



Deploying IP Office™ Platform Server Edition Solution

Release 9.1
Issue 02.14
December 2015

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

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

For full support, please see the complete document, *Avaya Support Notices for Hardware Documentation*, document number 03–600759.

For full support, please see the complete document, *Avaya Support Notices for Software Documentation*, document number 03–600758.

To locate this document on our website, simply go to <http://www.avaya.com/support> and search for the document number in the search box.

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.

“Hosted Service” means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON

BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

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 computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

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

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

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

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use 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 You a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner

would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: <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.

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

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	10
Purpose.....	10
Intended audience.....	10
Document changes since last issue.....	10
Related Resources.....	10
Documentation.....	10
Training.....	12
Viewing Avaya Mentor videos.....	12
Product compatibility.....	13
Additional resources.....	13
Support.....	14
Accessing Avaya DevConnect Application Notes.....	14
Deploying an IP Office Server Edition Solution.....	15
Chapter 2: Installing IP Office Server Edition server	17
Server Edition Primary server.....	17
Creating an installation USB drive.....	17
Creating an installation USB drive for manual installation or upgrade.....	18
Creating an installation USB drive for automatic installation.....	19
Creating an installation USB drive for automatic upgrade.....	19
Starting Web Manager.....	20
Installing IP Office Server Edition server manually.....	20
Installing IP Office Server Edition automatically	23
Default parameters.....	24
Configuring IP Office Server Edition using the ignition process.....	24
Starting IP Office Manager.....	28
Configuring the IP Office Server Edition server using IP Office Manager.....	29
Chapter 3: Provisioning Server Edition Secondary server	31
Server Edition Secondary server.....	31
Adding a Secondary server.....	31
Removing a Secondary server.....	32
Chapter 4: Provisioning a Server Edition Expansion System	34
Server Edition Expansion System.....	34
Server Edition Expansion System (V2) versus Server Edition Expansion System (L).....	34
Adding a Server Edition Expansion System (V2).....	36
Adding a Server Edition Expansion System (L).....	38
Removing an expansion system.....	39
Chapter 5: Converting a Standard Mode IP500 V2 System to Server Edition	41
Converting an IP500 V2 System Using the ICU.....	41
Manually Converting an IP500 V2 System.....	43

Converting an IP500 V2 to a Server Edition Expansion System (V2).....	47
Converting an IP500 V2 to a Server Edition Primary Server	47
Converting an IP500 V2 to a Server Edition Expansion System (L).....	49
Chapter 6: Configuring IP Office Server Edition Solution	51
IP Office Server Edition Solution.....	51
IP Office Server Edition LAN support.....	51
Adding a license.....	55
Activating resilience.....	56
Adding a user.....	57
Adding an extension.....	57
Adding a hunt group.....	58
Creating a template.....	59
Applying a template.....	59
Configuring alarms.....	60
Configuring the Linux Platform settings.....	61
Configuring a VLAN.....	61
Viewing system information.....	62
Configuring warning banner, alarms, and log files.....	64
On boarding.....	68
Starting Applications.....	69
Starting Avaya one-X [®] Portal for IP Office	69
Starting Voicemail Pro client	69
Starting SSA.....	70
Chapter 7: Configuring Avaya one-X[®] Portal for IP Office	72
Configuring Avaya one-X [®] Portal for IP Office users.....	72
Configuring IP Office Server Edition systems in Avaya one-X [®] Portal for IP Office	72
Configuring administration access for Avaya one-X [®] Portal for IP Office	73
Initializing AFA login for Avaya one-X [®] Portal for IP Office	74
Backing up and restoring one-X Portal.....	75
Backing up Avaya one-X [®] Portal for IP Office.....	75
Restoring Avaya one-X [®] Portal for IP Office.....	75
Administering a separate Avaya one-X [®] Portal for IP Office.....	76
Chapter 8: Configuring Voicemail Pro	77
Configuring Voicemail Pro.....	77
Installing Voicemail Pro client.....	77
Logging into Voicemail Pro server.....	78
Backing up and restoring voicemail.....	79
Backing up Voicemail Pro.....	79
Restoring Voicemail Pro stored on IP Office Server Edition server.....	80
Migrating Voicemail Pro to IP Office Server Edition.....	80
Chapter 9: Configuring passwords	84
Changing the Administrator password using Web Manager	84
Changing the Administrator password using Linux Platform settings.....	85

