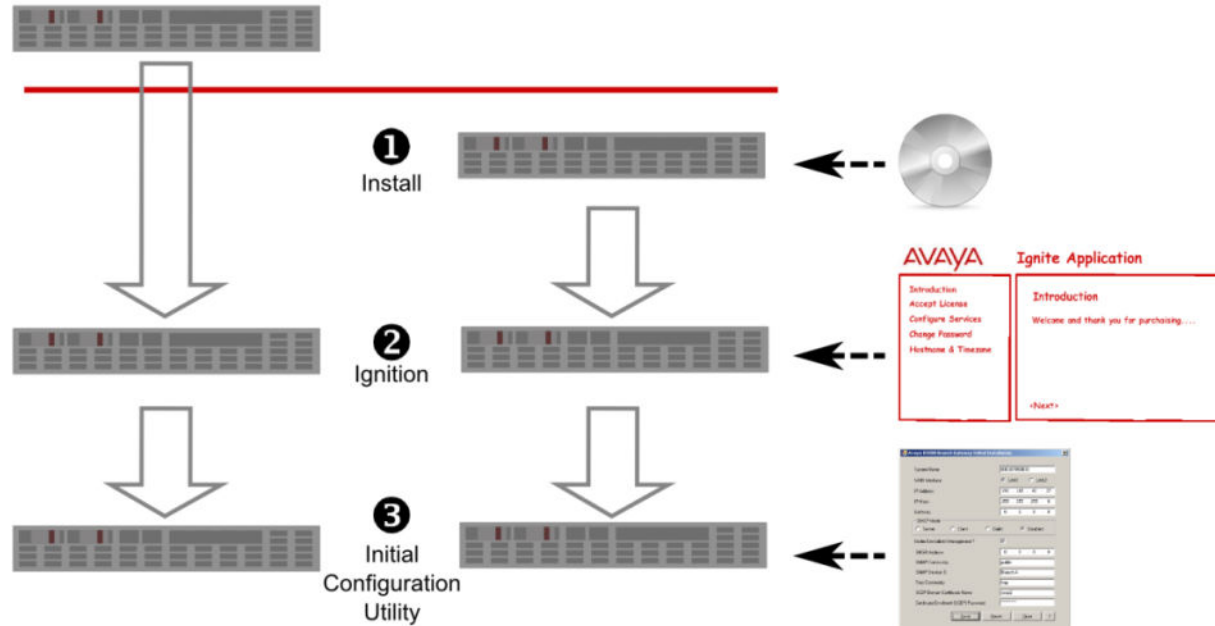
Visit the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live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

Deploying an IP Office Server Edition Solution

About this task

AVAYA Supplied Hardware

Non-Avaya Supplied Hardware
(Controlled introduction only)



* 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 the software for an IP Office Server Edition Solution that you install on any other servers. For more information, about the servers that Avaya supports, see the *Reference Configuration* document.

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

Procedure

1. If you have not purchased a pre-installed server from Avaya, then install IP Office Server Edition Solution on IP Office Server Edition 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 Server Edition Secondary and 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 Server Edition Secondary and Server Edition Expansion System.
7. Administer the various components using Web Manager and IP Office Server Edition Manager.

Chapter 2: Installing IP Office Server Edition server

Server Edition Primary server

Server Edition Primary server is a server where you can add up to 2000 users, IP trunking, and 256 conference channels. The primary server is the only hardware component that you need to deploy an IP Office Server Edition Solution. The primary server manages all the components of IP Office Server Edition Solution, as and when you scale up.

You can configure a 270393/DL360 and a 270395/DL120 or 302788/R210 as a Server Edition Primary server. On a 270393/DL360 server, you can add 2000 users, and on a 270395/DL120 or 302788/R210 server, you can add 750 users. For more information about capacity and specifications, see *IP Office Server Edition Reference Configuration* document.

Creating an installation USB drive

Universal Netboot Installer (UNetbootin) is a cross-platform utility that you can use to create a live USB drive containing a complete operating system that you can boot. You can load a variety of system utilities or install various Linux distributions or other operating systems without using a CD.

Before you begin

Ensure the following:

- You need a USB drive with 8 GB storage space.
Ensure that there are no files in the USB drive.
- Download the ISO image of IP Office Server Edition from <http://support.avaya.com>.
- Download UNetbootin from <http://unetbootin.sourceforge.net>.

About this task

You can install and upgrade IP Office Server Edition using a USB drive.

Note:

If you copy the files of the installation USB drive to another USB drive, you cannot use the copy of the installation USB drive to install IP Office Server Edition. You have to create a new installation USB drive.

Procedure

1. Insert the USB drive in the USB port of the system where you have downloaded the ISO image of IP Office Server Edition.
2. Launch UNetbootin.
3. Select **Diskimage** option.
4. Select **ISO** from the dropdown list
5. Browse to the location where you have downloaded the ISO image of IP Office Server Edition.
6. Set **Type** as **USB Drive**.
7. Select the drive of the USB drive in the **Drive** dropdown list.
8. Click **OK**.
The system displays the progress of installation.
9. Click **Exit**.

Related links

- [Creating an installation USB drive for manual installation or upgrade](#) on page 13
- [Creating an installation USB drive for automatic installation](#) on page 14
- [Creating an installation USB drive for automatic upgrade](#) on page 14

Creating an installation USB drive for manual installation or upgrade

Before you begin

Ensure that you have completed all the steps in [Creating an installation USB drive](#) on page 12.

About this task

To create an installation USB drive for manual installation or upgrade:

Procedure

1. In the USB drive, browse to the folder named *USB*.
2. Copy *syslinux.cfg* file.
3. Paste the *syslinux.cfg* file in the root folder of the USB drive.
The system displays **Confirm File Replace** dialog box.
4. Click **Yes**.

Next steps

Use the installation USB drive to install or upgrade IP Office Server Edition manually.

Related links

[Creating an installation USB drive](#) on page 12

Creating an installation USB drive for automatic installation

Before you begin

Ensure that you complete all the steps in [Creating an installation USB drive](#) on page 12

About this task

To create an installation USB drive for automatic installation:

Procedure

1. In the USB drive, browse to the folder named *USB*.
2. Copy *avaya_autoinstall.conf* file.
3. Paste the *avaya_autoinstall.conf* file in the root folder of the USB drive.

Next steps

Use the installation USB drive to install IP Office Server Edition automatically.

Related links

[Creating an installation USB drive](#) on page 12

Creating an installation USB drive for automatic upgrade

Before you begin

Ensure that you complete all the steps in [Creating an installation USB drive](#) on page 12.

About this task

To create an installation USB drive for automatic upgrade:

Procedure

1. In the USB drive, browse to the folder named *USB*.
2. Copy *avaya_autoupgrade.conf* file.
3. Paste the *avaya_autoupgrade.conf* file in the root folder of the USB drive.

Next steps

Use the installation USB drive to upgrade IP Office Server Edition automatically.

Related links

[Creating an installation USB drive](#) on page 12

Installing or upgrading 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 IP Office Server Edition server, perform this procedure to ensure you have the latest version of the software installed.

Before you begin

You need the following:

- IP Office Server Edition installation DVD .
- Alternatively, IP Office Server Edition installation USB drive. For more information, see [Creating an installation USB drive for manual installation](#) on page 13.
- IP Office Server Edition server.

+ Tip:

You can order the latest version of the IP Office Server Edition installation DVD from Avaya , download the latest version from [http:// support.avaya.com](http://support.avaya.com), or Avaya Product Licensing and Delivery System (PLDS). For more information about, PLDS see *License* section of *IP Office Manager* document.

For more information about the specification of the server, see *IP Office Server Edition Reference Configuration* document.

About this task

* Note:

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.

* Note:

To upgrade IP Office Server Edition from version 8.1 to version 9.0 see, [Upgrading IP Office Server Edition version 8.1 to 9.0](#) on page 109.

To install or upgrade IP Office Server Edition:

Procedure

1. Insert the installation DVD in the DVD drive of IP Office Server Editions server.
 - If you are using an installation USB drive, then insert the installation USB drive in the USB port of IP Office Server Edition server.
2. Restart IP Office Server Edition server.

* Note:

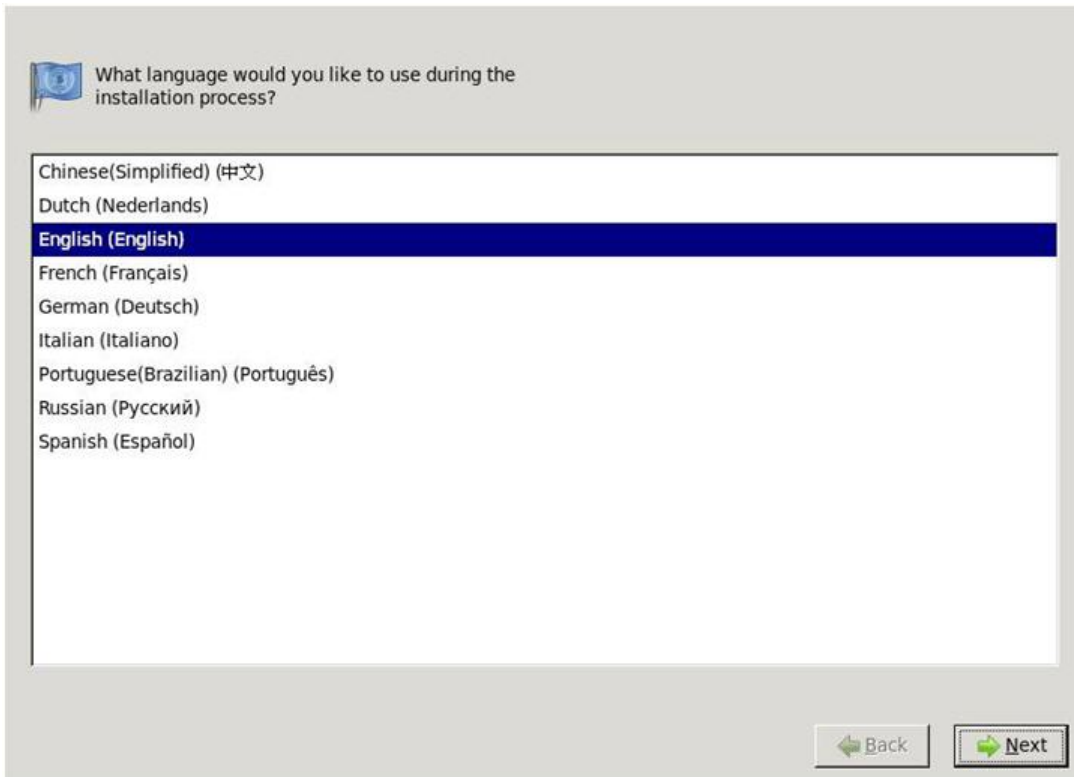
To restart IP Office Server Edition server, always use Web Manager. For more information, see [Restarting the server using Web Manager](#) on page 113. For a new installation, power cycle the server.

The system restarts and boots from IP Office Server Edition installation DVD or the installation USB drive.

*** Note:**

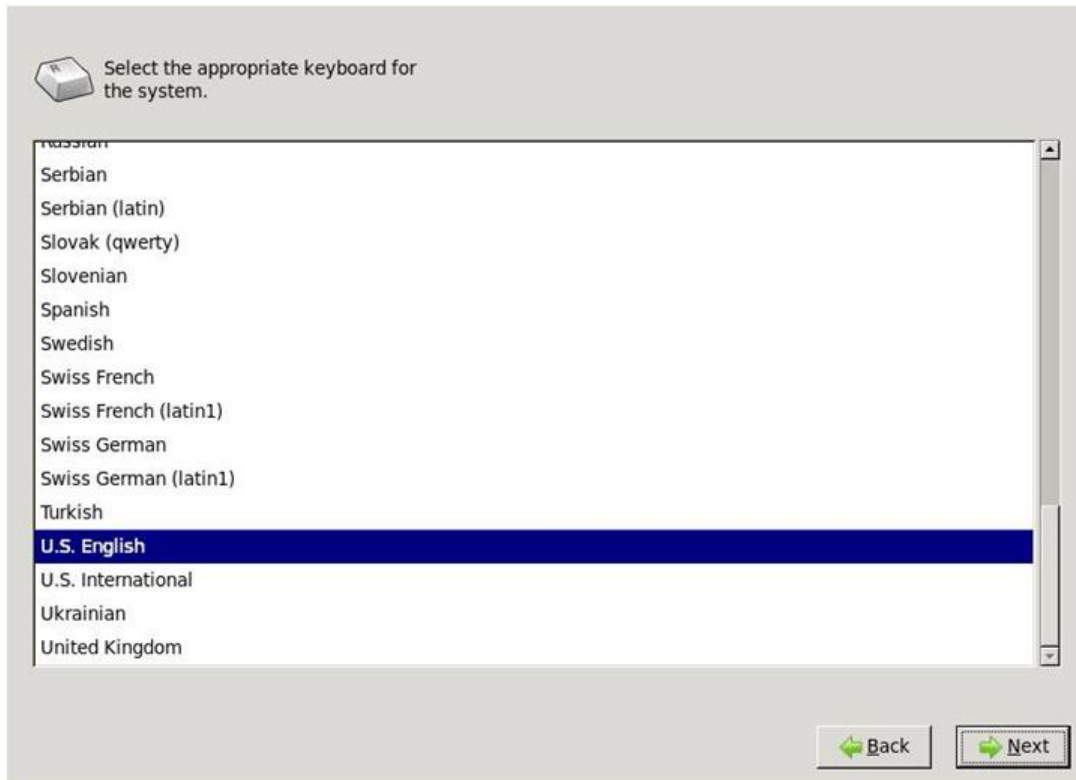
If the system does not restart or boot from IP Office Server Edition installation DVD or the installation USB drive, then verify the boot order in BIOS settings.

3. Click **Change Language** to select the language for use during the installation or upgrade process.



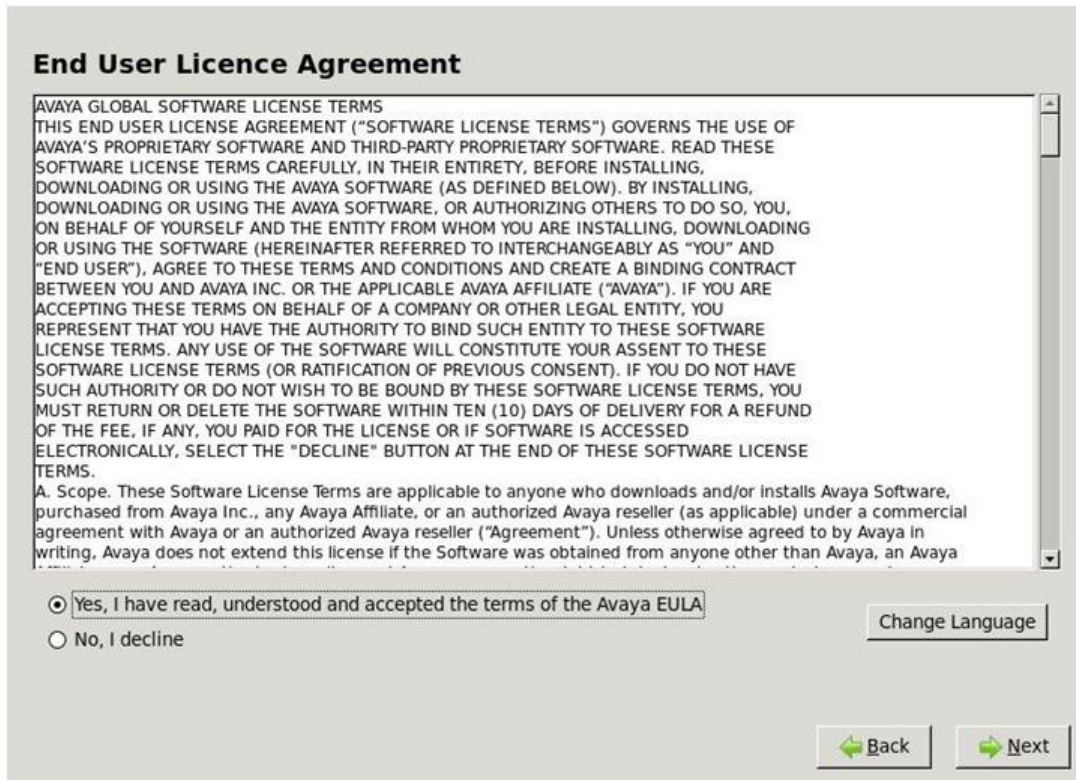
4. Click **Next**.

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 IP Office Server Edition on a server in which IP Office Server Edition is already installed, then the system displays the details of the applications that are already installed on a IP Office Server Edition server. The system also displays the details of the applications that the system will install.

Related links

- [Installing IP Office Server Edition server](#) on page 19
- [Operating system support](#) on page 53
- [Restarting the server using Web Manager](#) on page 113
- [Upgrading the system using an installation DVD or USB drive](#) on page 106
- [Adding a Secondary server](#) on page 37
- [Adding a Server Edition Expansion System \(L\)](#) on page 42
- [Adding a Server Edition Expansion System \(V2\)](#) on page 40
- [Adding a license](#) on page 54
- [Configuring IP Office Server Edition systems in Avaya one-X Portal for IP Office](#) on page 76

Installing IP Office Server Edition server

Before you begin

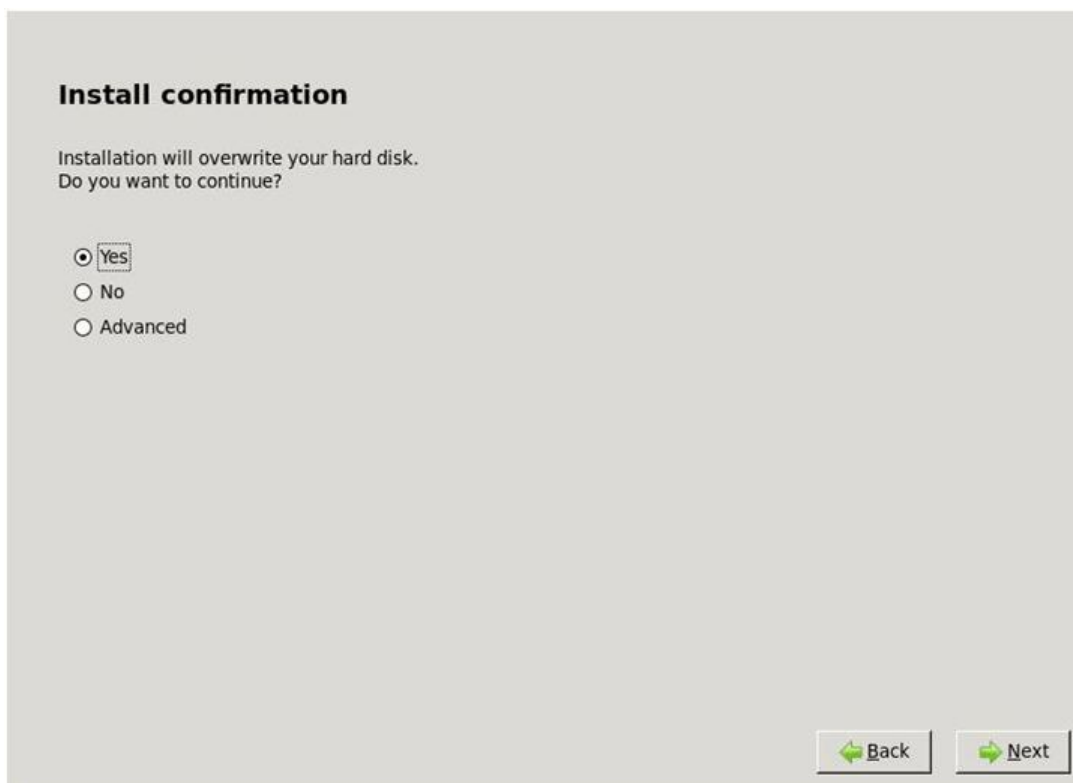
Ensure that you have completed all the steps in [Installing or upgrading server](#) on page 15.

About this task

To install IP Office Server Edition:

Procedure

1. Select **Install** if you want the system to replace the applications that are already installed.
2. Click **Next**.
3. Do one of the following:
 - Select **Yes** if you want to continue with the installation.
 - Select **No** if you do not want to continue with the installation.
 - Select **Advanced** if you want to configure addition settings such as hardware partitioning.