Changing the root user password.....	85
Changing the Security Administrator password for Server Edition server.....	86
Changing the passwords of common configuration Administrator	87
Chapter 10: Backup and restore.....	89
Backup overview.....	89
Backup and restore policy.....	89
Backup and Restore location.....	90
Backup data sets.....	91
Disk Usage.....	92
Managing Disk Space for Backup and Restore.....	93
Backing up an IP Office Server Edition server.....	94
Restoring an IP Office Server Edition server.....	95
Restoring a failed IP Office Server Edition server.....	96
Chapter 11: Upgrading.....	98
Server Edition upgrade policy.....	98
Server Edition downgrade policy.....	99
Upgrade Process Summary.....	100
Upgrade Procedures.....	101
Downloading ISO using Web Manager.....	101
Upgrading using Web Manager.....	102
Upgrading the system using an installation DVD or USB drive.....	104
Upgrading the system automatically.....	105
Upgrading or changing the version of an application on a local server using Linux Platform settings.....	106
Chapter 12: Shutting down a system.....	108
Shutting down a Server Edition Expansion System (V2) using IP Office Manager.....	108
Shutting Down a Linux Server Using Web Manager.....	108
Shutting down a Linux server using Linux Platform settings.....	109
Chapter 13: Changing the IP Address of a Server Edition Server.....	110
Changing the IP Address of the Primary Server.....	110
Changing the IP Address of a Secondary or Expansion Server.....	111
Chapter 14: Replacing the hardware of IP Office Server Edition.....	112
Replacing IP500 V2 system.....	112
Replacing System SD Card.....	112
Replacing an IP 500 V2 Field Replacable Unit.....	113
Replacing a Linux server.....	113
Restoring SSLVPN or IPOSS.....	115
Chapter 15: Capacity Planning.....	116
Primary and Secondary Server Capacity Planning.....	118
Maximum Extension, User, and Site Capacity.....	119
Maximum Trunk Capacity.....	120
Server Concurrent Call Capacity.....	121
Call Media Path.....	122

Avaya one-X® Portal Server Capacity Planning.....	123
IP500 V2 Expansion System Capacity Planning.....	124
Maximum Extension/User Capacity.....	124
Maximum trunk capacity.....	125
Concurrent Call Capacity.....	126
VCM Channel Capacity.....	128
Call Media Path.....	130
Linux Server Edition Expansion System Capacity Planning.....	131
Conferencing Capacity Planning.....	132
Voicemail, Auto Attendant, and IVR Capacity Planning.....	133
Voice Recording Capacity Planning.....	134
Multi-Site Network Link Capacity Planning.....	135
Call Destination Server.....	136
IP infrastructure, bandwidth, and VoIP Quality of Service.....	137
Call Traffic Profile.....	138
Resilience and Failover.....	139
Startup and Availability.....	140
Capacity planning for over 3000 users.....	140
Chapter 16: Troubleshooting.....	144
Warning message.....	144
Unable to login. IP Office is under Server Edition Manager Administration.....	146
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.	146
All systems appear online in IP Office Server EditionManager, but appear offline on the Linux Platform settings of the primary server.	147
Debugging steps.....	147
Logging in as a root user.....	148
Checking memory usage.....	149
Checking the version of Linux OS.....	151
IP Office Server Edition certificates.....	151
Identity certificates.....	152
After failback, the H323 phones do not automatically register back to the original server.....	152
Unable to export template.....	152
Solution.....	152
Users configured on Server Edition Expansion System are disconnected fromAvaya one-X® Portal for IP Office when the system starts registering SIP phones.....	153
Changing a System Configuration from Select to Non-Select.....	153
Chapter 17: Appendix A: Certificate Text.....	154

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 installation and upgrade procedures have been updated for release 9.1.