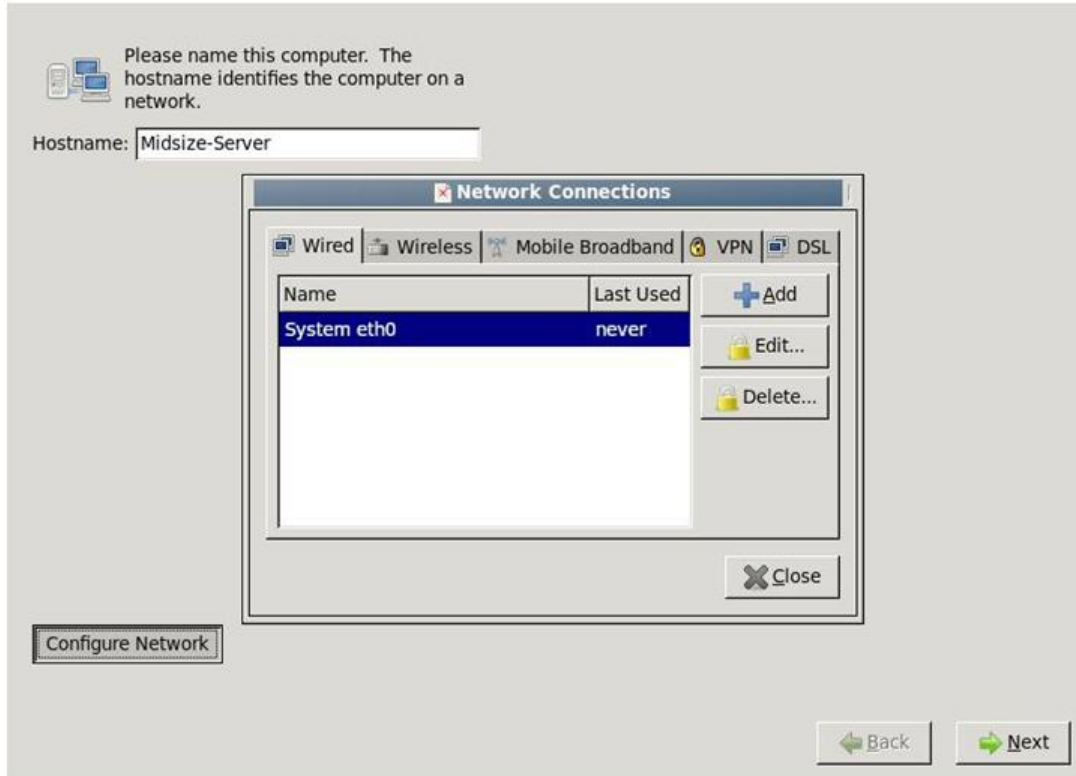


4. Click **Next**.
5. Type the name of the IP Office Server Edition server in the **Hostname** field.

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 (.).

6. 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.

7. Select the network connection that the system has identified.
8. 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

9. Click **Close** to close the **Network Connections** window.
10. Click **Next**.
11. Type the password for the root user in the **Root Password** field.



The root account is used for administering the system. Enter a password for the root user.

Root Password:

Confirm:

Back Next

12. Retype the password in the **Confirm** field.

The system displays a warning message if the strength of the password is weak.

*** Note:**

Make a note of the password that you set for root user because you cannot recover or reset the password for a root user later during the installation, if you forget the password.

13. Click **Next**.

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

14. Click **Next**.

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

15. Click **Next**.

The system displays an option to install TTS language packs

16. Do one of the following:

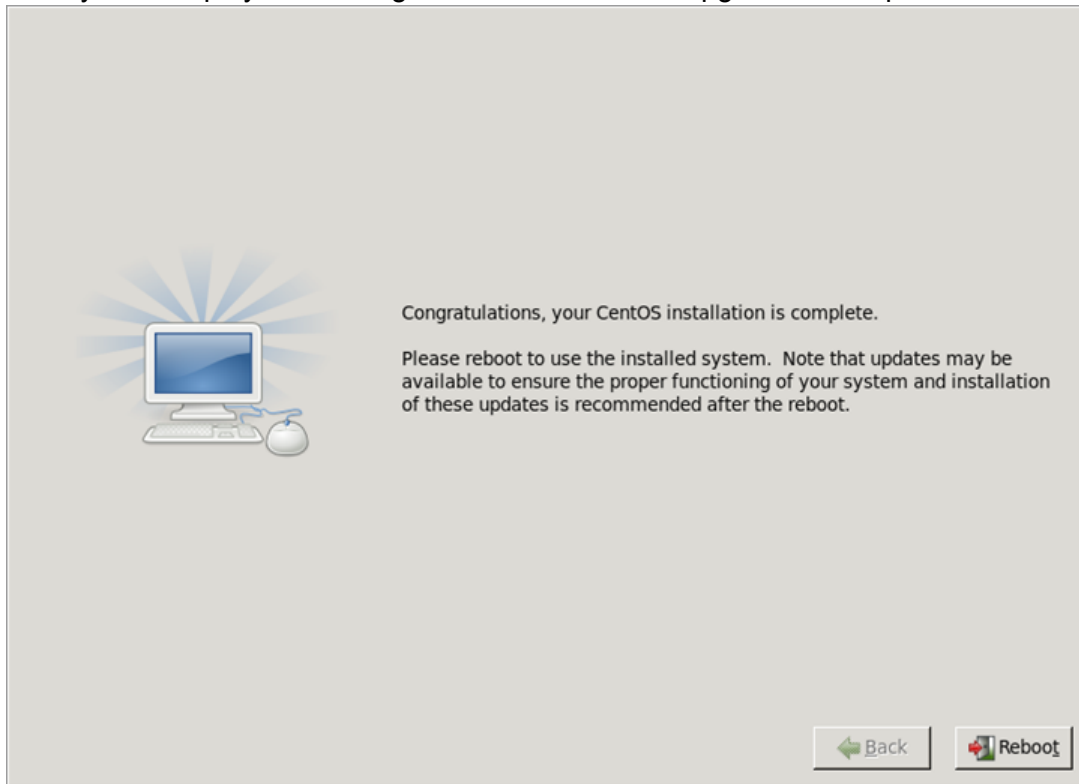
- a. To install TTS language packs, insert the TTS installation DVD, click **Continue**.
- b. To skip installation of TTS language packs, click **Decline**.

17. Click **Next**.

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

Result

The system displays a message if the installation or upgrade is complete.



Next steps

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

Related links

[Installing or upgrading IP Office Server Edition server manually](#) on page 15

Installing IP Office Server Edition automatically

Before you begin

You need the following:

- IP Office Server Edition server.
- IP Office Server Edition installation USB drive. For more information, see [Creating an installation USB for automatic installation](#) on page 14.

About this task

You can install IP Office 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 23

* Note:

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

Procedure

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

* Note:

To restart IP Office Server Editions server, always use Web Manager. For more information, see [Restarting the server using Web Manager](#) on page 113. For a new installation, turn off the power supply to the server.

The system restarts and boots from IP Office Server Edition installation USB.

* Note:

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

Result

The system installs IP Office Server Edition with the default parameters and shuts down IP Office Server Edition server.

Next steps

Remove the installation USB from the USB port of IP Office Server Edition server.

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	<ul style="list-style-type: none">• Connection name: System eth0• IP address: 192.168.42.1• Netmask: 255.255.255.0• Gateway: 0.0.0.0
System eth1	<ul style="list-style-type: none">• 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 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 Avaya one-X[®] Portal for IP Office.

*** 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 IP Office 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 IP Office Server Edition manually are the values that you set during the installation process.

Before you begin

You can gain access to Web Manager using a variety of browsers. Some of the browsers that you can use to gain access to Web Manager are:

- Internet Explorer version 8 and version 9
- FireFox version 13
- Google Chrome version 18
- Opera version 11
- Safari version 5

Note:

You must not gain access to Web Manager using the mobile versions of these browsers.

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> : 7071*



IP Office Server Edition R9.0

Linux release 6.3 (Final)

Please log on.

Logon:

Password:

Language: ▼

SID: c179102bd451a7ca59716681071d32412ca58120 [Print](#)

[Change password](#)

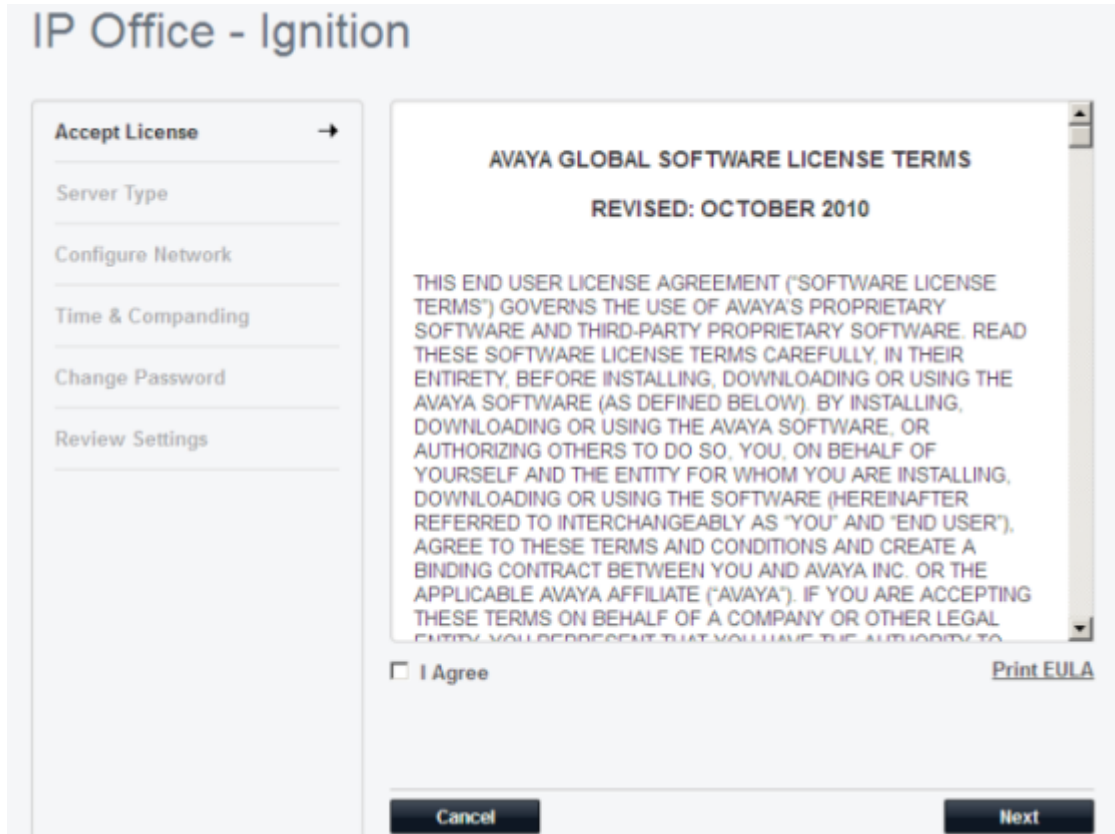
© 2013 Avaya Inc. All rights reserved · [View EULA](#)

The system displays the SID of the IP Office 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 *Administrator*.

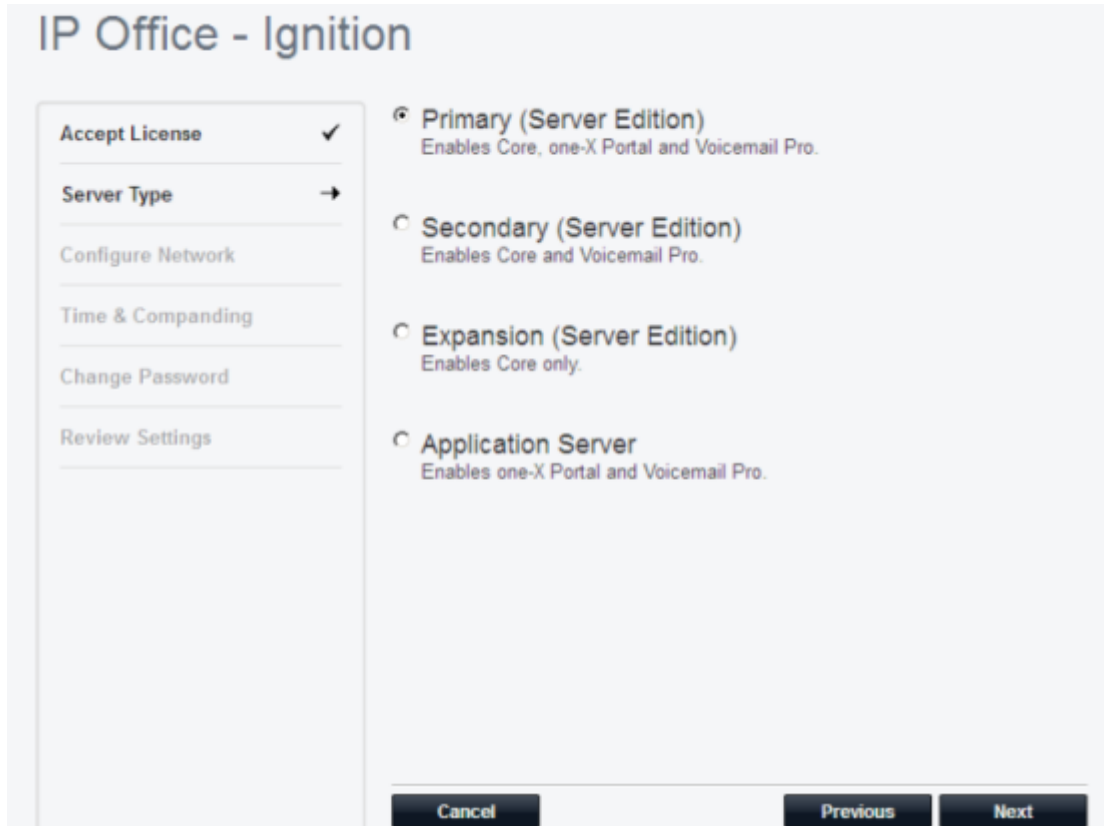
The user name is *Administrator* and the default password is *Administrator*. You must change the default password later to ensure that the system is secure.

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.



To go back to the previous page, click **Previous**. If you do not want to proceed with the Ignition process, click **Cancel**.

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 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.

IP Office Server Edition - Ignition

Network interface: eth0

Accept License ✓

Server Type ✓

Configure Network →

Time & Companding

Change Password

Review Settings

Assign IP Address:

Automatic (DHCP)

IP Address:

Netmask:

Assign System Gateway:

Gateway:

Assign System DNS Servers:

Automatic (DHCP)

Primary DNS:

Secondary DNS:

Hostname:

Cancel **Previous** **Next**

7. In the **Configure Network** page, click **Next**.

The screenshot shows the 'Configure Network' page of the IP Office Server Edition installation wizard. The page is titled 'IP Office Server Edition - Ignition'. On the left side, there is a vertical navigation pane with the following items: 'Accept License' (checked), 'Server Type' (checked), 'Configure Network' (checked), 'Time & Companding' (active, indicated by a right-pointing arrow), 'Change Password', and 'Review Settings'. The main content area is divided into two sections. The top section contains the following settings: 'Use NTP' (checked), 'NTP Server' (text input field containing '0.pool.ntp.org'), 'Date/Time' (date and time pickers showing '2013-08-22 / 09 : 55'), and 'Timezone' (dropdown menu showing 'Europe/Prague'). The bottom section is titled 'Companding' and contains two radio button options: 'µ-law' and 'A-law'. At the bottom of the page, there are three buttons: 'Cancel', 'Previous', and 'Next'.

8. 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.

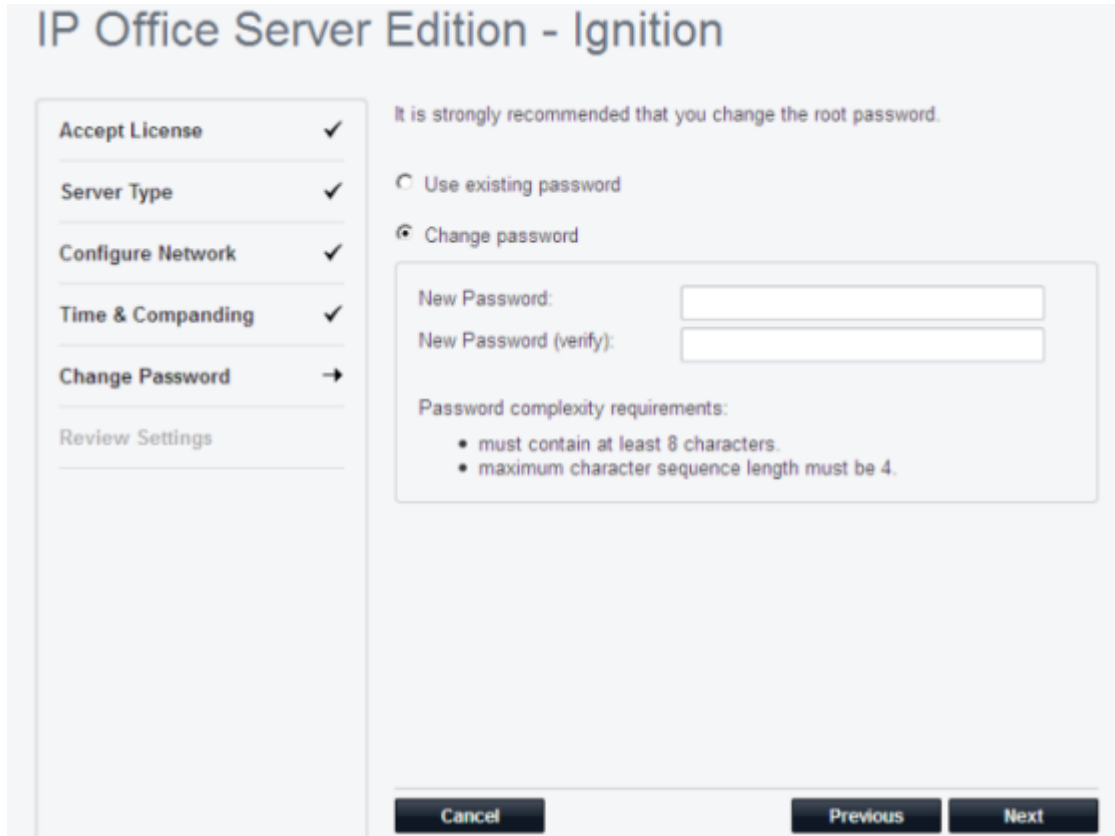
- b. Select the type of **Companding**.

*** 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**.



9. In the **Change Password** page do one of the following:

- Select **Use existing password**.

*** Note:**

Change the password to ensure that the system is secure.

- To change the existing password:
 - a. Select **Change password**.
 - b. Type a password in the **New Password** field.
 - c. 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.

- d. Click **Next**.

The system displays the details of the IP Office Server Edition server.

You can review the settings that you selected during the ignition process. To print the details of the IP Office 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.

IP Office Server Edition - Ignition

Accept License	✓
Server Type	✓
Configure Network	✓
Time & Companding	✓
Change Password	✓
Review Settings	→

System Identification:	c179102bd451a7ca59716681071d32412c458120
Server Type:	Primary
IP:	Automatic (DHCP)
Netmask:	Automatic (DHCP)
Gateway:	Automatic (DHCP)
Primary DNS:	135.124.57.10
Secondary DNS:	135.124.57.11
Hostname:	In03xx04
Timezone:	Europe/Prague
Use NTP:	Yes
NTP Server:	0.pool.ntp.org
Companding:	µ-law
Password:	Do not change

ATTENTION: Prior to ordering licenses for IP Office please confirm the following settings have been finalized: LAN1 and LAN2 IP addresses, Timezone and Hostname. Changing these settings will invalidate any existing licenses. Please see documentation for more detail.

10. Click **Apply**.

The system applies the changes.

Result

The system displays the Web Manager login page only if you have changed the default network configurations.

Next steps

Start IP Office Server Edition Manager.

Starting Web Manager

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

Before you begin

You need to have the ip address of IP Office Server Editions server.

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.

Starting IP Office Server Edition Manager

You can start IP Office Server Edition Manager using Web Manager for IP Office Server Edition server. In an IP Office Server Edition Solution where you have configured a Server Edition Secondary server for resilience, you cannot launch IP Office Server Edition Manager using Web Manager for Server Edition Secondary server, unless the Server Edition Primary server is down.

However, you can start the IP Office Server Edition Manager without using Web Manager if you have already installed IP Office Server Edition Manager on your computer. You can install IP Office Server Edition Manager on your computer using the IP Office Admin DVD or from **AppCenter** page of Server Edition Primary server. For more information, see *Systems — AppCenter field descriptions* section of *IP Office Web Manger for Server Edition and Standard Mode document*.

 **Note:**

When you start IP Office Server Edition Manager using Web Manager for 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 IP Office Server Edition Manager using Web Manager, install the Java Runtime Environment (JRE) Oracle version 1.6. or 1.7.x

About this task

You can configure and manage all the components of IP Office Server Edition Solution using IP Office Server Edition Manager.