Related Resources

Related links

- [Documentation](#) on page 10
- [Training](#) on page 12
- [Viewing Avaya Mentor videos](#) on page 12
- [Product compatibility](#) on page 13
- [Additional resources](#) on page 13

Documentation

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

- *Deploying Avaya IP Office™ Platform Server Edition Servers as Virtual Machines*
- *Administering Avaya IP Office™ Platform with Manager*
- *Administering Avaya IP Office™ Platform with Web Manager*
- *Administering Avaya IP Office™ Platform Voicemail Pro*
- *Administering Avaya one-X® Portal for IP Office™ Platform*
- *Deploying Avaya one-X® Portal for IP Office™ Platform*
- *Deploying Avaya IP Office™ Platform Voicemail Pro*
- *Deploying Avaya IP Office™ Platform SSL VPN Services*
- *Avaya IP Office™ Platform Solution Description*
- *Avaya IP Office™ Platform Security Guidelines*

Related links

[Related Resources](#) on page 10

[Finding documents on the Avaya Support website](#) on page 11

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at <http://support.avaya.com/>.
2. At the top of the screen, enter your username and password and click **Login**.
3. Click **Documents**.
4. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
5. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
6. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
7. Click **Enter**.

Related links

[Documentation](#) on page 10

Training

Avaya training and credentials are designed to ensure our Avaya Business Partners have the capabilities and skills to successfully sell, and implement, and support Avaya solutions and exceed customer expectations. The following credentials are available:

- Avaya Certified Sales Specialist (APSS)
- Avaya Implementation Professional Specialist (AIPS)
- Avaya Certified Support Specialist (ACSS)

Credential maps are available on the Avaya Learning website at www.avaya-learning.com

The following courses are available on the Avaya Learning website. After logging in to the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title
10S00005E	Knowledge Collection Access: SMB Implementation Only AIPS – Avaya IP Office (AIPS – 4000) Curriculum and Online Test
5S00004E	Knowledge Collection Access: SMB Support Only ACSS – SME Communications (ACSS – 3000) Curriculum
0S00010E	Knowledge Collection Access: SMB Implementation and Support AIPS – Avaya IP Office (AIPS – 4000) Curriculum and Online Test plus ACSS – 3000 Curriculum
2S00012W	APSS – Small and MidMarket Communications – IP Office™ Platform 9.1 and 9.1 Select – Overview
2S00013W	APSS – Small and MidMarket Communications – IP Office™ Platform 9.1 and 9.1 Select – Core Components
2S00014W	APSS – Selling IP Office™ Platform 9.1 and 9.1 Select
2S00010A	APSS – Selling IP Office Assessment

Included in all Knowledge Collection Access offers above is a separate area called IP Office Supplemental Knowledge. This floor in the Virtual Campus contains self-directed learning objects which cover IP Office 9.1 delta information. This material can be consumed by technicians well experienced in IP Office and only need this delta information to be up to date.

Related links

[Related Resources](#) on page 10

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

 **Note:**

Videos are not available for all products.

Related links

[Related Resources](#) on page 10

Product compatibility

For the latest and most accurate compatibility information go to <https://support.avaya.com/CompatibilityMatrix/Index.aspx>.

Related links

[Related Resources](#) on page 10

Additional resources

You can find information at the following additional resource websites.

Avaya

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

Avaya Enterprise Portal

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

Avaya IP Office Knowledge Base

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

Avaya maintenance, lifecycle and warranty information

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

Avaya Community

<http://www.aucommunity.com> is the official discussion forum for Avaya product users.

Non-Avaya websites

There are several web forums that discuss IP Office. Refer to these websites for information about how IP Office is used. Some of these forums require you to register as a member. These are not official Avaya-sponsored forums and Avaya does not monitor or sanction the information provided.

- Tek-Tips: <http://www.tek-tips.com>
- CZ Technologies IP Office Info: <http://ipofficeinfo.com>
- PBX Tech: <http://www.pbxtech.info/forumdisplay.php?f=8>

Related links

[Related Resources](#) on page 10

Support

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

Related links

[Accessing Avaya DevConnect Application Notes](#) on page 14

Accessing Avaya DevConnect Application Notes

The Avaya DevConnect program conducts testing with service providers to establish compatibility with Avaya products.

Procedure

1. Go to http://www.devconnectprogram.com/site/global/compliance_testing/application_notes/index.gsp.
2. Sign in or register.

3. Click a timeframe to search within.

Under **2014**, click **Q1: January — March**.

A list of all the application notes for that timeframe appears.

4. In the **Search** field, type `IP Office` and press **Enter**.

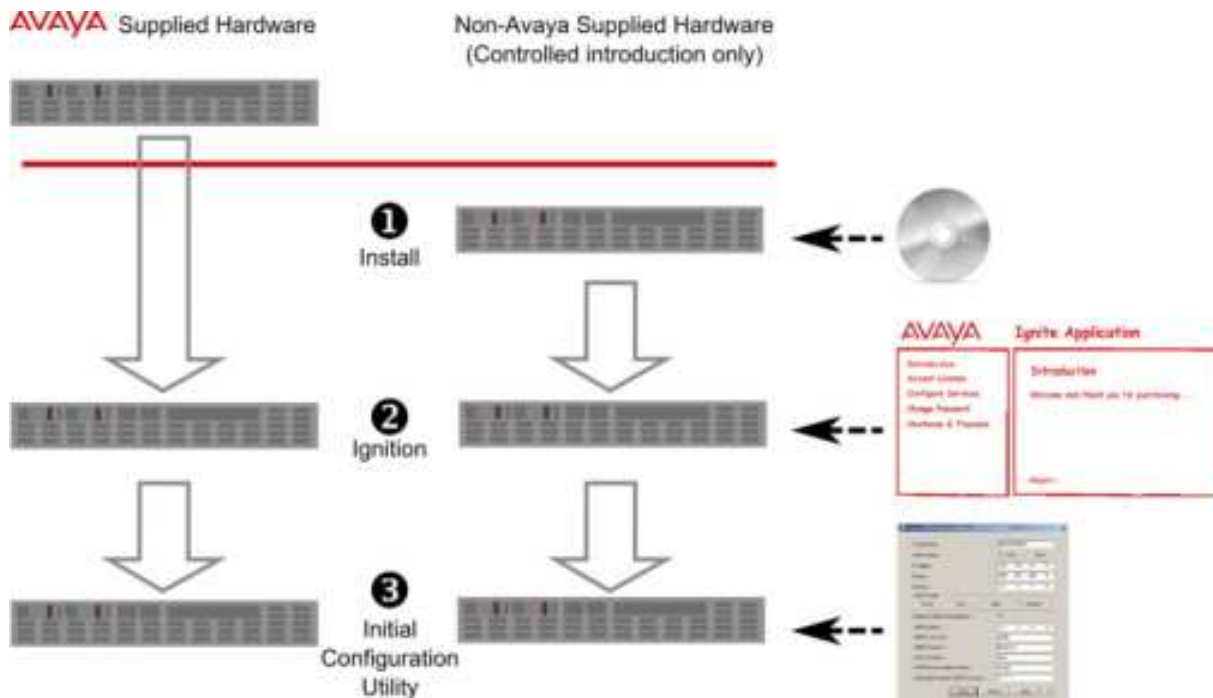
A list of relevant Application Notes appear.

Related links

[Support](#) on page 14

Deploying an IP Office Server Edition Solution

About this task



* Note:

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

*** Note:**

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

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

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

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 Server Edition on a supported server.
2. Configure the role of the server using the ignition process.
3. Configure the server using the Initial Configuration Utility.
4. Add the optional components such as a Server Edition Secondary server and a Server Edition Expansion System.
5. Upgrade to the latest IP Office Server Edition software release if a new version is available.
6. Add the licenses for a Server Edition Secondary and Server Edition Expansion System.
7. Administer the various components using IP Office Web Manager and IP Office Manager.