Procedure

1. Click **Actions**.

The system automatically loads the IP Office configuration file from the primary server. To load an alternate IP Office configuration file, select a server from the list before selecting **Launch Manager**.

2. In the menu list, select **Launch Manager**.

If the system displays any security warning to run the application, accept the warning and run the application.

Result

The system checks if IP Office Server Edition Manager is installed. The system also checks for the version of IP Office Server Edition Manager that is installed. The system prompts you to download and install the latest version of IP Office Server Edition Manager :

- If the version of IP Office Server Edition Manager is not the latest.
- If IP Office Server Edition Manager is not installed.

Next steps

Do one of the following:

- Click **OK**, to open the current version of IP Office Server Edition Manager that the system has detected.
- Download the latest version of IP Office Server Edition Manager that the system displays and install IP Office Server Edition Manager.

Note:

In the final step of the installation process, do not select the Launch Manager option.

Restart the browser after installing IP Office Server Edition Manager.

After you install IP Office Server Edition Manager, to open IP Office Server Edition Manager directly from a personal computer, select **Start > Programs > IP Office > Manager**.

Related links

[Operating system support](#) on page 53

[Restarting the server using Web Manager](#) on page 113

[Upgrading the system using an installation DVD or USB drive](#) on page 106

Configuring IP Office Server Edition server using IP Office Server Edition Manager

This is the third and final stage in commissioning IP Office Server Edition using the initial configuration utility in IP Office Server Edition Manager.

Note:

You do not have to configure Avaya one-X[®] Portal for IP Office using the initial configuration utility in IP Office Server Edition Manager.

Before you begin

Start IP Office Server Edition Manager.

Procedure

1. Select **File > Advanced > Initial Configuration**.

The system displays a warning message that reads:

The system configuration will be extensively modified and converted as per ICU option section.

2. Click **OK**.
3. Set the configuration of IP Office Server Edition server in Avaya IP Office Initial Configuration

The screenshot shows the 'Avaya IP Office Initial Configuration' dialog box. The 'System Type' section has three radio buttons: 'Basic Mode', 'Midsize Edition' (which is selected), and 'IPO Linux'. Below this, there are text input fields for 'System Name' (containing 'Expansion#1(L)'), 'Locale' (a dropdown menu showing 'United Kingdom (UK Englis'), and 'Services Device ID'. The 'LAN Interface' section has two radio buttons: 'LAN1' (selected) and 'LAN2'. Below that are IP address fields for 'IP Address' (192 . 168 . 0 . 40), 'IP Mask' (255 . 255 . 255 . 0), and 'Gateway' (192 . 168 . 0 . 1). The 'DHCP Mode' section has four radio buttons: 'Server', 'Client', 'DialIn', and 'Disabled' (selected). At the bottom of the configuration area are three more IP address fields: 'Midsize Edition Primary Server' (192 . 168 . 0 . 50), 'Midsize Edition Secondary Server' (192 . 168 . 0 . 60), and 'DNS Server' (192 . 168 . 0 . 1). At the very bottom of the window are four buttons: 'Save', 'Reset', 'Close', and a help button with a question mark.

window.

- a. Set the **System Type** as **Server Edition Primary**, **Server Edition Secondary**, or **Server Edition Expansion**.
- b. Select **Retain Configuration Data** to retain the existing configuration data.
If you do not select **Retain Configuration Data**, the system sets the default values.

- c. Set the name to identify the system in the **System Name** field.
Typically the location or the name of the company is used to identify the configuration. The Gatekeeper feature uses this name to identify the system. The name must be unique within any network of system. The **System Name** field is unique and you cannot use characters such as <, >, |, \0, :, *, ?, . or /.
- d. Set the default telephony and language settings for the system in the **Locale** field.
- e. 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.
- f. Select the LAN interface for the system in the **LAN Interface** section.
- g. Set the IP address of the server in the **IP Address** field.
- h. Set the IP mask address of the server in the **IP Mask** field.
- i. Set the gateway address of the server in the **Gateway** field.
- j. Set **DHCP Mode**.
- k. Type the IP address of the Server Edition Secondary server in the **Server Edition Secondary** field.
- l. Type the IP address of the DNS server in the **DNS Server** field.
- m. Click **Save** to save the configuration details that you set for the system.

For more details about setting the initial configuration in IP Office Server Edition Manager, see the *Initial Configuration Menus* section of the *IP Office Manager* document.

Chapter 3: Provisioning Server Edition Secondary server

Server Edition Secondary server

The Server Edition Secondary server is an optional server where you can add an additional 2000 users, IP trunking, and 256 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 270393/DL360 and a 270395/DL120 or 302788/R210 as a Server Edition Secondary.

 **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 more information about capacity and specifications, see *IP Office Server Edition Reference Configuration* document.

Adding a Secondary server

Before you begin

1. Install IP Office Server Edition on the server that you want to add as a Server Edition Secondary server. If you have purchased a pre-installed IP Office Server Edition server, perform this procedure to ensure you have the latest version of the software installed.
2. Set the role of the server as *Secondary* server in the ignition process.
3. Start IP Office Server Edition Manager using Web Manager for the server.

About this task

To add a Secondary server to IP Office Server Edition Solution using IP Office Server Edition Manager:

Procedure

1. Click **Secondary Server** in the **Add** section of the **Server Edition** window.
2. Enter the IP address of the Secondary server or browse for the secondary server in the **Add Secondary Server** dialog box.
3. Click **OK**.

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. Do one of the following:
 - Click **Yes** if you want to create an offline configuration for the system.
 - Click **No** if you do not want to create an offline configuration for the system.
 - Click **Discard** if you do not want to add the configuration of the system.

For more information on creating an offline configuration, see the *IP Office Manager* document.

Result

The system displays the details of the Secondary server in the **Server Edition** window.

Note:

When you configure Server Edition Secondary 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 Secondary server.

Related links

[Adding a Server Edition Expansion System \(L\)](#) on page 42

[Adding a Server Edition Expansion System \(V2\)](#) on page 40

[Installing or upgrading IP Office Server Edition server manually](#) on page 15

[Adding a license](#) on page 54

[Configuring IP Office Server Edition systems in Avaya one-X Portal for IP Office](#) on page 76

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.

About this task

To remove a secondary server that is a part of IP Office Server Edition Solution using IP Office Server Edition Manager:

Procedure

1. In the **Server Edition** window, right-click 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 4: 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 Primary. Server Edition Expansion System can be a Server Edition Expansion System (V2) that uses the IP500 V2 hardware or Server Edition Expansion System(L) that is based on the HP DL120G7 or Dell R210 hardware. Server Edition Expansion System (L) supports only IP network and a maximum of an additional 750 users. Server Edition Expansion System (V2) supports both analogue, TDM and IP networks, a maximum of an additional 384 users, and data features such as IP routes, NAT, Firewall, and IPsec. You can add up to 30 expansion systems to Server Edition Primary server and it can be any combination of Server Edition Expansion System (V2) or Server Edition Expansion System (L).

Adding a Server Edition Expansion System (V2)

Before you begin

1. Install IP Office Server Edition on the server that you want to add as a Server Edition Expansion System server. If you have purchased a pre-installed IP Office Server Edition server, perform this procedure to ensure you have the latest version of the software installed.
2. Set the role of the server as *Expansion* server in the ignition process.
3. Start IP Office Server Edition Manager.
4. Configure the server using the initial configuration utility of IP Office Server Edition Manager.

Note:

You can convert an existing IP500 V2 to Server Edition Expansion System (V2). For more information on converting an IP500 V2 to Server Edition Expansion System (V2), see *the IP500 V2 Conversion* section of the *IP Office Manager* document.

You can also configure the server using the initial configuration utility of IP Office Server Edition Manager, save the configuration as offline and then configure the server using the ignition process.

About this task

To add a Server Edition Expansion System (V2) to IP Office Server Edition Solution using IP Office Server Edition Manager:

Procedure

1. Click **Expansion System** in the **Add** section of the **Server Edition** window.
2. Enter the IP address of the expansion system or browse for the expansion system in the **Add Expansion System** dialog box.
3. Click **OK**.

If you have not configured a Server Edition Expansion System 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 Expansion System server, you can select the offline configuration that you saved.

- Click **Yes** if you want to create an offline configuration for the system.
- Click **No** if you do not want to create an offline configuration for the system.
- Click **Discard** if you do not want to add a configuration for the system.

For more information on creating an offline configuration see the *IP Office Manager* document.

4. Configure the expansion system using the initial configuration utility.

For more details about setting the initial configuration in IP Office Server Edition Manager, see the *IP Office Manager* document.

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 server.

Related links

[Adding a Secondary server](#) on page 37

[Adding a Server Edition Expansion System \(L\)](#) on page 42

[Installing or upgrading IP Office Server Edition server manually](#) on page 15

[Adding a license](#) on page 54

[Configuring IP Office Server Edition systems in Avaya one-X Portal for IP Office](#) on page 76

Adding a Server Edition Expansion System (L)

Before you begin

1. Install IP Office Server Edition on the server that you want to add as a Server Edition Expansion System server. If you have purchased a pre-installed IP Office Server Edition server, perform this procedure to ensure you have the latest version of the software installed.
2. Set the role of the server as *Expansion* server in the ignition process.
3. Start IP Office Server Edition Manager.
4. Configure the server using the initial configuration utility of IP Office Server Edition Manager.

About this task

To add a Server Edition Expansion System (L) to IP Office Server Edition Solution using IP Office Server Edition Manager:

Procedure

1. Click **Expansion System** in the **Add** section of the **Server Edition** window.
2. Enter the IP address of the expansion system or browse for the expansion system in the **Add Expansion System** dialog box.
3. Click **OK**.

If you have not configured a Server Edition Expansion System 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 Expansion System server, you can select the offline configuration that you saved.

- Click **Yes** if you want to create an offline configuration for the system.
- Click **No** if you do not want to create an offline configuration for the system.
- Click **Discard** if you do not want to add a configuration for the system.

For more information on creating an offline configuration see the *IP Office Manager* document.

4. Configure the expansion system using the initial configuration utility.

For more details about setting the initial configuration in IP Office Server Edition Manager, see the *IP Office Manager* document.

Result

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

Note:

When you configure 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 Server Edition Expansion System server.

Related links

[Adding a Secondary server](#) on page 37

[Adding a Server Edition Expansion System \(V2\)](#) on page 40

[Installing or upgrading IP Office Server Edition server manually](#) on page 15

[Adding a license](#) on page 54

[Configuring IP Office Server Edition systems in Avaya one-X Portal for IP Office](#) on page 76

Removing an expansion system

Before you begin

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

About this task

To remove an expansion system that is a part of IP Office Server Edition Solution using IP Office Server Edition Manager:

Procedure

1. In the **Server Edition** window, 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:**

Default the expansion system that you removed, using IP Office Manager before you use the expansion system in another deployment

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	Server Edition Expansion System (V2)	Server Edition Expansion System (L)	Server Edition Expansion System (L) Comments
Operating system	IP Office OS – Multos	Linux Centos	
Endpoint Support	Maximum 384 from: Analogue Digital SIP H.323 IP DECT Wi-Fi	Maximum 500 from: SIP H.323 IP DECT Wi-Fi	Analogue supported through SIP ATA
Trunk Support	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)	Maximum 250/125 from: SIP H.323	Analogue supported through SIP ATA 250 is for DL360 125 is for DL120 / R210 IP trunk capacity is registered trunks, not channels
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	G.711A/mu G.729a G.722	

Table continues...

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

Feature	Server Edition Expansion System (V2)	Server Edition Expansion System (L)	Server Edition Expansion System (L) Comments
	T.38		
Conferencing	Base platform DSP: 128 Conference channels, 64 party maximum	Integrated media server: 128 Conference channels, 64 party maximum	
Administration	IP Office Manager Web Management System Manager (B5800)	IP Office Manager Web Management Web Control	Web Management used for on-boarding
Licensing ID	SD Card Can be moved	System ID Fixed to hardware	
IPSec/L2TP/PPP	Supported	Not supported	
CTI WAV	Supported	Not supported	CTI Pro is supported
LAN 1/LAN 2	See, <i>IP Office Server Edition LAN support</i> section	See, <i>IP Office Server Edition LAN support</i> section	
PKI trust domains	Not supported in Server Edition Supported only in Essential/Preferred/ B5800	Not supported	Certificate management or PKI not supported on Web Control
Music On Hold	Analogue extn input Audio jack Wav file Beep	Wav file Wav directory Beep	Wav directory up to 255 files
Rated performance			
Call processing (BHCC)	7200	14400 (DL360) 7200 (DL120/R210)	7,200 with one-X Portal users active
Maximum concurrent direct media calls	384	500	
Maximum concurrent RTP Relay calls	120	256 (DL360) 128 (DL120/R210)	
Maximum concurrent TDM<-> IP calls	120	n/a	
Maximum concurrent transcoding calls	74 (148/2)	256 (DL360)	Maximum concurrent transcoding calls

Configuration data

You can migrate a Server Edition Expansion System (V2) and run the ICU on existing systems without reapplying the configuration data, and you can also retain maximum possible configuration areas.

*** Note:**

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

The following table lists what the system retains and modifies, and what you should use when manually converting a configuration using CSV import or export:

Config Area	ICU Operation: 'Retain cfg' not checked	ICU Operation: 'Retain cfg' checked	Migration be allowed?	Potential migration issues	SE Manager Detect/ Correct?	Comments
System	Numerous change	Numerous change, same as default	Partial	Will reset SE mode Remove many ICU changes resulting in: <ul style="list-style-type: none"> • Licensing • Network • Directory • Time • SE Mode • Syslog 	No Some	Should not allow whole system settings to be migrated The only way to preserve settings within the system record is to use the ICU on a live configuration. Will set only necessary values
Line	All IP trunks removed. SE SCN trunks added	All SCN trunks removed. SE SCN trunks added	Partial	No SCN trunks should be allowed Line numbering duplication No Analog/Digital on Linux	Yes Yes	Incorrect SCN trunks will screw licensing and resilience Manager line renumber not solution wide Only if V2 -> Linux considered

Table continues...

Config Area	ICU Operation: 'Retain cfg' not checked	ICU Operation: 'Retain cfg' checked	Migration be allowed?	Potential migration issues	SE Manager Detect/ Correct?	Comments
Unit	No	No	No	None – unit entries are regenerated	No	Pointless migration
Extension	IP extensions deleted Analog/digital Extensions un-numbered	No changes	Yes	Duplicate extension numbers Duplicate extension IDs No Analog/Digital on Linux	Yes Yes	Resolvable in SE manager Resolvable in SE manager Only if V2 -> Linux considered
User	All users deleted	No changes	Yes	Duplicate user names Duplicate user extns CCR Agent settings	Yes Yes Yes	Resolvable in SE manager Resolvable in SE manager Resolvable in SE manager
Hunt Group	Delete all - Except on Primary	Delete all	No	Non SCN hunt groups not supported Hunt groups only on Primary	YesYes	Shouldn't be allowed
Short codes	Feature codes deleted - Except on Primary	No changes	Yes	Existing global feature Short codes stop being global Existing Call routing	Varies No	Any common feature short code that is not part of the migrated configuration will disappear from top level Resolvable in SE manager If SE manager in 'Consolidated' mode, a prompt to harmonize to the Primary common items is offered.

Table continues...

Config Area	ICU Operation: 'Retain cfg' not checked	ICU Operation: 'Retain cfg' checked	Migration be allowed?	Potential migration issues	SE Manager Detect/ Correct?	Comments
						Resolvable in SE manager
RAS	No changes	No changes	Yes			
ICR	Delete all	No changes	Yes	Existing global ICRs stop being global	Varies	Any common ICR that is not part of the migrated configuration will disappear from top level. Resolvable in SE manager If SE Manager in 'Consolidated' mode, a prompt to harmonize to the Primary common items is offered.
License	Delete all	No changes	Yes	Some will not be supported	Yes	Once saved and loaded from IP Office, marked as invalid/ obsolete Resolvable in SE manager
Time Profile	Delete all	No changes	Yes	Existing global Time Profiles stop being global	Varies	Manager allows per device Time Profiles, any that map to common Time Profiles will make that Time Profile disappear from top level

Table continues...

Config Area	ICU Operation: 'Retain cfg' not checked	ICU Operation: 'Retain cfg' checked	Migration be allowed?	Potential migration issues	SE Manager Detect/ Correct?	Comments
						Resolvable in SE manager If SE manager in 'Consolidated' mode, a prompt to harmonize to the Primary common items is offered.
Firewall Profile	No changes	No changes	Yes			Only for Office 500 Expansion System migrations, no Linux support
IP Route	Add gateway route	Add gateway route	Yes			
User Rights	Delete all - Except on Primary	No changes		Existing global user rights stop being global	Varies	Manager allows per device user rights, any that map to common user rights will make that Time Profile disappear from top level Resolvable in SE manager If SE manager in 'Consolidated' mode, a prompt to harmonize to the Primary common items is offered.

Table continues...

Config Area	ICU Operation: 'Retain cfg' not checked	ICU Operation: 'Retain cfg' checked	Migration be allowed?	Potential migration issues	SE Manager Detect/ Correct?	Comments
E911	No changes	No changes	No			E911 not formally supported
ARS	Add default entry for primary/ secondary	Add default entry for primary/ secondary	Yes	Existing Call routing	No	Resolvable in SE manager
Directory	Delete all - Except on Primary	Delete all - Except on Primary	Yes	Expansion/ Secondary directory entries cannot be deleted	Yes	Use CSV export/import to migrate to Primary Use non-SE manager to delete entries
Security Settings	Increase security level	Increase security level	Yes	ICU may not work if PKI trust domain active	No	PC running ICU would require to be in PKI trust domain May have to be changed manually if security setting extensively modified
Call log	No changes	No changes	Yes		No	Internal 'configuration' file on SD Card mapped to users. Not deleted on upgrade or change of mode Standard->SE
DHCP allocation	No changes	No changes	Yes		No	Internal 'configuration' file on SD Card containing

Table continues...

Config Area	ICU Operation: 'Retain cfg' not checked	ICU Operation: 'Retain cfg' checked	Migration be allowed?	Potential migration issues	SE Manager Detect/ Correct?	Comments
						DHCP allocations. Not deleted on upgrade or change of mode Standard->SE

Chapter 5: Configuring IP Office Server Edition Solution

IP Office Server Edition Solution

After you configure all the required components in an IP Office Server Edition Solution use IP Office Server Edition Manager to manage and configure additional settings.

 **Warning:**

You should ensure the Multi-Site Network (SCN) links between Server Edition devices are either all LAN1, or all LAN2. Failure to adhere to this can reduce efficiency and limit some functionality. 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. For more information, see *IP Office Server Edition LAN support* section of this guide.

 **Warning:**

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

Web Manager

Web Manager is a web based solution management application that you can use for performing tasks such as upgrades, backup and restore, day to day user management, using a viewing syslog control, Linux platform administration, creating and modifying admin users.

The following table lists the various tasks that you can perform using the different management interfaces.

Task	Server Edition Manager	Web Manager
Installation	Yes	No
Initial configuration	Yes (ICU)	No
IPOSS on-boarding (SSL VPN)	No	Yes
Upgrades	No	Yes
Backup/Restore	No	Yes

Table continues...

Linux platform configuration	No	Yes
User administration	Yes	Yes
Hunt group, Line, Extension, License	Yes	No
Call routing	Yes	No
Security Administration	Yes	Yes
Embedded File management	Yes	No
VMPPro client launch	Yes	Yes
One-X Portal administration launch	Yes	Yes

IP Office Server Edition Manager

IP Office Server Edition Manager is an application that you can use to manage all the components of IP Office Server Edition Solution. You can launch IP Office Server Edition Manager using Web Manager.

This chapter covers only some of the key settings that you need, to configure for the IP Office Server Edition server using IP Office Server Edition Manager. For example:

- Adding licenses
- Getting the System ID (SID)
- Activating resilience
- Adding extensions, hunt groups
- Creating and applying templates

Note:

For more information about the default Initial Configuration Utility, obtaining the licenses, configuring Incoming call routing, Outgoing call routing, setting time profiles, System directory, administering the system offline, setting up resilience, creating users, extensions, hunt groups using the auto create option, configuring the security settings, converting an existing IP500 V2 system to a Server Edition Expansion System (V2), see the *IP Office Server Edition Mode* section of the *IP Office Manager* document.

Operating system support

Server support

The following server operating systems support IP Office Server Edition Manager:

- Windows Server 2003 (32 bit only)
- Windows Server 2008 Service Pack 2 (32 and 64 bit)

Client support

The following client operating systems support IP Office Server Edition Manager:

- Windows Vista Enterprise Service Pack 2 (32 and 64 bit)
- Windows XP Professional Service Pack 3 (32 bit only)
- Windows 7 (32 and 64 bit)

Adding a license

The license keys are unique strings based on the features that are activated and the unique identity of the system. The unique identity for IP500 V2 expansion system is the Feature Key serial number and the System ID for a Linux system.