Chapter 2: Installing IP Office Server Edition server

Server Edition Primary server

The primary server is the only hardware component that you need to deploy an IP Office Server Edition Solution. The primary server manages all the components of an IP Office Server Edition Solution, as and when you scale up.

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

Creating an installation USB drive

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 must create a new 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>.

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**.

Next steps

Set up the USB drive for manual or automatic installation.

Related links

[Creating an installation USB drive for manual installation or upgrade](#) on page 18

[Creating an installation USB drive for automatic installation](#) on page 19

[Creating an installation USB drive for automatic upgrade](#) on page 19

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 17.

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 17

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 17

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 17

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 17.

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 17

Starting Web Manager

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

Web Manager is supported on the following browsers.

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

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

Before you begin

You must have the IP address of IP Office Server 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.

Installing IP Office Server Edition server manually

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

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

Before you begin

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

Procedure

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

*** Note:**

To restart a Server Edition server, always use Web Manager. For more information, see [Restarting a Server using Web Manager](#) on page 108. For a new installation, power cycle the server.

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

*** Note:**

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

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

The system prompts you to install or upgrade. If you are installing Server Edition on a server in which Server Edition is already installed, then the system displays the details of the applications that are already installed. The system also displays the details of the applications that the system will install.

11. Select **Install** if you want the system to replace the applications that are already installed.
12. Click **Next**.
13. Do one of the following:
 - Select **Yes** if you want to continue with the installation.
 - Select **Advanced** if you want to configure addition settings such as hardware partitioning.
14. Click **Next**.
15. Type the name of the IP Office Server Edition server in the **Hostname** field.

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

16. Click **Configure Network**.

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

 **Note:**

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

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

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

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

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

- Connection name: System eth1
- IP address: 192.168.43.1
- Netmask: 255.255.255.0
- Gateway: 0.0.0.0

19. Click **Close** to close the **Network Connections** window.
20. Click **Next**.
21. Type the password for the root user in the **Root Password** field.
22. Retype the password in the **Confirm** field.

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

23. Click **Next**.

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

24. Click **Next**.

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

25. Click **Next**.

The system displays an option to install TTS language packs

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

27. Click **Next**.

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

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

Related links

[Adding a Secondary server](#) on page 31

[Adding a Server Edition Expansion System \(L\)](#) on page 38

[Adding a Server Edition Expansion System \(V2\)](#) on page 36

[Adding a license](#) on page 55

[Configuring IP Office Server Edition systems in Avaya one-X Portal for IP Office](#) on page 72

Installing IP Office Server Edition automatically

You can install Server Edition automatically using the installation USB drive. The system automatically configures the default parameters during the installation. For more information, see [Default parameters](#) on page 24

*** Note:**

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

Before you begin

You need the following:

- IP Office Server Edition installation USB drive. For more information, see [Creating an installation USB for automatic installation](#) on page 19.

Procedure

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

*** Note:**

To restart Server Edition server, always use Web Manager. For more information, see [Restarting a Server using Web Manager](#) on page 108. For a new installation, turn off the power supply to the server.

The system restarts and boots from Server Edition installation USB.

*** Note:**

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

Default parameters

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

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

Language for installation	US English
Keyboard for the system	US English
Hostname	MAC_HOSTNAME: : 00:AE:EF:00:00:00
System eth0	<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 Application Server.

 **Note:**

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

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

*** Note:**

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

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

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

About this task

To start the ignition process:

Procedure

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

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

2. Log in as *root*.

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

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

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

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

*** Note:**

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

6. Click **Next**.

The system displays information for additional hardware. The page is populated when an additional hard disk is added to be used when running Contact Recorder for IP Office on the server.

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

7. Click **Next**.

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

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

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

9. In the **Time & Companding** page:

a. Select **Use NTP**.

*** Note:**

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

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

*** Note:**

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

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

c. Click **Next**.