Before you begin

1. Start IP Office Server Edition Manager.
2. You need one IP Office Server Edition license for Server Edition Primary, Server Edition Secondary, and one license for each of the Server Edition Expansion System(L) and Server Edition Expansion System(V2). You need to configure these licenses in the Server Edition Primary server.

For more information about licenses, see the *Licenses* section of the *IP Office Manager* document.

About this task

The system recognizes the features that are active only based on the license keys. To add the license using IP Office Server Edition Manager:

Procedure

1. Select the system for which you want to add the license in the navigation pane.
2. Right-click **License**.
3. Select **New**.

You can also add a new license by clicking the **Create a New Record** icon and selecting **License** in the detailed pane.

4. Type the license key in the **License Key** field.
5. Click **OK**.

The system displays the name of the license in the **License Type** and the status as *Unknown* in the **License Status** fields.

6. Click the **Save Configuration** icon.
7. Close and reopen the configuration.

After you reopen the configuration the system displays the status as *Valid* in the **License Status** field in the detailed pane.

Result

The system displays the new license that you added under **License** in the navigation pane.

Related links

[Adding a Secondary server](#) on page 37

[Adding a Server Edition Expansion System \(L\)](#) on page 42

[Adding a Server Edition Expansion System \(V2\)](#) on page 40

[Installing or upgrading IP Office Server Edition server manually](#) on page 15

[Configuring IP Office Server Edition systems in Avaya one-X Portal for IP Office](#) on page 76

Activating resilience

IP Office Server Edition Solution offers resilience to IP Office.

Before you begin

You can activate resilience only if you have configured a Server Edition Secondary in IP Office Server Edition Solution.

About this task

When you add a secondary server to IP Office Server Edition Solution, the resilience for primary and secondary servers are active by default. However, when you add an expansion system to IP Office Server Edition Solution, resilience options for the expansion system are not active by default.

You can activate resilience for users or extension configured on an expansion system to either a Server Edition Primary or Server Edition Secondary only. You cannot split the resilience for an expansion system between Server Edition Primary and Server Edition Secondary. You cannot activate the resilience for an expansion system to another expansion system.

To activate resilience using IP Office Server Edition Manager:

Procedure

1. Click **Resilience Administration** in the **Server Edition** window.
2. Select the resilience settings that you would like to activate in the **Resilience Administration** window.
3. Click **OK**.

Note:

The voice network trunk from the primary server to the secondary server retains voicemail backup to secondary regardless of the IP Phone and hunt group resilience that you choose. The IP Office Server Edition Manager updates the relevant settings in device configurations.

*** Note:**

You can activate the resilience for an expansion system either on a primary server or a secondary server only. You cannot activate the resilience for an expansion system on both the primary server and secondary server.

For more information about resilience, see the *Setting Up Resilience* section of the *IP Office Manager* document.

Adding an extension

An extension is associated with a base extension (directory) number and any settings of a user with the same directory number. Users with a login code can change extensions by logging in and out, so the directory number is not fixed to an extension. When you set a *base extension* number for an extension to associate a default user of that extension when no users log in to that extension.

You can configure a maximum of 2000 extensions on each of Server Edition Primary, Server Edition Secondary, and Server Edition Expansion System (L). You can configure a maximum of 384 extensions on a Server Edition Expansion System(V2).

Over an entire IP Office Server Edition Solution you can configure a maximum of 2000 extensions.

You can also add extensions using the auto create feature in IP Office Server Edition Manager. For more information, see the *Configuration Settings* section of the *IP Office Manager* document.

Before you begin

Start IP Office Server Edition Manager

About this task

To add an extension using IP Office Server Edition Manager:

Procedure

1. In the navigation pane, select the system for which you want to add an extension.
2. Right-click **Extension**, and select **New**.
3. Enter the configuration settings for an extension.

For more information see the *Configuration Settings* section of the *IP Office Manager* document.

4. Click **OK**.

Result

The system displays the new extension under **Extension** in the navigation pane.

Adding a hunt group

A hunt group is a collection of users who are accessible through a single directory number. Any available member of the group can answer the calls to that hunt group. You can set the order in which calls are presented to the users.

You can add a maximum of 300 hunt groups in an IP Office Server Edition Solution . You can add a maximum of 3000 users across 300 hunt groups and in each hunt group you can add a maximum of only 750 users.

Before you begin

Start IP Office Server Edition Manager.

About this task

To add a hunt group using IP Office Server Edition Manager:

Procedure

1. In the navigation pane, select the system for which you want to add a hunt group.
2. Right-click **Hunt Group**, and select **New**.
3. Enter the configuration settings for the hunt group.

For more information on the configuration settings for hunt group, see the *IP Office Manager* document.

4. Click **OK**.

Result

The system displays the new hunt group under **Hunt Group** in the navigation pane.

Creating a template

You can create a template for users, extensions, hunt groups, services, tunnels, firewall profiles, time profiles, IP routes, ARS forms, and lines. The system stores these templates by default in Server Edition Primary server. You can use these templates to add new users, extensions, hunt groups, services, tunnels, firewall profiles, time profiles, IP routes, ARS forms, and lines.

Before you begin

Start IP Office Server Edition Manager.

About this task

To create a template using IP Office Server Edition Manager:

Procedure

1. In the navigation pane, select the profile that you would like to create.
2. Right-click the profile and select **New**.

3. In the detailed pane, enter the details for the profile you selected.

For more information on users, extensions, hunt groups, services, tunnels, firewall profiles, time profiles, IP routes, ARS forms, lines and their settings, see the *IP Office Manager* document.

4. Click **OK**.
5. Click **Export as Template (Binary)** in the detailed pane.
6. Save the template for the profile that you created in the default folder named *template*.

Typically the default location is `C:\Program Files\Avaya\IP Office\Manager\Manager_files\template`

Applying a template

Before you begin

1. Start IP Office Server Edition Manager.
2. Create the templates for profiles such as users, extensions, hunt groups, services, tunnels, firewall profiles, time profiles, IP routes, ARS forms, and lines.

About this task

For more information about the templates and how to apply templates, see the *IP Office Server Edition mode* section in the *IP Office Manager* document.

To apply the templates that you created for the profiles using IP Office Server Edition Manager:

Procedure

1. In the navigation pane, select the profile you want to create.
2. Right-click the profile and select **New from Template (Binary)**.
3. Select the template that you would like to apply for the profile.

To select a template from a folder where you have saved the template click **Open from file**.

Result

The system displays the new profile in the navigation pane.

Configuring alarms

Before you begin

Start IP Office Server Edition Manager.

About this task

The system reports events occurring on the various IP Office applications and the control units. The system uses various methods of reporting events in addition to the real-time and historical reports available through the System Status Application (SSA). You can create multiple event destinations each specifying which events and alarms to include, the method of reporting to use such as SNMP, Syslog or Email, and where to send the events. You can configure up to five alarm destinations for SNMP, two alarm destinations for Syslog, and three alarm destinations for SMTP email.

All the components of IP Office Server Edition Solution forward the alarms using Syslog to Server Edition Primary server and are a part of the server logs. You can view and download these logs using Linux Platform settings. You can configure the system to send alarms to another location using IP Office Server Edition Manager.

To configure alarms using IP Office Server Edition Manager:

Procedure

1. Select **System** in the navigation pane.
2. Select the **System Events** tab.
3. Type the configuration details in the **Configuration** tab.
4. Add the destination for the events in the **Alarms** tab.

For more information on the fields and the configuration settings, see the *System Events* section of the *IP Office Manager* document.

5. Click **OK**.

Linux Platform settings

You can configure Linux Platform settings for a IP Office Server Edition system using Web Manager .

Before you begin

1. Start Web Manager.

Alternatively, on a client computer, start the browser and type `https:<IP address of IP Office Server Edition>:7070/WebManagement/WebManagement.html`.

2. Log in as *Administrator*.

The default password is `Administrator`.

About this task

You can monitor and configure the log files, download and update the applications using Linux Platform settings.

Procedure

1. Click **Platform**.

The system displays Systems window.

2. Under **Control Units**, select the IP Office Server Edition for which you want to start Linux Platform settings.

Result

The system opens Linux Platform settings for the IP Office Server Edition system.

Note:

To open Linux Platform settings for the IP Office Server Edition system in a new tab, click **Launch in new tab**.

Related links

[Configuring VLAN](#) on page 60

[Viewing system information](#) on page 65

Configuring VLAN

Before you begin

Start Linux Platform settings.

About this task

To create a Virtual LAN (VLAN) :

Procedure

1. Select **Settings > System**
2. In the **Network** section, select the network interface where you want to create a VLAN from the **Network Interface** drop-down list.
3. Click **Create Subinterface**.

The system displays Create New Subinterface dialog box.

4. Type the Id for the VLAN in **VLAN Id** field.

The Id of the VLAN that you create must be an integer between 1 and 4094.

5. Set the IP address and the subnet mask for the VLAN.
 - Select **Use DHCP** to assign the IP address and subnet mask for the LAN automatically using DHCP.
 - Clear **Use DHCP** if you do not want to assign the IP address and subnet mask for the LAN using DHCP.
 - a. Type the IP address of the VLAN in **IP Address** field.
 - b. Type the subnet mask in the **Subnet Mask** field.
6. Click **Create**.

Related links

[Linux Platform settings](#) on page 59

[IP Office Server Edition LAN support](#) on page 61

IP Office Server Edition LAN support

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 Expansion System (L).
- No firewall or IP routing support on Linux – all traffic is routed between LAN1 and LAN2 .

In addition, the LAN2 interface of the Server Edition Expansion System (L) has fewer capabilities than LAN1.

- Avaya one-X® Portal client cannot listen to voicemail messages.
- You cannot launch the IP Office Server Edition Manager from Web Control.
- The system cannot access the external MAPI and SMTP voicemail server through LAN2. Use the LAN1 of Server Edition Expansion System (L) for all ethernet traffic and disconnect LAN2.

When in doubt, disconnect the LAN2 of the IP Office Server Edition and use LAN1 for all ethernet traffic.

The following table details the LAN supported features for Server Edition Expansion System (V2) and Server Edition Expansion System (L) platforms in IP Office Release 8.1:

Feature	IP500 V2 LAN1	IP500 V2 LAN2	Linux LAN1	Linux LAN2	Notes
Interface L1-L4					
Interface Support	✓	✓	✓	✓	
Physical<->logical interface mapping	Fixed: 'LAN'	Fixed: 'WAN'	✓	✓	
Speed	10/100	10/100	10/100/ 1000	10/100/ 1000	
Duplex	Full/half	Full/half	Full/half	Full/half	
802.1Q VLAN support	✗	✗	✓	✓	Static VLAN assignment through administration IP500 V2 strips any received VLAN tag
DSCP/ToS	✓	✓	✓	✓	Linux LAN2 uses LAN1 DSCP settings – any LAN2 settings are ignored

Table continues...

Feature	IP500 V2 LAN1	IP500 V2 LAN2	Linux LAN1	Linux LAN2	Notes
Default gateway/ route	✓	✓	✓	✓	Linux through ignition or Web Control
Proxy ARP	✓	✓	✗	✗	IP500 V2 acts as an L3 router
IP Multicast	✓	✓	✗	✗	
Inter LAN					
Firewall	✓	✓	✗	✗	No configurable firewall between Linux LAN interfaces
IP Routes	✓	✓	✗	✗	No configurable IP routing between Linux LAN interfaces. All received Linux LAN traffic that is not terminated on the node is forwarded to the other interface.
NAT/NAPT	✓	✓	✗	✗	
PPP	✓	✓	✗	✗	
Clients					
1XP client – basic	n/a	n/a	✓	✓	
1XP client – VM listen	n/a	n/a	✓	✗	
One-X Communicator Preferred	n/a	n/a	✓	✓	
One-X Communicator Preferred – VM listen	n/a	n/a	✓	✗	
Flare Communicator	✓	✓	✓	✓	
SoftConsole	✓	✓	✓	✓	
VMPro – MAPI Link	n/a	n/a	✓	✗	Two way MS Exchange VM Integration
VMPro – SMTP	n/a	n/a	✓	✗	One way IMAP/Exchange VM integration
Administration					

Table continues...

Feature	IP500 V2 LAN1	IP500 V2 LAN2	Linux LAN1	Linux LAN2	Notes
IP Office Manager	✓	✓	✓	✓	Also accessible through IPOSS remote tunnel (SSLVPN)
Server Edition Manager	✓	✓	✓	✓	Access should be the same LAN1/2 interface as the inter-node connections Also accessible via IPOSS remote tunnel (SSLVPN)
SSA	✓	✓	✓	✓	Also accessible through IPOSS remote tunnel (SSLVPN)
SysMon	✓	✓	✓	✓	Also accessible through IPOSS remote tunnel (SSLVPN)
Web Manager	n/a	n/a	✓	✓	Cannot launch other clients including Manager and Linux Platform settings when not accessed through LAN 1 Also accessible through IPOSS remote tunnel (SSLVPN)
Linux Platform settings	n/a	n/a	✓	✓	Also accessible through IPOSS remote tunnel (SSLVPN)
VMPPro Client	n/a	n/a	✓	✓	Was Web Control in Server Edition Release 8.1 Also accessible through IPOSS remote tunnel (SSLVPN)
Admin launch from Web Manager	n/a	n/a	✓	✗	Launch of IP Office Manager, SSA, Voicemail Pro client from Web Control
Protocols					
DHCP	✓	✓	✓	✓	Client and server
BOOTP	✓	✓	✗	✗	
TFTP	✓	✓	✓	✓	
HTTP/S	✓	✓	✓	✓	Client and server, including embedded file management, web services, phone files

Table continues...

Feature	IP500 V2 LAN1	IP500 V2 LAN2	Linux LAN1	Linux LAN2	Notes
					Backup/restore
SCP	✗	✗	✓	✓	Backup/restore
FTP	✗	✗	✓	✓	Backup/restore
SFTP	✗	✗	✓	✓	Backup/restore
PPP	✓	✓	✗	✗	
IPsec	✓	✓	✗	✗	
VLAN (L2TP/PPTP)	✓	✓	✗	✗	
RIPv2	✓	✓	✗	✗	
SSLVPN	✓	✓	✓	✓	
NTP	✓	✓	✓	✓	Client and server operation
TIME	✓	✓	✗	✗	RFC 868
TSPI	✓	✓	✓	✓	CTI interface for TAPI and one-X Portal
SNMP	✓	✓	✓	✓	Traps and MIBs, v1 only
SMDR	✓	✓	✓	✓	Emission and collection
DNS	✓	✓	✓		
Syslog (UDP + TCP)	✓	✓	✓	✓	Alarms, audit trail, debug
Telephony					
H.323 trunks (including SCN)	✓	✓	✓	✓	LAN1 and LAN2 should not be mixed for SCN. Should be all LAN1 or all LAN2. This also includes Server Edition Manager access
H.323 phones	✓	✓	✓	✓	Phones must be configured with 'local' registrar IP address – for example, not possible to access LAN2 registrar through LAN1
H.323 Remote worker phone	✓	✓	✓	✓	
IP DECT	✓	✓	✓	✓	
SIP trunks	✓	✓	✓	✓	
SIP phones	✓	✓	✓	✓	
STUN	✓	✓	✓	✓	

Table continues...

Feature	IP500 V2 LAN1	IP500 V2 LAN2	Linux LAN1	Linux LAN2	Notes
IP Office softphone	✓	✓	✓	✓	
One-X Communicator Essential	✓	✓	✓	✓	

Related links

[Configuring VLAN](#) on page 60

Viewing system information

You can view various information related to the system such as the status of the application services, CPU usage, Up time, RAID levels and others.

Before you begin

Start Linux Platform settings.

Procedure

1. Click **Platform**.
The system displays Systems window.
2. Under **Control Units**, select the IP Office Server Edition for which you want to start Linux Platform settings.

Result

The system displays the information in the **System** page.

Related links

[Linux Platform settings](#) on page 59

[Systems — System field descriptions](#) on page 65

Systems — System field descriptions

Navigation: **Platform** > **System**

The System page provides a status overview of the server currently selected in the Control Units list. The main content pain contains two sections, **Services** and **System**.

Services

A list of the services being supported by the server and provides a status summary. Use the Start All and Stop All buttons to start or stop all services on the server. The following status elements are displayed.

Field	Description
Start automatically check box	When enabled, the service is configured to start automatically.
Service name and software version	The service name, software release number and build number.
Up Time	The system running time since the last server start.
Mem/CPU Usage	Displays the current memory and CUP usage. Clicking the current usage text opens a summary graph.
Stop/Start	Click to stop or start the service.
Notifications	A summary of the most recent log messages generated by the services running on the control unit. Detailed information is available on the Logs page.

System

Provides a general overview of the sever status and controls to shutdown or reboot the server. Note that it may take up to 10 minutes for CPU usage data to appear after a server reboot.

Control	Description
Shutdown	Selecting Shutdown stops all the application services and then shuts down the server. Use this process when it is necessary to switch off the server for any period. Once the shut down is complete, power to the server can be switched off. To restart the server, switch the power back on.
Reboot	Selecting Reboot stops all the application services and then stops and restarts the server and services.

The left side of the display contains graphs for CPU Usage History, Memory Usage, Disk Usage. The right side of the display contains the following status information.

Field	Description
OS/Kernel	The overall version of the Linux operating system installed on the server and the version of the operating system kernel.
Up Time	The system running time since the last server start.
Server Time	The current time on the server.
Average CPU Load	The average CPU load (percentage use) for the preceding minute, 5 minute and 15 minute periods.
Material Code	The material code for the server. This code is used as part of the system registration with the Avaya Global Registration Tool (GRT).
Model Info	The model information for the server.
System Manufacturer Serial No	The manufacturer's serial number for the server.
Speed	The processor speed.
Cores	The number of processor cores.
Hard Disk Size	The hard disk size.

Table continues...

Field	Description
RAM	The amount of RAM memory.
Disk RAID Levels	The RAID type, if any, being used.
Disk Array Types	The type of disk array being used for RAID.
Virtualized	Indicates if the server is running as a virtualized session.
Last Successful Logon	The date and time of the last successful logon, including the current logon.
Unsuccessful Logon Attempts	A count of unsuccessful logon attempts.

Related links

[Viewing system information](#) on page 65

Configuring warning banner, alarms, and log files

Configuring the age of the log files

Before you begin

Start Linux Platform settings.

About this task

The system notifies you 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. To configure the number of days that these log files need to be retained in the system:

Procedure

1. Select **Setting > General**.
2. 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.

Related links

[Linux Platform settings](#) on page 59

Viewing the log files

Before you begin

Start Linux Platform settings.

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

Select **Logs > Debug Logs**.

- To view the logs of an application, select the application listed in the **Application** drop down list under the **Application Log** table.

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

Related links

[Linux Platform settings](#) on page 59

Configuring syslog files

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

Before you begin

Start Linux Platform settings.

About this task

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

Procedure

1. Click **Settings**.
2. Select **General** tab.
3. 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.

4. Click **Save**.

Example

Related links

[Linux Platform settings](#) on page 59

Viewing the syslog records

Before you begin

- Start Linux Platform settings.
- Configure the syslog events that the server should receive. For more information, see *Configuring the syslog files*.

About this task

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

Procedure

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.

Related links

[Linux Platform settings](#) on page 59

Downloading the log files

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

Before you begin

Start Linux Platform settings.

About this task

To download the log files:

Procedure

1. 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.

2. 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.

Related links

[Linux Platform settings](#) on page 59

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.

Before you begin

Start Linux Platform settings.

About this task

You can set a warning banner that appears in the login page.

Procedure

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

Related links

[Linux Platform settings](#) on page 59

On boarding

On boarding is a process through which you can register a system for remote support and maintenance from Avaya. This section is a short summary about on boarding.

For more details on how to configure and administer SSL VPN services, see the *Avaya IP Office SSL VPN Solutions Guide*.

Before you begin

Start Web Manager.

About this task

To start the on boarding process:

Procedure

1. Log in as Administrator.

The default password is *Administrator*

2. In the Solution View window , click the **Settings** icon of IP Office Server Edition server that you want to on board.
3. In the menu list, click **On-boarding**.

The system displays On-boarding window.

4. In the **Inventory** section specify if the IP Office Server Edition server is a TAA series hardware.

For more information about this filed, click the help icon in the **Inventory** section.

5. Click **Get Inventory File**.

The system downloads the inventory file in .xml format.

6. In the **Registration** section, click **Register IP Office**.

The system opens the Avaya Global Registration Tool Web site after you enter all the information the system prompts you to upload inventory file. After the system registers IP Office Server Edition server, you receive an on-boarding file. The on-boarding file contains configuration settings for the SSL VPN service.

For more information about this filed, click the help icon in the **Registration** section. You can also see, *iposS Equipment Registration and Remote Connectivity Training Module* document on support.avaya.com.

7. In the **Up-load On-boarding File** section, browse to the location where you downloaded the on-boarding file.
8. Click **Upload**.

The system uses the information in the file to update the system configuration.

Result

The system displays a message to confirm that the on-boarding file has been installed successfully. After the on boarding process is complete the Avaya support team can remotely manage the system.

Adding a user

By default, no users are present on IP Office Server Edition systems. You can add a user to a Server Edition Primary, Server Edition Secondary, or Server Edition Expansion System that hosts the physical extension so that the users can log in to the extension to make or receive calls.

You can configure a maximum of 2000 users on each of Server Edition Primary, Server Edition Secondary, and Server Edition Expansion System (L). You can configure a maximum of 384 users on a Server Edition Expansion System (V2).

Over an entire IP Office Server Edition Solution you can configure a maximum of 2000 users.

You can also add users using the auto create feature in IP Office Server Edition Manager. For more information, see the *Configuration Settings* section of the *IP Office Manager* document.

Before you begin

Log in to Web Manager as Administrator.

About this task

To add a user using Web Manager:

Procedure

1. Click **Call Management**.
The system displays Users window.
2. Click **+Add User**.
3. Select the system to which you want to add a user.
4. Enter the configuration settings for the user.

 **Note:**

Ensure that the user name and the extension number is unique. No two users can have the same user name and extension numbers.

If the extension number that you specify for a user does not match the existing base extension number of an extension on the same system, The system prompts you to create a new record for an H323 or SIP extension.

For more information on the configuration settings for the user, see the *Configuration Settings* section of the *IP Office Manager* document.

5. Click **Ok**.

Result

The system displays the new user in the Users window.

Starting Applications

Starting Avaya one-X[®] Portal for IP Office

Avaya one-X[®] Portal for IP Office is a browser based application that you can use to make and receive calls, send instant messages, configure your phone remotely and others.

Before you begin

Log in to IP Office Server Edition using Web Manager.

About this task

You can start Avaya one-X[®] Portal for IP Office application on Server Edition Primary server or Avaya one-X[®] Portal for IP Office configured in the application server using Web Manager.

Note:

You can also start Avaya one-X[®] Portal for IP Office using IP Office Server Edition Manager. For information about starting Avaya one-X[®] Portal for IP Office using IP Office Server Edition Manager, see the *IP Office Server Edition mode* section of the *IP Office Manager* document.

Procedure

1. In the Solution View window , click the dropdown icon of the IP Office Server Editions system for which you want to start Avaya one-X[®] Portal for IP Office.
2. In the menu list, click **Launch one-X Portal**.

Result

The system starts Avaya one-X[®] Portal for IP Office.

Starting Voicemail Pro client

Before you begin

Log in to IP Office Server Edition using Web Manager.

About this task

You can use Voicemail Pro client to create and manage the call flows, record the calls and others.

Note:

You can also start Voicemail Pro client using IP Office Server Edition Manager. For information about starting Voicemail Pro client using IP Office Server Edition Manager, see the *IP Office Server Edition mode* section of the *IP Office Manager* document.

Procedure

1. In the Solution View window , click the dropdown icon of the IP Office Server Edition system for which you want to start VM Pro.

2. In the menu list, click **Launch VM Pro**.

Result

The system checks if Voicemail Pro client is installed. The system also checks for the version of Voicemail Pro client that is installed. The system prompts you to download and install the latest version of Voicemail Pro client:

- If the version of Voicemail Pro client is not the latest.
- If Voicemail Pro client is not installed.

Next steps

Do one of the following:

- Click **OK**, to open the current version of Voicemail Pro client that the system has detected.
- Download the latest version of Voicemail Pro client that the system displays and install Voicemail Pro client.

Note:

Restart the client computer after installing Voicemail Pro client.

After you install Voicemail Pro client, to open Voicemail Pro client directly from a personal computer, select **Start > Programs > IP Office > Voicemail Pro Client**.

Starting SSA

You can use System Status Application (SSA) to monitor the status of a system.

Before you begin

Log in to IP Office Server Edition using Web Manager.

The component of the IP Office Server Edition Solution for which you want to start SSA must be online.

About this task

Note:

You can also start SSA using IP Office Server Edition Manager. For information about launching SSA using IP Office Server Edition Manager, see the *IP Office Server Edition mode* section of the *IP Office Manager* document.

Procedure

1. In the Solution View window, click the dropdown icon of the IP Office Server Editions system for which you want to start SSA.
2. In the menu list, click **Launch SSA**.

If the system displays any security warning to run the application, accept the warning and run the application.

Result

The system opens SSA.

Chapter 6: Configuring Avaya one-X[®] Portal for IP Office

Configuring Avaya one-X[®] Portal for IP Office users

To ensure that the users configured in IP Office Server Edition Manager are able to use Avaya one-X[®] Portal for IP Office you need to configure Avaya one-X[®] Portal for IP Office.

About this task

By default Avaya one-X[®] Portal for IP Office is installed on the Server Edition Primary server. However, to support more than 300 active Avaya one-X[®] Portal for IP Office users you need to configure Avaya one-X[®] Portal for IP Office as a standalone server.

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

Configure users in IP Office Server Edition server or restore the user data from the existing Avaya one-X[®] Portal for IP Office.

To configure Avaya one-X[®] Portal for IP Office users:

Procedure

1. Start IP Office Server Edition 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 the *IP Office Manager* document.

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

To ensure that all users can use the services of Avaya one-X[®] Portal you need to configure all the Server Edition Expansion Systems and Server Edition Secondary of 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 (DSML IP-Office) provider.

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

Related links

[Adding a Secondary server](#) on page 37

[Adding a Server Edition Expansion System \(L\)](#) on page 42

[Adding a Server Edition Expansion System \(V2\)](#) on page 40

[Installing or upgrading IP Office Server Edition server manually](#) on page 15

[Adding a license](#) on page 54

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/onexpportal-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.
6. Click **Change Password**.

Next steps

Initialize the AFA login.

Initializing AFA login for Avaya one-X® Portal for IP Office

You need an AFA login to perform backup and restore operations for Avaya one-X® Portal for IP Office.

About this task

To configure an AFA login:

Procedure

1. On a client computer, start the browser and type *https://<IP address of Server Edition>:8080/onexportal-afa.html*.
2. Login as *Superuser*. The default user name is *Superuser* and password is *MyFirstLogin1_0*.
3. Type the name you want the system to display in the **Display Name** field of Avaya one-X® Portal for IP Office.
4. Type the new password in the **Password** and **Confirm Password** fields.
5. Set the location on the server where you want the system to store the backup files in the **Backup Folder**.

 **Note:**

Even if you are taking a backup and restore from an FTP or local folder on a computer, the system uses the location on the server that you set for storing the files temporarily.

Backing up and restoring one-X Portal

Backing up Avaya one-X® Portal for IP Office

Before you begin

 **Note:**

To perform a backup and restore always use Web Manager. For more information, see [Backing up and restoring the server](#) on page 94 . If you use Avaya one-X® Portal for IP Office to backup and restore, the system does not provide the integrations.

Start Avaya one-X® Portal for IP Office.

About this task

You can backup the Avaya one-X® Portal for IP Office database, Presence and Mobility settings on a local server, an FTP server, or a local drive. You can take a backup manually through the Avaya one-X® Portal for IP Office Administration Web page. You can take unlimited sets of the backup files. The system sets a limit on space used to backup file on a local drive. To backup Avaya one-X® Portal for IP Office:

Procedure

1. Log in as *Superuser*.

For more information on logging in as *Superuser*, see the *Administering one-X Portal for IP Office* document.

2. Click **DB Operations**.
3. Click **Backup**.

For more information about backup settings, see *Administering one-X Portal for IP Office* document.

Restoring Avaya one-X® Portal for IP Office

Before you begin

- Start Avaya one-X® Portal for IP Office using Web Manager
- Ensure that you shutdown all the services on the server.

About this task

You can restore Avaya one-X® Portal for IP Office database, Presence and Mobility settings from a local server, an FTP server, or a local drive. To restore Avaya one-X® Portal for IP Office:

Procedure

1. Log in as *Superuser*.

For more information on logging in as *Superuser*, see the *Administering one-X Portal for IP Office* document.

2. Click **DB Operations**.
3. Click **Restore**.

For more information on restore settings, see the *Administering one-X Portal for IP Office* document.

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

Server Edition Primary supports a maximum of 300 active Avaya one-X® Portal for IP Office users. You can disable the Avaya one-X® Portal service on Server Edition Primary server and dedicate a separate Avaya one-X® Portal for IP Office to support more than 300 active Avaya one-X® Portal for IP Office users. A separate Avaya one-X® Portal for IP Office supports up to 750 users.

Before you begin

- Start Linux Platform settings.
- Take a backup of the existing user data.
- Install and configure the server as Avaya one-X® Portal for IP Office in the ignition process.

About this task

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

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 Office on Server Edition Primary server.
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® Portal in 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 7: Configuring Voicemail Pro

Configuring Voicemail Pro

The Voicemail Pro application provides the basic 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 the Voicemail 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 the Voicemail 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 94 . 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:**

You 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 86

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 85

[Restoring Voicemail Pro not stored on IP Office Server Edition server](#) on page 86

[Backup and restore limitations](#) on page 87

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 85

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 Editions server:

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 85

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 manually 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>`

```
*****
*           IP Office for Linux           *
*                                         *
*      WARNING: Authorised Access Only   *
*****

Welcome Administrator it is Wed Jun 13 05:05:03 BST 2012
> admin
Please enter password:
Admin> root
Password:
[root@localhost ~]#
```

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 85

Chapter 8: Configuring 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 Services window.

2. Click **Preferences** .

The system displays Preferences dialog.

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

4. Retype the new password of the *Administrator* 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**.

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. Click **Save**.

Result

The system changes the password and displays the status of 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 root user password

Before you begin

Start 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.

Chapter 9: Backing up and restoring

Backing up and restoring the primary server

Backing up IP Office Server Edition server

To recover a failed server or a failed server upgrade 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

 **Note:**

You cannot restore the backup the data of one IP Office Server Edition Solution component to another component, unless, either the IP Address or the system id (LAN1 mac address) of the components are the same.

- You can schedule a backup, set the proxy, and a remote server using **Solution Settings**. For more information, see *Using IP Office Server Edition Web Manager*.
- Log into Web Manager as *Administrator*.

About this task

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

Procedure

1. In Solution window, select the component of IP Office Server Edition Solution that you want to backup.

To backup all the components of IP Office Server Edition Solution, select **Actions** checkbox .

2. Click **Actions**.
3. In the menu list, select **Backup**.

The system displays Backup window.

4. Do one of the following:
 - To backup immediately:
 - a. In **Select Remote Server** drop down list, select the remote server that you have set.
 - To backup immediately using a proxy:
 - a. In **Select Remote Server** drop down list, select the remote server that you created.
 - b. Enable **Use Proxy**.
 - c. In **Select Proxy** list, select the proxy details that you created.
 - To backup at a scheduled time:
 - a. In **Select Remote Server** drop down list, select the remote server that you have set.
 - b. Enable **Schedule job**.
 - c. In **Select Schedule** list, select the schedule option that you created.
 - To backup the IP Office sets:
 - a. In **Select Remote Server** drop down list, select the remote server that you have set.
 - b. In **Select IP Office Sets** list, select the IP Office set that you want to backup.
 - To backup one-X Portal sets:
 - a. In **Select Remote Server** drop down list, select the remote server that you have set.
 - b. In **Select one-X Portal Sets** list, select the one-X Portal set that you want to backup.
 - To backup Voicemail Pro sets:
 - a. In **Select Remote Server** drop down list, select the remote server that you have set.
 - b. In **Select Voicemail Pro Sets** list, select the Voicemail Pro set that you want to backup.
 - To backup CSIPO sets:
 - a. In **Select Remote Server** drop down list, select the remote server that you have set.
 - b. In **Select CSIPO Sets** list, select the CSIPO set that you want to backup.
5. In **Add Label** field, type a label for the backup.
6. Click **OK**.

Result

The system backup the components and notifies the status of backup in the Dashboard of Web Manager.

Related links

[Backup and restore policy](#) on page 96

[Backup data sets](#) on page 97

[Backup and Restore location](#) on page 97

Backup and restore policy

It is essential to implement a considered, robust and secure backup policy before any failure or other restore requirements. It is not possible to define a single approach that would meet all possible customer needs; each installation should be assessed before a policy is implemented. Consider the following aspects as a part of such a policy:

- Ignition settings. These should be printed or saved for each Linux Server after initial ignition.
- IPOSS/SSLVPN onboarding.xml file: One for each on-boarded system should be saved.
- License key data: All ADI license key files should be saved.
- Manual configuration backup for each IP Office after initial installation and major configuration change.
- Manual configuration backup for Voicemail Pro after initial installation and major configuration change.
- Manual configuration backup for one-X Portal after initial installation and major configuration change.
- Periodic configuration backup for every IP Office.
- Periodic configuration backup for one X Portal – Primary and Application Server only
- Periodic configuration backup for Voicemail Pro – Primary only
- Periodic voice mailbox and recording data backup – Primary only
- The timing of backup operation: This should be done when little or no traffic is present on the target system, but the backup process itself is not service-affecting.
- The timing of restore operation: This should be done when no traffic is present on the restored system. The restore process is service affecting – any restored component will automatically restart immediately the restore is complete.
- Security, integrity, location and capacity of backup data storage.

 **Note:**

backup of an Avaya Linux server does not include any local backup data.

- Security of backup data communication
- Backup prior to any software upgrade
- Retention of backup data for older software versions should a *downgrade* need to be considered.

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. Periodic backups using Web Manager have up to 14 instances and a single manual backup instance, after which the system overwrites the oldest set. These instances are for each backup server and regardless of the backup data set; for example two weekly separate backup tasks of all IP Office configurations and Voicemail configuration overwrite the first set after 7 weeks.

Related links

[Backing up IP Office Server Edition server](#) on page 94

Backup data sets

The following table provides information about the backup data sets:

Data Set	Content	Notes
IP Office Configuration (V2)	Configuration, Security Settings, DHCP Allocations, Call log	When selected for IP500 V2 Expansion systems
IP Office Configuration (L)	Linux Server Settings, Web Management Settings, Configuration, Security Settings, DHCP Allocations, Call log	When selected for Primary, Secondary, one-X Portal Server, and Linux Expansion systems This backup set does not include any back data on the server itself.
One-X Portal Configuration	one-X Portal server settings	
Voicemail Pro Configuration	Voicemail Pro server preferences, Call flows	
Messages & Recordings	Voice mailbox contents, Call recordings	
Voicemail Pro Full	Voicemail Pro server preferences, Call flows, Voice mailbox contents, Call recordings	

Related links

[Backing up IP Office Server Edition server](#) on page 94

Backup and Restore location

IP Office Linux Server as the Backup/Restore location

You can set any Linux Server of IP Office Release 9.0 as the backup and restore location. The following table provides details of backup file store for the following protocols and settings:

Protocol	Port	Remote Path	User Name/ Password	Notes
HTTP	8000	/avaya/backup	none	HTTP supported by all IP Office components
SFTP	22	/var/www/html/avaya/backup	Any service user with <i>WebControl Admin</i> rights,	SFTP supported by Linux-based components

Table continues...

			Root (not recommended)	
SCP	22	/var/www/html/avaya/backup	Any service user with WebControl Admin rights, Root (not recommended)	SCP supported by Linux-based components

*** Note:**

To restore use the same *Remote Server* (protocol, port and path) settings.

Related links

[Backing up IP Office Server Edition server](#) on page 94

Restoring IP Office Server Edition server

You can restore the primary server using the backup file on a local drive or a remote file server, which can optionally be the secondary server.

Before you begin

Ensure that you have taken a backup of the server.

About this task

You can restore the primary server using the backup file on a remote file server using Web Manager:

Procedure

1. In Solution window, select the component of IP Office Server Edition Solution that you want to restore.
To backup all the components of IP Office Server Edition Solution, select **Actions** checkbox .
2. Click **Actions**.
3. In the menu list, select **Restore**.
The system displays Restore window.
4. Do one of the following:
 - To restore from a remote server:
 - a. In **Select Remote Server** drop down list, select the remote server that you have set.
 - To restore using a proxy:
 - a. In **Select Remote Server** drop down list, select the remote server that you created.
 - b. Enable **Use Proxy**.
 - c. In **Select Proxy** list, select the proxy details that you created.

5. Click **Get Restore Points**.

The system displays the restore points with details such as name of the backup, type of backup, IP address of the server, the version, sets of backup, and the time stamp of the backup in **Select Restore Point** table.

6. Select the restore point from the **Select Restore Point** table.
7. Click **OK**.

Result

The system restores the components and notifies the status of restore in the Dashboard of Web Manager.

Restoring a failed IP Office Server Edition server

Before you begin

Note:

You cannot restore the backup the data of one IP Office Server Edition Solution component to another component, unless, either the IP Address or the system id (LAN1 mac address) of the components are the same.

Ensure that you shutdown all the services on the server.

About this task

To restore a failed IP Office Server Edition server:

Procedure

1. Install the IP Office Server Edition server.
For more information about installing, configuring IP Office Server Edition using ignition process and IP Office Server Edition Manager, see Chapter 2 of this document.
2. Restore the following:
 - a. Restore the Server Edition Primary server.
 - b. Restore the Voicemail Pro server.
 - c. Restore the Avaya one-X[®] Portal for IP Office server.
3. Add the Server Edition Secondary server.
4. Add the Server Edition Expansion System.

Chapter 10: Upgrading

Upgrade and downgrade policy

Server Edition upgrade policy

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

1. Review the release notes of the prospective version before you upgrade.
2. Ensure that a correct Server Edition Software Upgrade license is available.
3. Take a backup of the solution backup from Primary Server before you upgrade:
 - For Release 9.0, take a backup of the system using Web Manager and the backup should include all systems, components and configuration data sets.
 - For Release 8.1, take a backup of the system backup using Web Control, and in addition for a complete backup that includes the security settings of each of the component, perform a Backup Memory Card command using IP Office Manager for Server Edition.
4. Perform an upgrade when no traffic is present on the system because it will affect the service.
5. Take a Solution backup after any upgrade

Minor Upgrades

1. *Minor* Server Edition upgrade is an upgrade from one release to another minor release in that series including Service Packs (SP). For example: 9.0 GA to an 9.0 SP or 9.0 SP to another 9.0 SP
2. *Minor* upgrade does not require a manual pre or post upgrade activities such as database exporting/import, configuration resets.
3. *Minor* upgrade does not result in the loss of configuration, logs or other stored data.

Major Upgrades

Insert content for the first section.

1. *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 8.1 FP to 9.0 GA
2. *Major* does not require a manual pre or post upgrade activities such as database exporting/import, configuration resets, however this cannot be guaranteed.

3. *Major* upgrade does not result in the loss of configuration, logs or other stored data, however this cannot be guaranteed

Upgrade Licenses

1. To upgrade from one Server Edition release to another, for example, from 8.1 to 9.0 , 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.
2. 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.

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.

* Note:

For both the Server Edition and Application Server, after an upgrade from 8.1 to 9.0 , SNMP configuration settings are removed. SNMP can be configured using IP Office Manager.

* Note:

Avaya reserve the right to change the Server Edition upgrade policy at some time in the future

Server Edition downgrade policy

Both *Minor* and *Major* Server Edition downgrades are supported, however after 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 may 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 may performing a complete reinstallation and re-ignition.
7. You can perform a *Major* Linux server downgrade, for example, 8. 1 FP to 9.0 GA, 8.0 GA to 9.0 GA) may 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 IP Office Manager, memory card Restore command, or upgraded through the downgraded Server Edition PrimaryWeb Control or Web Manager.

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. 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 of the correct configuration version or the administer a 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.

Summary

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

- 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

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

- Installation DVD or USB drive.
- Web Manger — to upgrade local or remote server.

*** 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, USB, primary server path, and 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 using **Solution Settings**. For more information about setting the remote server and proxy settings, see *Using IP Office Server Edition Web Manager*.
- Log into Web Manager as *Administrator*.

About this task

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

Procedure

1. In Solution window, click **Actions**.
2. In the menu list, select **Transfer ISO**.

The system displays Transfer ISO window.

3. 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 USB drive of primary server.
 - a. Insert the installation USB drive in the USB port of the primary server.
 - b. In **Download from** field, select **USB Primary Server**.
- 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.

Upgrading using Web Manager

After you download the latest ISO in the primary server, the system displays  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 one-X Portal, or Contact Store for IP Office are the same.

Before you begin

- To schedule an upgrade, set schedule options using **Solution Settings**. For more information about schedule options, see *Using IP Office Server Edition Web Manager*.
- Log into Web Manager as *Administrator*.
- Download the latest ISO using Web Manager.

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.

Procedure

1. In Solution window, select the component of IP Office Server Edition Solution that you want to upgrade.

To upgrade all the components of IP Office Server Edition Solution, select **Actions** checkbox .

2. Click **Actions**.

3. In the menu list, select **Upgrade**.

The system displays Upgrade window.

4. Do one of the following:

- To upgrade immediately:

- a. In **Upgrade from** field, select **Primary Server**.

- To upgrade at a scheduled time:

- a. In **Upgrade from** field, select **Primary Server**.

- b. Enable **Schedule job**.

- c. In **Select Schedule** list, select the schedule option that you created.

5. Click **OK**.

The system displays information about software run-time license information in Upgrade dialog.

6. Click **Yes**.

The system displays Agreement window.

7. Read and accept the license agreement.

8. Click **Next**.

Result

The system upgrades the components and notifies the status of upgrade in the Dashboard of Web Manager.

Upgrading the system using an installation DVD or USB drive

Before you begin

Ensure that you have completed all the steps in [Installing or upgrading server](#) on page 15.

About this task

To upgrade IP Office Server Edition:

Procedure

1. Select **Upgrade**.

The system preserves the user data when you upgrade.

2. Click **Next**.

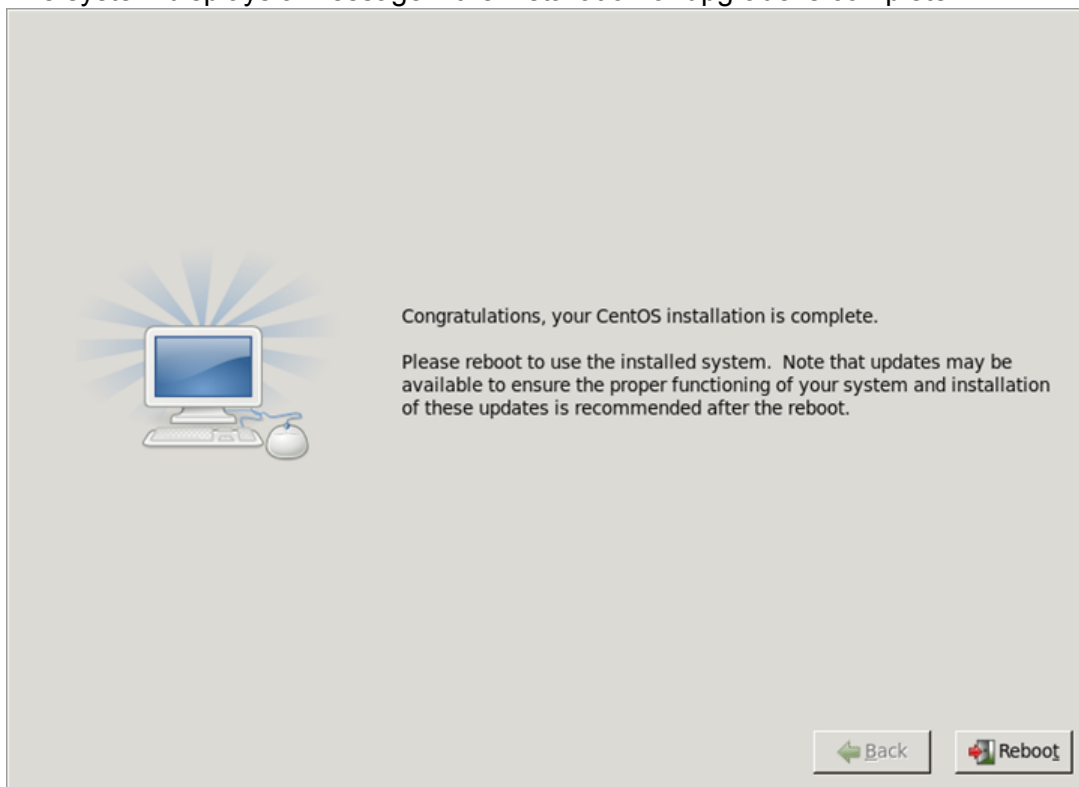
The system displays details such as the location of *upgrade.log* file.

3. Click **Next**.

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

Result

The system displays a message if the installation or upgrade is complete.



*** Note:**

When you upgrade IP Office Server Edition from release 8.1 to 9.0, the system upgrades the version of CentOS to 6.3. For more information see, [Checking the version of CentOS](#) on page 141.

Next steps

Remove the installation DVD or the installation USB drive from the DVD drive or the USB port, and click **Reboot**. Log in to the sever using the Web browser on another computer in the network.

Upgrading the system automatically

Before you begin

- Ensure that all components of IP Office Server Edition Solution are at Release 8.1

You need the following:

- IP Office Server Edition server.
- IP Office Server Edition installation USB drive. For more information, see [Creating an installation USB drive for automatic upgrade](#) on page 14.

*** Note:**

- After you upgrade to Release 9.0 you will not be able to downgrade to an older Release. You will have to reinstall IP Office Server Edition server.
- Upgrade standalone Avaya one-X[®] Portal separately.
- After you upgrade to Release 9.0 you cannot use backup data of Release 8.1. After you upgrade, to ensure service continuity take a complete solution backup using Web Manager.

About this task

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

Procedure

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

*** Note:**

To restart IP Office Server Edition server, always use Web Manager. For more information, see [Restarting the server using Web Manager](#) on page 113. For a new installation, turn off the power supply to the server.

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

*** Note:**

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

Result

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

*** Note:**

When you upgrade IP Office Server Edition from release 8.1 to 9.0, the system upgrades the version of CentOS to 6.3. For more information, see [Checking the version of CentOS](#) on page 141.

Next steps

Remove the installation USB drive from the USB port of IP Office 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**.


Upgrading IP Office Server Edition version 8.1 to IP Office Server Edition version 9.0

Web Control is the solution management application for IP Office Server Edition version 8.1

and Web Manager is the solution management application for IP Office Server Edition version 9.0.

To upgrade an IP Office Server Edition version 8.1 to IP Office Server Edition version 9.0, you begin the upgrade using the Web Control and complete the upgrade using Web Manager.

When you download a new version of the software in the repository server for update files, the

system displays an  update available icon for the servers, in the **Servers** section of Web Control.

Before you begin

Ensure that you upgrade an existing IP 500 V2 that is not version 8.1 or later using the IP Office Manager.

About this task

*** Note:**

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

Procedure

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

The default port number is 7070.

2. Logon as *Administrator*.
3. Select **Solution Management**.

4. In the **Solution Upgrade File** section type `https://IP address of the host server:port number/abe-x.x.x-x.iso` in the **URL of file containing updates** field.

5. Click **Save File**.

The system displays the status of the file download. If you do not want to download the file click **Cancel**.

6. In the **Solution Upgrade Actions**, click **Update Primary**, to upgrade the primary server.


 **Note:**

The system takes about 40 minutes to upgrade. You will lose the connectivity to the system during the upgrade because the system also upgrades the Web Control.

7. After the system upgrades the primary server, on a client computer, start the browser and type `https:// <IP address of the Server> :<port number>`.

The default port number is 7070. The system displays Web Manager.

8. Logon as *Administrator*.

The system displays  update available icon in the Solution window for the servers.

9. In Solution window, select the component of IP Office Server Edition Solution that you want to upgrade.

10. Click **Actions**.

11. In the menu list, select **Upgrade**.

The system displays Upgrade window.

12. Do one of the following:

- To upgrade immediately:
 - a. In **Upgrade from** field, select **Primary Server**.
- To upgrade at a scheduled time:
 - a. In **Upgrade from** field, select **Primary Server**.
 - b. Enable **Schedule job**.
 - c. In **Select Schedule** list, select the schedule option that you created.

13. Click **OK**.

The system displays information about software run-time license information in Upgrade dialog.

14. Click **Yes**.

The system displays Agreement window.

15. Read and accept the license agreement.

16. Click **Next**.

Result

The system upgrades the components and notifies the status of upgrade in the Dashboard of Web Manager.

Chapter 11: Shutting down a system

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

To shut down a system using IP Office Server Edition Manager:

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**.

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

Restarting the server using Web Manager

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

Before you begin

Start Linux Platform settings.

About this task

To restart a server:

Procedure

1. Click **Platform**.
The system displays Systems window.
2. Under **Control Units**, select the IP Office Server Edition you want to reboot.
3. In the **System** section of the **System** page, click **Reboot**.
4. In the **Warning** dialog box, click **Yes** to confirm that you want to reboot the system.

The system displays the login page. Do not log in again because the system is in the process of stopping the services.

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 12: Replacing the hardware of IP Office Server Edition

Replacing IP500 V2 system unit

Before you begin

- At all times follow the relevant safety and static handling procedures. For further information see, *Warnings* section of the *IP500 V2 installation guide*.
- Take an SD card backup using either IP Office 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 IP Office 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. Turn the power on of the system – local connectivity only.
5. Check status using the locally attached IP Office Manager and SSA.
6. Reconnect to the network.
7. Check the configuration using IP Office Manager for Server Edition and Web Manager.

You do not have to restore in this instance; all necessary data is on the SD card, licenses are valid as well.

Replacing System SD Card

Before you begin

At all times follow the relevant safety and static handling procedures. For further information see, *Warnings* section of the *IP500 V2 installation guide*.

Procedure

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

You do not have to shutdown the system.

2. Remove SD card.
3. 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.
4. 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.

5. Using IP Office Manager for Server Edition, administer new local licenses, delete old.
6. Validate status and configuration with IP Office Manager for Server Edition, Web Manager, IP Office Manager for Server Edition, and SSA.
7. Take a backup using Web Manager and 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 Field Replacable Unit of IP 500 V2 component

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 the *IP500 V2 installation guide*.

Replacing a Linux server

Before you begin

- 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.
- The HP DL360 hard drives and power supplies are hot swap; there is no need for chassis replacement. These items should be replaced whilst 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.

- If not down already, shutdown 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 HP DL120 with Dell R210.

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 system – local connectivity only
2. Upgrade to the latest version of IP Office Server Edition Solution using the local Web Manager.
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 using the same settings as the original ICU
5. On the Web Manager of Server Edition Primary , run node restore with override for new ID .
The system restores all configuration and data saved in the original backup. If this is an Application Server that is not a part of Server Edition, use local Web Manager to restore.
6. Reconstitute the security settings because they are locked to the System ID and are not restored by default.
 - If the system is supported through, see [Restoring SSLVPN/IPOSS](#) on page 117
 - If you are replacing a Server Edition Primary server, set all the non-default security setting using IP Office Manager.
 - If you are replacing a Server Edition Secondary, Server Edition Expansion System, or an Application Server, use the *Synchrosize Security* feature of Web Manager.
7. Validate status and configuration with Web Manager, IP Office Manager for Server Edition, and SSA.
8. Take a backup using Web Manager.
9. Using IP Office Manager for Server Edition, administer new local licenses, delete old.
Any local licenses will become invalid after 30 days; an offline license swap-out exists.

Example

Next steps

Replacing Virtual Server

About this task

To replace a Virtual Server:

Procedure

1. Do one of the following:
 - If original server running and vMotion supported; execute vMotion onto the new server.
The system migrates all configuration, data and licenses onto the new platform.
 - If the original server not running or vMotion not supported, reinstate VM snapshot image.
 - If the system does not support vMotion or VM snapshot image, do a fresh installation on the replacement hardware.
2. On Web Manager of Server Edition Primary , run node restore with override for new ID .
The system restores all configuration and data saved in the original backup. If this is an Application that is not a part of Server Edition, use local Web Manager to restore.
3. Reconstitute the security settings because they are locked to the System ID and are not restored by default.
 - If the system is supported through, see [Restoring SSLVPN/IPOSS](#) on page 117
 - If you are replacing a Server Edition Primary server, set all the non-default security setting using IP Office Manager.
 - If you are replacing a Server Edition Secondary, Server Edition Expansion System, or an Application Server, use the *Synchrosize Security* feature of Web Manager.
4. Validate status and configuration with vSphere Client console, Web Manager, IP Office Manager for Server Edition, and SSA.
5. Take a backup using Web Manager.
6. Using IP Office Manager for Server Edition, administer new local licenses, delete old.
Any local licenses becomes 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 security settings or configuration data do one of the following:

- If the onboarding.xml file is available, import the original onboarding.xml using Web Manager.

- If the onboarding.xml file is not available but the configuration data is available, restore the configuration and add the following certificate that expires in 2020 to IP Office's Trusted Certificate Store using IP Office Manager:

```
-----BEGIN CERTIFICATE-----
MIIGKTCCBRGgAwIBAgIQZBvoIM4CCBPzLU0tldZ
+ZzANBgkqhkiG9w0BAQUFADCBYjELMAkGA1UEBhMCMVVMxZzAVBgNVBAoTD1ZlcmlTaWduLCBjb250bWUwMR8wHQYDVQQL
LExzZWZlJmU2LnbiBUcnVzdCBOZXN3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBwZXJpU2lnbiwgSW5jLiAtIEZvcjB
hdXRob3JpemVkIHVzZSBvbnx5MUUwQWYDVQQDEzZWZlJmU2LnbiBDbGFzcyAzIFB1YmVzYyBQcm1tYXJ5IE5lcnR
pZmljYXRpb24gQXV0aG9yaXR5IC0gRzUwHhcNMTAwMjA4MDAwMDAwNmMjA3MjM1OTU5WjCBvDELMAkGA1U
EBhMCMVVMxZzAVBgNVBAoTD1ZlcmlTaWduLCBjb250bWUwMR8wHQYDVQQLLExzZWZlJmU2LnbiBUcnVzdCBOZXN3b3JrMTs
wOQYDVQQLEzJUZlZlJmU2LnbiBUcnVzdCBOZXN3b3JrMTs3d3cudmVyaXNpZ24uY29tL3JwYSAoYykgMDE2MDQGA1U
EAMtVmVyaVNPZ24gQ2xhc3MgMyBjb250bWUwMR8wHQYDVQQLLEzEoYykgMjAwNiBwZXJpU2lnbiBUcnVzdCBOZXN3b3JrMTs
FAAOCAQ8AMIIBCgKCAQEAmdacYvAV9IGaQqHjZjxOdF8mfUdzasVLv/+NB3eDfxCjG4615HycQmLi7IjfbKkERBD
+qqqFLPTU4bi7u1xHbZzFYG7rNVICreFY1xy1TIbxfNiQDk3P/
hwB9ocenHKS5+vDv85burJlSLZpDN9pK5MSSAvJ5s1fx+0uFLjNxC+kRLX/
gYtS4w9D0SmNNiBXNUpPyiHb5SgzoHRsQ7AlYhv/JRT9Cm
mTnprqU/
iZucff5NYAc1Pe712mDK4KTQzfZg0EbawurSmaET0q03n40mY5o1so5BptMs5pITRNGtFghBMT7oe2sLktiEuP7
TfbJUQABH/weaoEq0OC5T9YtRQIDAQABo4ICFTCCAHEwEgYDVR0TAQH/BAGwBgEE/
wIBADBwBgNVHSAEATBnMGUGC2CGSAGG
+EUBBxcDMFYwKAYIKwYBBQUHAQEWHGh0dHBzOi8vd3d3LnZlcmlzaWduLmNvbS9jcHMwKgYIKwYBBQUHAQIwHhoc
aHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYTAOBG9wOjBwZXN3b3JrMTs3d3cudmVyaXNpZ24uY29tL3JwYSAoYykgMDE2MDQGA1U
MFcwVRYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGGUj
+XTGoasjY5rwr8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVyaXNpZ24uY29tL3ZzbG9nb35naWYwNAYDVR0lB
C0wKwYIKwYBBQUHAwEGCCsGAQUFBWMCBglghkgBhvhCBAGCmCGSAGG
+EUBCAEwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBzABhhodHRwOi8vb2Nzc5Z2ZlJmU2Lnbi5jb20wNAYDVR0f
BC0wKzApoCegJYYjaHR0cDovL2Nybc5Z2ZlJmU2Lnbi5jb20vcGNhMy1nNS5jcmwwKAYDVR0RBCEwH6QdMBsGTAX
BgNVBAMTEFZlcmlTaWduTVBLSS0yLTcwHQYDVRO0BBYEFNebfNgi0BX3a1fzimbWMO8RgC1MB8GA1UdIwQYMBaA
FH/TZafC3ey78DAJ80M5+gKvMzEzMA0GCSqSIsIb3DQEBBQUAA4IBAQBxtX1zUkrdl000Ky6v1EalSVACT/
gvF3DyE9wfIYaqw98NzZURniuXXhv0bpavBCrWDbFjGIVRWAXIeLVQgh3oVXY
QwRR9m66SOZdTLD0z6k1dYzmp8N5td0lksVWmzWoxZTDphDzqS4w2Z6BVxiEOgbEtt9LnZq/9/XaxvMIsxxx
+rNAVnwzeneUW/ULU/sOX7xo+68q7jA3eRaTJX9NEP9X+79uOzMh3nnchhdZLUNkt6Zmh
+q81kYZGoaLb9e3SQBb260/KZru99MzrzqP0nkzKXmnUG623kHdq2FlveasB+1XwiiFm5WVu/
XzT3x7rfj8GkPsZC9MGAht4Q5mo
-----END CERTIFICATE-----
```

Chapter 13: Capacity planning

Introduction

This covers various aspects of Release 9.0 IP Office Server Edition capacity and performance that may have an influence on the design of a specific solution of a customer.

Read the following resources before you proceed with planning:

- The *IP Office Server Edition Solution Overview Guide* for the correct software release: This gives a high level view on deployment components and options along with detailed capacities and scalability tables.
- IP Office Technical Bulletins: Bulletins announce the general availability of new releases and their content. They can be found at: <http://marketingtools.avaya.com/knowledgebase/>
- IP Office Technical Tips: provide more detailed information on new features, changes to supported limits or potential issues. They can be found at: <http://marketingtools.avaya.com/knowledgebase/>
- Known caveats: These might indicate limitations of behaviour or errors in the published documentation. They can be found at: <http://marketingtools.avaya.com/knowledgebase/businesspartner/caveats/index.php>

The *IP Office Server Edition Solution Overview Guide* provides information about solution components, their capabilities and capacities sufficient to allow a high level design. Use this capacity planning section subsequently to qualify and refine the design.

The most complex single component to consider is generally Server Edition Expansion System (V2) because of the combination of VoIP with digital and analogue, and the flexibility of constructs.

The Linux components such as Server Edition Primary, Server Edition Secondary and Server Edition Expansion System (L) are VoIP only and single construct, help in deciding whether to move Avaya one-X[®] Portal for IP Office from Server Edition Secondary to a separate platform for capacity.

Server Edition Primary capacity planning

IP Office Server Edition Solution Overview Guide describes the planning for Server Edition Primary. Also review the following sections in this document to plan Server Edition Primary capacity.

Note:

Use HP DL360 server for Server Edition Primary when the total solution users or extensions exceed 1500.

Server Edition Secondary capacity planning

IP Office Server Edition Solution Overview Guide describes the planning for Server Edition Secondary. Also review the following sections in this document to plan Server Edition Secondary capacity.

*** Note:**

Use HP DL360 server for Server Edition Secondary when the total solution users or extensions exceed 1500.

Stand-alone Avaya one-X® Portal planning

IP Office Server Edition Solution Overview Guide describes the planning for Avaya one-X® Portal. Also review the following sections in this document to plan Avaya one-X® Portal capacity.

*** Note:**

The maximum supported total solution call rate is 7,200 BHCC when Avaya one-X® Portal users are active.

Planning Server Edition Expansion System (V2) capacity

When designing a IP Office Server Edition Solution that includes a Server Edition Expansion System (V2) you need to consider the following:

- Maximum trunk and extension capacity for every Server Edition Expansion System (V2)
- The VCM channel capacity for every Server Edition Expansion System (V2)
- The total concurrent VoIP call capacity of Server Edition Expansion System (V2)
- Call media destination location and type; both intermediate and final
- Direct or indirect VoIP media
- Multi-Site Network link capacities
- IP Infrastructure and VoIP QoS
- Trunk utilization and call traffic profile
- Resilience and failover

*** Note:**

You must assess all the factors listed because one factor can limit the other.

Related links

[Maximum extension capacity](#) on page 121

[Maximum trunk capacity](#) on page 121

[Concurrent VoIP Call Capacity](#) on page 122

[Maximum VCM Channel capacity](#) on page 123

[Call Media Type](#) on page 124

[Conference capacity](#) on page 124

[Voice recording](#) on page 125

[Voicemail](#) on page 126

[Multi-Site Network link capacities](#) on page 126

[Call media destination](#) on page 127

[IP Infrastructure, Bandwidth & VoIP QoS](#) on page 128

[Trunk utilization and call traffic profile](#) on page 128

[Resilience and Failover](#) on page 129

Maximum extension capacity

A single Server Edition Expansion System (V2) can support 384 users and up to:

- 384 Analogue extensions
- 384 Digital extensions
- 384 VoIP extensions (H.323, SIP or DECT R4)

The total may not exceed 384 extensions. The capacity of Analogue and digital extension is dependent on the hardware of the system unit. The following table lists the various constructs and the resulting maximum capacity:

*** Note:**

This table does not list all variants. Only the variants that provide the maximum capacity are listed.

Base Card #1	Base Card #2	Base Card #3	Trunk Card #4	Exp. Module #1-8	Exp. Module #9-12	Max Digital	Max Analogue	MaxVoIP
Phone 8	Phone 8	Phone 8	4 Port Exp	Phone 30	Phone 30	0	384	0
DS 8	DS 8	DS 8	4 Port Exp	DS 30	DS 30	384	0	0
						0	0	384

H323, DECT R4 and SIP extension capacity is also limited by available licenses.

Related links

[Planning Server Edition Expansion System \(V2\) capacity](#) on page 120

Maximum trunk capacity

A single Server Edition Expansion System(V2) can support up to:

- 204 Analogue trunks
- 8 E1/PRI Digital trunks with 240 channels
- 8 T1/PRI Digital trunks with 192 channels
- 16 BRI digital trunks with 32 channels
- 125 SIP trunks with 128 channels
- 2 H323/SCN trunks with 250 channels per trunk

Analogue and digital trunk capacity is dependent upon the hardware of the system unit. The following table shows the various constructs and the resulting theoretical maximum:

*** Note:**

All variants are not listed in the table. The maximum possible trunk channels that is listed can be supported, but other factors reduce what can be utilized on a concurrent basis.

Trunk Card #1	Trunk Card #2	Trunk Card #3	Trunk Card #4	Expansion Module #1-8	Expansion Module #9-12
Dual PRI	Dual PRI	Dual PRI	Dual PRI	ATM 16	
ATM 4	ATM 4	ATM 4	4 Port Exp	ATM 16	ATM 16
BRI 8	BRI 8	BRI 8	BRI 8	ATM 16	

*** Note:**

SIP and PRI trunk capacity is also limited by available licenses. The number of SIP trunk channel licenses requested by each system is defined by the **Maximum SIP Sessions** setting on the **System > Telephony** tab of Server Edition Manager.

Related links

[Planning Server Edition Expansion System \(V2\) capacity](#) on page 120

Concurrent VoIP Call Capacity

The concurrent call capacity between the digital or analog extensions and digital or analog trunks is non-blocking. All the extensions and trunks may be involved in the calls. Any VoIP calls do not affect the capacity. Server Edition Expansion System (V2) has a number of concurrent call capacities that can influence the design of IP Office Server Edition Solution :

Parameter	Value	Comment
Concurrent VoIP calls: direct media	384	Calls with direct media between VoIP endpoints or trunks
Concurrent VoIP calls: indirect media, IP500 V2 VCM	120	Calls between the VoIP and digital or analogue domain
Concurrent VoIP calls: indirect media, IP500 V2 RTP relay	120	Calls between VoIP endpoints or trunks that cannot go direct media, but do not require a VCM

These are not cumulative figures – for example a mix of two call types changes the capacity to a value between the two values. When the capacity exceeds the value, Server Edition Expansion System (V2) does not limit the number of concurrent calls and makes a best effort to service all. VoIP voice quality degrades as load increases; high overload conditions affect the performance of Server Edition Expansion System (V2) in general.

Concurrent call maximum capacity can be administered using Server Edition Manager in a number of ways to ensure that the limits are not exceeded.

- **Number of Channels** and **Outgoing Channels** setting in the **VoIP Line** tab of H323 trunks

- **Max Calls per Channel** setting in the **SIP URI** tab of SIP trunks
- **Call Admission Control** area of the **Location** settings

Related links

[Planning Server Edition Expansion System \(V2\) capacity](#) on page 120

Maximum VCM Channel capacity

Voice compression (VCM) channels enable Server Edition Expansion System (V2) to convert media. For example, media between analogue or digital and the Voice over IP (VoIP) domains. These are essential when routing trunk calls to or from VoIP endpoints.

It is important to note that media communication with any other Server Edition component requires the use of VoIP, including Server Edition Primary, Server Edition Secondary, other Server Edition Expansion Systems, call recording, attendants, IVR, conferencing and voicemail.

Three base card types provide VCM channel capacity for Server Edition Expansion System (V2) :

- VCM 32
- VCM 64
- Combination card

Each base card can carry a trunk module however the Combo card can only support BRI and analogue, hence if more than two dual PRI cards are required, the VCM capacity is reduced. Also note that the type of trunk module fitted to the Combo card is fixed. The following table shows various constructs and the resulting theoretical maximum:

*** Note:**

All the variants are not listed in the table. only the variants that provide the maximum capacity are listed.

Base Card #1	Base Card #2	Base Card #3	Base Card #4	Maximum G.711 calls	Maximum G.729 calls	Maximum G.723 calls	Maximum G.722 calls
VCM 64	VCM 64			128	120	88	120
VCM 64	VCM 64	Combo		138	130	98	130
VCM 64	VCM 64	Combo	Combo	148	140	108	140

The capacity listed in the table is for a bidirectional channel between a VoIP and an analogue or digital endpoint and assumes the calls are of the same codec type. Differing codec types can be supported at the same time; the lowest channel figure should be used for calculations. VCM channels are also used to play call progress tones to VoIP extensions and perform transcoding. Transcoding is used where the VoIP codec differs between two legs of a call; for example a VoIP endpoint supporting only G.729 calling a SIP trunk with just G.711a. This type of transcoding uses two VCM channels and should be avoided wherever possible. When the system runs out of VCM resources, Server Edition Expansion System (V2) manages this common resource as efficiently as possible but if there are insufficient at any one time:

- Outgoing calls are not connected (do not receive dial tone)
- Incoming calls queue up until a VCM channel is free

- Transfers cannot be made

*** Note:**

These events do not occur in calls that do not involve VoIP, or for VoIP direct media with a few caveats. For more information, see http://marketingtools.avaya.com/knowledgebase/businesspartner/ipoffice/mergedProjects/manager/index.htm?config_forms_system_vcm.htm

Related links

[Planning Server Edition Expansion System \(V2\) capacity](#) on page 120

Call Media Type

Where calls start and remain in the digital and or analogue domain, the VCM and VoIP capacities of Server Edition Expansion System (V2) are not affected. The base capacity remains 384 concurrent calls.

Where calls go between VoIP and digital or analogue domains within Server Edition Expansion System (V2) , the indirect media limit of 120 concurrent calls and VCM availability is applicable.

Where calls go between VoIP domains for example, SIP trunk to H.323 there are two options:

- Direct — does not use the routing engine of Server Edition Expansion System (V2) and hence the base capacity remains 384 concurrent calls. Direct media is a configurable parameter for VoIP trunks and extensions it is active by default.
- Indirect — occurs either where configured, or if direct media is not possible even if it is configured. Some of the reasons are:
 - VoIP traffic routed between the LAN1 and LAN2 interface
 - Unsuccessful codec negotiation including silence suppression, DTMF transport as well as basic codec support
 - VoIP endpoint does not support direct media

Related links

[Planning Server Edition Expansion System \(V2\) capacity](#) on page 120

Conference capacity

Each Server Edition Expansion System(V2) supports a local conference capability with a capacity of 128 conference parties. You can find further details at: <http://marketingtools.avaya.com/knowledgebase/businesspartner/ipoffice/mergedProjects/productdescription/index.html?ipofficeconferencingcapacity.htm>

A number of factors determine the location of the conference resource used:

- An ad hoc conference uses the conference capacity of the system on which you are logged in.
- Meet-me conference using the personal meet-me bridge uses the system on which you are logged in..

- Meet-me conference created by Voicemail Pro call flows, or the Conference meet-me shortcode feature uses the system on which the feature is invoked.

Server Edition Expansion System (V2) conferences exist in the digital domain; hence all VoIP parties including trunk or extension require a VCM channel for that duration

. Recording a conference requires an additional conference channel, as well as a VCM and SCN trunk channel as the recording destination is on Server Edition Primary or Server Edition Secondary during fail over. Neither IP Office nor Voicemail Pro can automatically link or move conference locations, but existing conferences are connected together.

When the conferences run out of resources, the system attempts to record calls, join or create conferences are rejected.

Related links

[Planning Server Edition Expansion System \(V2\) capacity](#) on page 120

Voice recording

Call recording uses a three party conference per recorded call.

Conference recording adds a further conference channel to an existing conference.

Each recording requires one licensed and available voicemail channel, a VCM and SCN trunk channel as the recording destination is on Server Edition Primary or Server Edition Secondary during a fail over.

Point of recording determines the location of conference resource:

- Incoming Call Route (ICR) is recorded at trunk
- User recording done at the location of the user
- System recording at the location of the system
- Conference recording at conference location.

The maximum supported voice recording call rate is 3,600 BHCC for Server Edition Expansion System (V2), 9,000 BHCC for Server Edition Expansion System (L).

The total solution voice recording channel capacity is determined by the number of licensed voicemail channels which can be up to 150. This is a common resource used by voicemail leave and collect operations.

When the system runs out of resources, further attempts to record calls or conferences will not be successful.

To ensure channel capacity is available for recordings, use the IP Office Manager for Server Edition settings *Voicemail Channel Reservation* on System | Voicemail tab of Server Edition Primary to reserve channels exclusively for recording.

The solution voice recording capacity is fixed at 333 hours total. This is separate from the voicemail recording capacity. Refer to Voicemail Pro documentation for more information.

When the system runs out of recording storage resources, attempts to record calls or conferences will not be successful and the system plays announcements accordingly.

Related links

[Planning Server Edition Expansion System \(V2\) capacity](#) on page 120

Voicemail

When you leave a voicemail for a user or hunt group, the system uses one licensed and available voicemail channel and an SCN trunk channel as the recording destination is on Server Edition Primary or Server Edition Secondary during fail over . If the source of the caller is digital or analog, the system requires an additional VCM channel.

Voicemail collect operation uses one licensed voicemail channel and an SCN trunk channel. If the destination of the caller is digital/ or nalog, the system requires an additional VCM channel on that Server Edition Expansion System (V2).

The total solution voicemail channel capacity is determined by the number of licensed or supported voicemail channels which can be up to 150 for the HP DL360 server or 75 for the HP DL120/Dell R210 server. This is a common resource used by call recordings, Auto-Attendants, Announcements and others .

When the system runs out of voicemail resources, calls continue to alert and do not switch to voicemail. Voicemail collect fails to connect to the Voicemail server. Calls to Attendants continue to alert. Text To Speech (TTS) will not be output during call flows.

Note:

The TTS channel capacity is 40.

To ensure voicemail channel capacity is available for voicemail collect and leave, use the IP Office Manager for Server Edition settings Voicemail Channel Reservation on System | Voicemail tab of Server Edition Primary to reserve channels exclusively for specific uses.

The solution voicemail capacity is fixed at 60 minutes per user or group mailbox. This is separate from the call recording capacity. Refer to Voicemail Pro documentation for more information.

When the system runs out of recording storage resources, voicemail leave operations will receive an announcement that the user/group's mailbox is full. Voicemail collect continues to function.

Related links

[Planning Server Edition Expansion System \(V2\) capacity](#) on page 120

Multi-Site Network link capacities

A multi-site network link is the internal H.323 SCN trunk connection between each component of Server Edition. The links are arranged in a star topology with Server Edition Primary at the centre or double star when a Server Edition Secondary is a component of Server Edition.

Regardless of direct/indirect media, VCM or codec used, a further capacity consideration is the Multi-site network links between all components of Server Edition. Each IP500 V2 or Linux link has a maximum capacity of 250 channels/calls. The maximum incoming and outgoing channels are independently configurable in IP Office Manager for Server Edition using the H323 Line | VoIP Line tab, and both lines have 20 channels by default.

This is per link, not a per system limit; for example a Server Edition Primary or Server Edition Secondary may have up to 250 concurrent calls to each Server Edition Expansion System. Due to the star topology of Server Edition calls between Server Edition Expansion System go through Server Edition Primary or Server Edition Secondary therefore these calls must also be taken into account when considering Multi-site network link capacity.

It is not possible to add additional multi-site network links – if the capacity is exhausted additional Server Edition Secondary or Server Edition Expansion Systems should be considered.

If the configured values exceed, additional outgoing calls can be routed through the ARS configuration providing an alternative route exists; additional incoming calls are automatically routed, again providing an alternative route exists. Alternative routes only exist when a Server Edition Secondary is present. If no alternative route, incoming calls remain ringing until a channel is free, outgoing calls indicate busy.

Related links

[Planning Server Edition Expansion System \(V2\) capacity](#) on page 120

Call media destination

When planning Server Edition Expansion System (V2) from a media perspective it is important to note that communication with any other Server Edition component uses VoIP and hence is limited by the media capacities. This includes:

- Calls to or from Primary/Secondary and other Expansions
- Call recording - one channel per recorded call
- Auto Attendants/IVR - one channel per call
- Conferencing when the conference focus is not the V2 Expansion - one channel per local member
- Local conferences involving remote users - one channel per remote member
- Voicemail leave and collect - one channel per VM caller
- Announcements - one channel per call when receiving announcements
- Centralized Music on Hold – one channel per central MOH source when playing to held calls

For all VoIP connections between systems, the codec used will be according to the H323/SCN trunk settings of those two nodes.

Consider intermediate destinations to ensure adequate capacity. For example a consultation call opens a secondary channel for the consultation while the initial call is still connected.

Lastly, any call on the H323/SCN trunk will take into consideration administered channel limits and Call Admission Control (CAC) if active. Please refer to the CAC documentation for behaviours when CAC limits are exceeded.

Related links

[Planning Server Edition Expansion System \(V2\) capacity](#) on page 120

IP Infrastructure, Bandwidth & VoIP QoS

It is not within the scope of this document to cover detailed aspects of Ethernet and IP infrastructure. A VoIP FAQ is included in *IP Office Product Description*, see: http://marketingtools.avaya.com/knowledgebase/businesspartner/ipoffice/mergedProjects/productdescription/index.html?whatisqualityofservice_.htm

An IP Office bandwidth calculator is also available at : <http://marketingtools.avaya.com/knowledgebase/tools/bandwidth/index.htm>

In addition to the network requirements for VoIP calls, additional bandwidth should be reserved for the corresponding inter-node signalling and management paths. This should any access via SSLVPN.

The following recommended minimum bandwidths should available:

Traffic	Recommended Minimum bandwidth	Comments
Inter-node Signalling/Status	128 kbit/s	Between Server Edition Primary, Server Edition Secondary and Server Edition Expansion Systems. No signalling directly between Server Edition Expansion Systems
One-X Portal CTI	96 kbit per call(or 192 kbit/s @ 7,200 BHCC)	Between one-X Portal server location and Server Edition Expansion System when one-X Portal server active
Web Management	1024 kbit/s	Between Web Manager computer and Server Edition Primary
IP Office Manager for Server Edition	256 kbit/s	Between IP Office Manager for Server Edition computer and each component of IP Office Server Edition Solution

Further network bandwidth may be required for SSA, SysMonitor, syslog or SNMP.

Related links

[Planning Server Edition Expansion System \(V2\) capacity](#) on page 120

Trunk utilization and call traffic profile

General Traffic Engineering is outside the scope of this document, however the following Server Edition specific factors should be considered:

- The maximum BHCC of a Server Edition Expansion System (V2) is 7,200

- The maximum BHCC of a Server Edition Expansion System (L) is 7,200
- The maximum BHCC of a Server Edition Primary (HP DL360) is 7,200 when Avaya one-X[®] Portal users are active or 18,000 when not.
- Avaya one-X[®] Portal users include: Web Client, Call Assistant, Outlook Integration, Lync Integration, one-X preferred Mobile Clients.
- Total solution BHCC must not exceed 7,200 BHCC when Avaya one-X[®] Portal users are active

Related links

[Planning Server Edition Expansion System \(V2\) capacity](#) on page 120

Resilience and Failover

If Server Edition resilience is supported and failover is active, various traffic and loadings can change and must be considered in the planning phase:

- If Server Edition Primary fails when Server Edition Secondary is present, the system routes all non-local Server Edition Expansion System calls, Voicemail, IVR and Auto Attendant to Server Edition Secondary
- If Server Edition Primary fails when Server Edition Secondary is present, the system moves Hunt group processing and management access to Server Edition Secondary. This increases the management bandwidth from Server Edition Secondary to Server Edition Expansion Systems.
- The total number of extensions or users on Server Edition Secondary or Server Edition Primary must not exceed 1500. For a 2000 user solution a Server Edition Secondary should be present and Server Edition Expansion System extension backup should be configured to split the load between the two servers

Related links

[Planning Server Edition Expansion System \(V2\) capacity](#) on page 120

Planning Server Edition Expansion System (L) capacity

When designing a Server Edition Solution that includes a Server Edition Expansion System (L), the aspects that are covered for Server Edition Expansion System (V2) also need to be assessed, with the following differences:

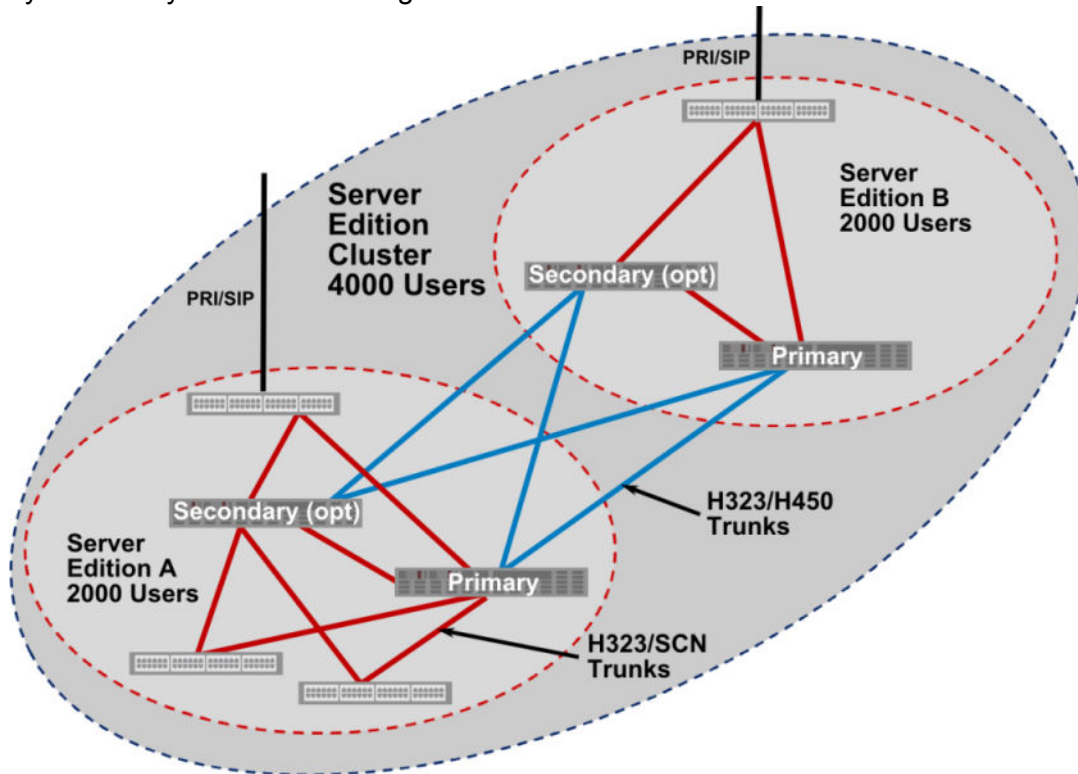
- Maximum extension capacity for each Server Edition Expansion System (L)
 - No digital or analog extensions
 - Maximum users/extensions 500, except DECT R4 which is 384
- Maximum trunk capacity for each Server Edition Expansion System (L)
 - No digital or analog trunks
 - Maximum SIP channels 256 total

Capacity planning

- The concurrent call capacity of Server Edition Expansion System (L)
 - No analog or digital calls
 - Indirect media capacity 128
 - Direct media capacity 500
- The VCM channel capacity for each Server Edition Expansion System (L)
 - Only transcoding is relevant; 128 channels
- Call media type
Same as Server Edition Expansion System(V2)
- Conference Capacity
 - The conference capacity is the same as Server Edition Expansion System (V2)
 - The conference engine is VoIP, hence no VCM channels are required
- Voice recording
 - The maximum supported voice recording call rate is 9,000 BHCC for a Server Edition Expansion System (L)
- Voicemail
 - Same as Server Edition Expansion System (V2) , except no VCM channels are required
- Multi-Site Network link capacities
Same as Server Edition Expansion System (V2)
- Call media destination
Same as Server Edition Expansion System (V2)

Capacity planning for over 2000 users

To provide a cost effective solution of more than 2000 users to larger customers, two Server Edition systems may be connected together to form a *Cluster* with a total of 4000 users or extensions.



You can create a cluster is achieved by creating two separate Server Edition systems, then cross connecting using H.323 + H.450 trunks to provide the appearance to users of a single system.

Each Server Edition system has its own Server Edition Primary and Applications, and optional Server Edition Secondary and Server Edition Expansion Systems; each Server Edition system needs to be managed separately. The systems are set up through configuration to share a common dial plan and directory.

Feature	Server Edition	SE Cluster	Notes
Maximum users or extensions	2000	4000	2000 per system
Directory	Single directory	Common directory with manual synchronisation between the two systems	Can use auto synchronisation for system directory
Directory Size	5000	5000	
Dial Plan	Single dial plan	Single dial plan	example. 21xxxx is on A and 22xxxx is on B

Table continues...

Trunk Sharing across nodes	Yes	Yes	Requires additional ARS and ICR setup
Dial by name	Yes	Yes	Requires common directory
Hold/Transfer	Yes	Yes	
Internal dialling and calling user name	Yes	Yes	
Direct Media	Yes	Yes	
Busy and Presence Indicators	System Wide	Limited to local SE	
Hot Desking	System Wide	Limited to local SE	Partial resolution with multiple accounts
Hunt Groups	Fully Networked	Partially Networked	Hunt groups are limited to an SE system but can be linked between systems
Music On Hold	4 per node, either local or from Primary	4 per node, either local or from local Primary	Cannot stream MoH from other Primary
SMDR	Single stream per node	Single stream per node	
Voicemail	Single	Single VM per SE	
One-X Portal	Single	Single one-X server per SE	
SCN telephony features	System Wide	Limited to local SE	

Inter Server Edition link

- The links between the two Server Edition systems are achieved using H323 trunks with the following recommended settings:
 - Supplementary Services: H450
 - Allow Direct Media Path: Active
 - Out Of Band DTMF: Active

One trunk should be added between each Server Edition Primary and each Server Edition Secondary. This allows calls from one system to appear as though internally dialled on the other.

Directory

To enable users of one system to be visible in the directory of the other, each directory of Server Edition Primary configuration requires a copy of the other system:

- Export users of each component as CSV using IP Office Manager for Server Edition.
- Extract Full Name and Extension fields from each file into a single CSV directory file. See the following for more information on the file formats: http://marketingtools.avaya.com/knowledgebase/businesspartner/ipoffice/mergedProjects/installation/index.htm?importing_and_exporting_settings.htm
- Hunt groups or common system directory entries can also be added to the directory file at this time if required.

- Import the resultant CSV directory file into the other Server Edition Primary only using IP Office Manager for Server Edition.
- The centralized system directory mechanism distributes to all other components.

If an external LDAP directory is also used, one Server Edition Primary can be configured with the LDAP source, and the other using the first as the HTTP source. Care should be taken not to exceed the various directory capacities. For more information on directory options and capacities: http://marketingtools.avaya.com/knowledgebase/businesspartner/ipoffice/mergedProjects/manager/index.htm?centralized_system_directory.htm

Dial plan

Each user and hunt group of the cluster must have a unique name and number. Branch prefix should not be used as this conflicts with the internal routing.

Outgoing Call routing

The default outgoing call routing provides a fall-back ARS on every Server Edition Expansion System to Server Edition Primary then Server Edition Secondary . When creating a cluster it is recommended that a further fall-back ARS is added between each Server Edition Primary each Server Edition Secondary . PSTN/SIP trunks on one system can be accessed from the other using ARS and/or dial short codes, along with additional Incoming Call Routes.

Hunt Groups

Each Server Edition system has separate hunt groups. It is not possible to configure hunt groups with members of both systems. It is possible to support limited overflow between systems by the use of an overflow group with local users that have hunt group call forwarding enabled to a remote user. This is only supported on rotary and sequential ring types and must not be used to link hunt groups.

Administration

Each Server Edition system is managed as a separate entity although both solutions can be managed from the same workstation if required.

Versions or Upgrades

Both Server Edition systems should be the same software version. Each should be upgraded separately from the associated Server Edition Primary server .

Chapter 14: Troubleshooting

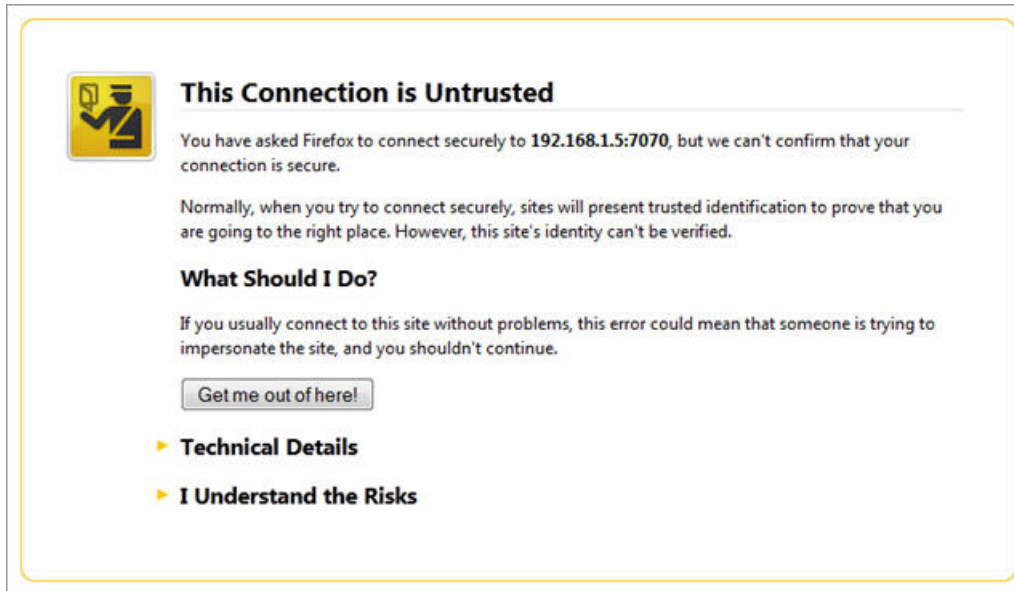
Warning message

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

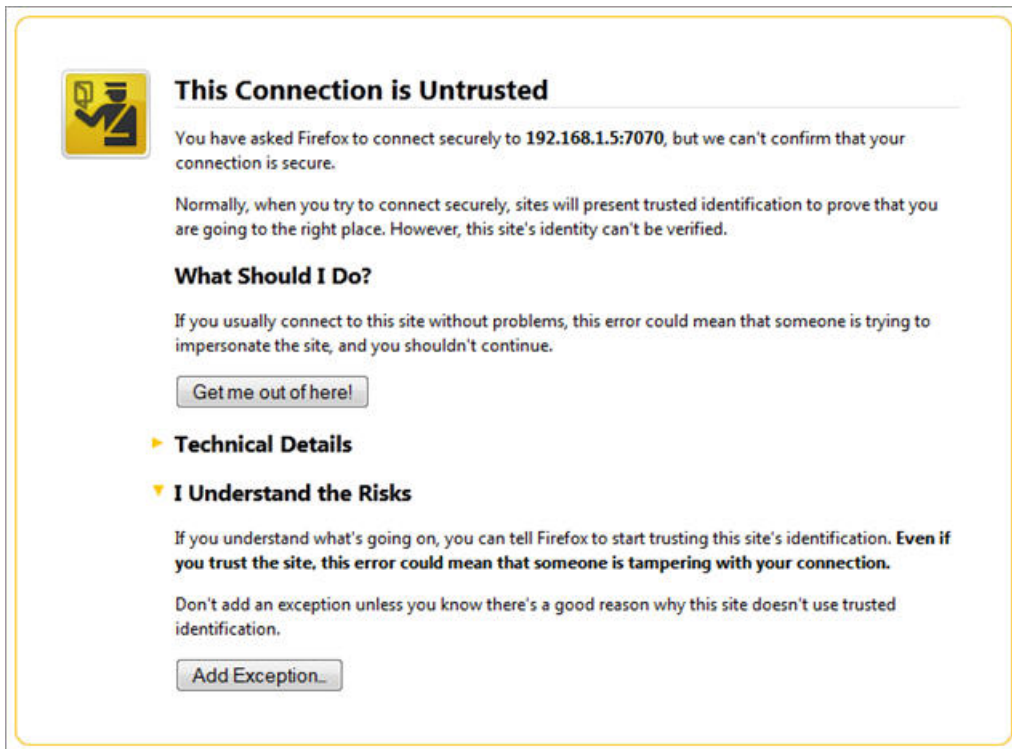
This Connection is Untrusted

*** Note:**

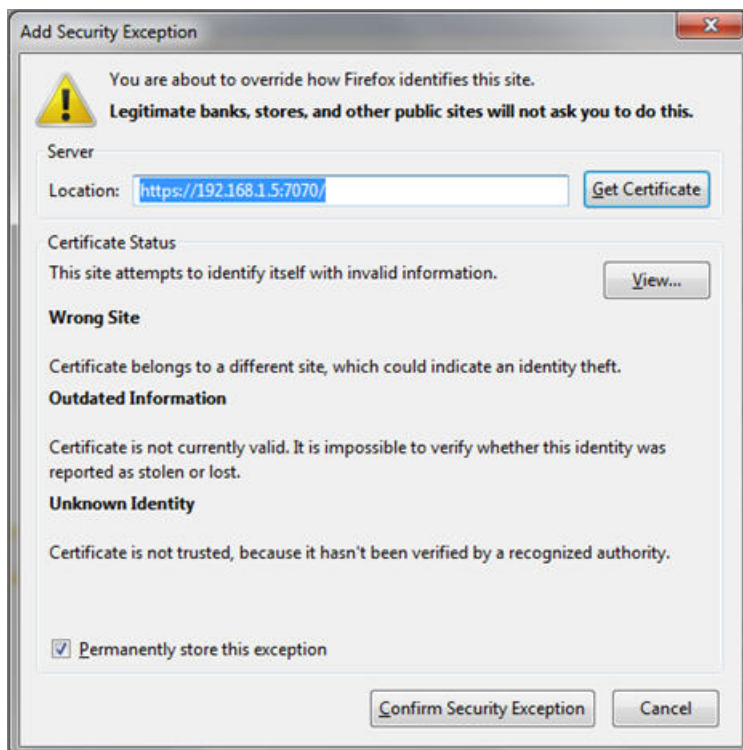
These are the images that the system displays when you open a Firefox browser.



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*.

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 Edition Manager.

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

Solution:

Ensure that there is a bidirectional IP connectivity from IP Office Server Edition Manager 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 System is 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 System is the member of Administrator rights group.
- Ensure that there is a bidirectional connectivity from Server Edition Primary server to Server Edition Expansion System and Server Edition Secondary server for the TCP ports 8443 and 9080.

Debugging steps

This section 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 138
- [Checking memory usage](#) on page 139
- [Checking the version of Linux OS](#) on page 141
- [Downloading the log files](#) on page 69
- [Viewing the log files](#) on page 67

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>`

```
*****
*          IP Office for Linux          *
*                                     *
*      WARNING: Authorised Access Only  *
*****

Welcome Administrator it is Wed Jun 13 05:05:03 BST 2012
> admin
Please enter password:
Admin> root
Password:
[root@localhost ~]#
```

Related links

[Debugging steps](#) on page 137

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. For more information, see [Viewing system information](#) on page 65.

Before you begin

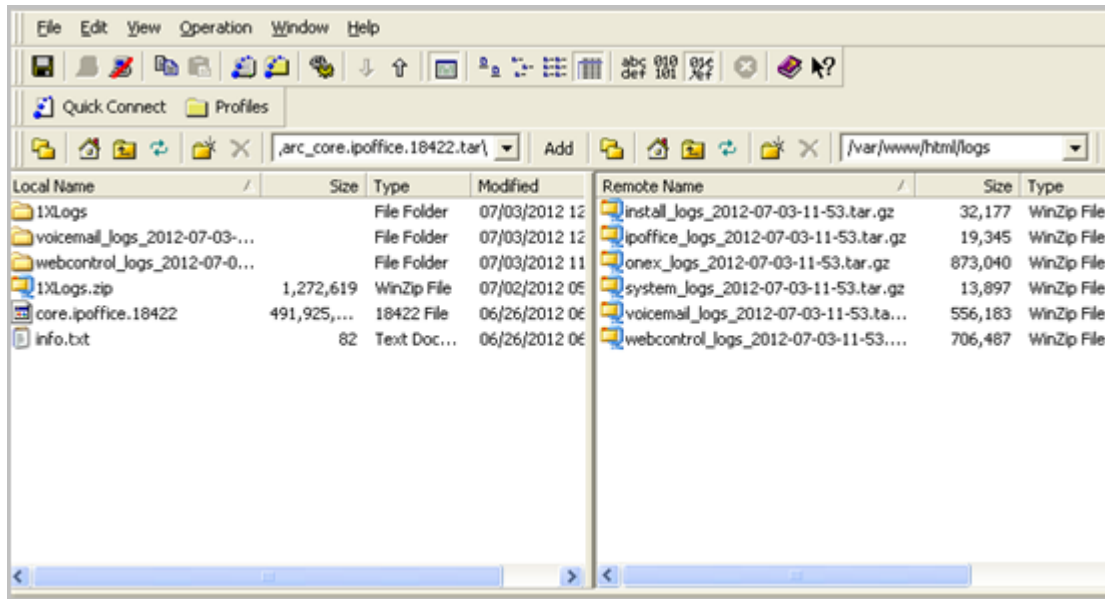
Log in as *Administrator* using SSH Secure File Transfer client

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
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 [kssoftirqd/0]
    0 [migration/0]

```

Related links

[Debugging steps](#) on page 137

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 138.

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 137

IP Office Server Edition certificates

IP Office Server Edition server 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. The following table lists the components that support identity certificates:

Component	Comment
IP Office Management	Administer via IP Office Manager
IP Office Telephony	Can be the same as IP Office Management
One-X Portal Client Server	When HTTPS enabled
One-X Portal Presence Server	
Web Management	Only HTTPS enabled
Web Control	Linux platform management Only HTTPS enabled

Default identity certificates

Server Edition default certificates, are in most cases entirely unsecure, but they are essential to allow initial provisioning.

The following table lists the default identity certificates when an IP Office system is first started:

Component	Component	Security Value
IP500 V2	<p>Unique, self-signed, created on initial start-up</p> <p>Secure but not trusted by anything else (e.g. your browser).</p> <p>Name on the certificate is "ipoffice-nnnnnnnnnn.avaya.com" where 'nnnnnnnnnn' is the LAN1 mac address</p>	Some
IP Office for Linux	<p>Unique, self-signed, created on initial start-up</p> <p>Secure but not trusted by anything else (e.g. your browser).</p> <p>Name on the certificate is "ipoffice-nnnnnnnnnn.avaya.com" where 'nnnnnnnnnn' is the LAN1 mac address</p>	Some
Web Management	<p>Hard-coded, common to all instances, insecure in every way.</p> <p>The name on the certificate is 'ipoffice-default.avaya.com'</p>	None
Web Control (Linux platform management)	<p>Hard-coded, common to all instances, insecure in every way.</p> <p>The name on the certificate is 'ipoffice-default.avaya.com'</p>	None

Table continues...

One-X Portal web server	Hard-coded, common to all instances, insecure in every way. The name on the certificate is 'ipoffice-default.avaya.com'	None
One-X Portal presence server	Hard-coded, common to all instances, insecure in every way. The name on the certificate is 'ipoffice-default.avaya.com'	None

Administering identity certificates

New identity certificates must be administered on Web Manager, Web Control, Avaya one-X[®] Portal and Voicemail Pro for any level of security. The IP Office certificate can be securely copied using Web Manager or Web Control, to all other web servers such as Web Manager, Web Control, Avaya one-X[®] Portal and Voicemail Pro on that server. This feature can be used to copy the default certificate or a new one. See, Web Manager > Platform > Settings > General > Web Control.

* Note:

If Web Manager detects that the IP Office and other web servers differ, the system displays a warning.

You can add an identity certificate to IP Office in a number of ways:

- Added through an IP Office Manager using one obtained from a certificate authority
- Default the security settings which creates another unique, self-signed instance with same name but differing instance
- Obtained automatically from a Certificate Authority (CA) via the Simple Certificate Enrolment Protocol (SCEP)

PKI and trust domains

IP Office Server Edition does not support PKI authorization and trust domains.

Identity Certificates and Browser Access

If the identity certificate offered by Web Manager is untrusted by that browser, it can be typically accepted as a security exception. However different browsers treat the default certificates differently:

- Mozilla Firefox allows permanent acceptance for each server
- Microsoft Internet Explorer 9 allows permanent acceptance for each server
- Google Chrome warns every time

Furthermore, opening up Linux Platform settings from Web Management is in fact another session – which, when coupled with the default certificates, causes further problems of access. This can be alleviated for FireFox and Internet Explorer by using the Launch in new tab feature of Web Manager.

To provide trusted and warning-free browser access, the identity certificate administered on IP Office and copied to the other components should be derived from a 'root' CA certificate trusted by the browser; in addition the name on the identity certificate should reflect the IP address or domain name for that server; use the Alternate name field to include other LAN1, LAN2 and domain names.

The H323 phones do not automatically register back to the Primary 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. The system temporarily logs the users of the H323 phones logged on the Primary server to the Secondary server. However, even after the Primary server is functional the users of the H323 phones remain logged on the Secondary server.

Solution

To ensure that the H323 phone users are logged back to the Primary server, reset the H323 phones.

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 90.

Users configured on Server Edition Expansion System are disconnected from Avaya 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.

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

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.

Index

A

administering one-X Portal	80
administrator	90
Administrator	89 , 91
AFA	78
alarms	58
audience	
deployment	
automatic	
default paramaters	23
install	23
upgrade	107

B

backup	79 , 84 , 94
backup and restore policy	96

C

call media destination	127
call traffic	
trunk utilization	128
capacity planning	119
certificates	141
change history	9
conference capacity	124
configuration data	46
configurations	
offline	136
upload	136
configure	77
custom folder	87

D

data sets	97
debug	137
deploying	11
deployment	
audience	
document purpose	9
downgrade	101
download	69

E

error	144
expansion system	40 , 43 , 44
capacity	120
expansion system,	

users	76
expansion system (L)	42
capacity	129
expansion system (V2)	40
extension	56

F

failed server	
restore	99

H

Hunt Group	57
------------------	--------------------

I

identity certificates	142
ignition process	24
infrastructure	
Bandwidth	128
VoIP QoS	128
Initial configuration utility	34
install	15 , 19
Voicemail Pro	82
Install	
automatic	14
intended audience	9
IP Office Server Edition Manager	53
ISO download	103

L

LAN support	61
license	54
Linux Platform	59
local server	108
location	97
lockout	136
log files	67
logging in	83
login	138

M

Manager	33 , 112
media type	124
memory	139
migrate	85
multi-site network	126

O

offline	137
on board	70
one-X Portal	73 , 76 , 79
operating system	53
over 2000 users	131

P

password	90 , 91
platform	
system	65
Platform	90
primary server	12 , 94
purpose of document	9

R

related documents	10
remove	39 , 43
replace	
FRU	115
IP500 V2	114
Linux server	115
SD card	114
resilience	55
failover	129
H323	144
restart	113
restore	79 , 85 , 98
restoring	86
revision history	9
root user	90

S

secondary server	37 , 39
shut down	112 , 113
SIP phones	144
solution management	32
SSA	74
SSLVPN	
IPOSS	
restore	117
support	
contact	10
synchronize passwords	92
syslog	68
syslog records	69
system information	65
systems	
system	65

T

template	58
templates	57
trunk capacity	121

U

untrusted connection	134
upgrade	103 , 106 , 109
automatic	14
web manager	104
upgrade policy	100
USB	12
manual	13
user	72

V

VCM Channel capacity	123
version	141
Virtual server	117
VLAN	60
voicemail	84 , 85
voicemail capacity	126
Voicemail Pro	82
Voicemail Pro client	73
voice recording capacity	125
VoIP call capacity	122

W

warning banner	70
Web Manager	52
Administrator	89 , 91