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

*** Note:**

The following account passwords are synchronized.

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

- Setting the IP Office Administrator account password also sets the same password for the Linux Administrator user account.
- To change the existing passwords:
 - a. Type a password in the **New Password** field.
 - b. Retype a password in the **New Password (verify)** field.

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

*** Note:**

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

- c. Click **Next**.

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

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

*** Note:**

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

- To automatically generate a certificate, select **Generate CA automatically** and then click **Next**.
- To import a certificate, perform the following.
 - a. Select **Import CA**.
 - b. Click **Browse**, navigate to the certificate location and select the file.
 - c. Click **Upload**.
 - d. In the **Password** field, enter the password for the certificate.

12. Click **Next**.

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

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

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

*** Note:**

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

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

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

15. Click **Apply**.

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

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

Next steps

Start IP Office Manager.

Starting IP Office Manager

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

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

* Note:

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

Before you begin

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

Procedure

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

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

Result

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

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

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

Next steps

Do one of the following:

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

Configuring the IP Office Server Edition server using IP Office Manager

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

Before you begin

Start Manager.

Procedure

1. Start Manager and log on as **Administrator**.
2. Click **File > Advanced > Initial Configuration**.

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

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

- a. Set the **System Type** as **Server Edition Primary**, **Server Edition Secondary**, or **Server Edition Expansion**.

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

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

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

Do not select Hosted Deployment for non-hosted systems.

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

- e. Set the default telephony and language settings for the system in the **Locale** field.
- f. Set the device IP of the system in the **Services Device ID** field.

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

- g. Select the LAN interface for the system in the **LAN Interface** section. In the LAN Interface field, select the LAN interface for the system.
- h. Set the IP address of the server in the **IP Address** field.
- i. Set the IP mask address of the server in the **IP Mask** field.
- j. Set the gateway address of the server in the **Gateway** field.
- k. Set **DHCP Mode**. In the DHCP Mode area, select the appropriate option.
- l. Type the IP address of the Server Edition Secondary server in the **Server Edition Secondary** field.
- m. Type the IP address of the DNS server in the **DNS Server** field.
- n. Click **Save** to save the configuration details that you set for the system.

The system reboots.

Chapter 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 users, IP trunking, and conference channels. The secondary server provides resilience to the users, phones, hunt groups and voicemail configured on the primary server. The secondary server also provides resilience to the users and phones configured on an expansion system. The secondary server is the management access point when the primary server is offline.

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

 **Note:**

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

For information on capacity, see [Capacity Planning](#) on page 116.

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, then you can skip this step and proceed to [Configuring using the ignition process](#) on page 24.
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 38

[Adding a Server Edition Expansion System \(V2\)](#) on page 36

[Installing IP Office Server Edition server manually](#) on page 20

[Adding a license](#) on page 55

[Configuring IP Office Server Edition systems in Avaya one-X Portal for IP Office](#) on page 72

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. Server Edition Expansion System (V2) supports both analogue, TDM and IP networks 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).

Related links

[Server Edition Expansion System \(V2\) versus Server Edition Expansion System \(L\)](#) on page 34

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

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

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

Table continues...

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

Table continues...

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

Related links

[Server Edition Expansion System](#) on page 34

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.
 - If you have purchased a pre-installed Server Edition server, perform this procedure to ensure you have the latest version of the software installed.
 - If you are converting an existing IP500 V2 system, see [Converting an IP500 V2 System](#) on page 41.
2. Set the role of the server as *Expansion* server in the ignition process.
3. Start Manager.
4. Configure the server using the Manager initial configuration utility (ICU)

You can also configure the server using the initial configuration utility of 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 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 31

[Adding a Server Edition Expansion System \(L\)](#) on page 38

[Installing IP Office Server Edition server manually](#) on page 20

[Adding a license](#) on page 55

[Configuring IP Office Server Edition systems in Avaya one-X Portal for IP Office](#) on page 72

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 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 31

[Adding a Server Edition Expansion System \(V2\)](#) on page 36

[Installing IP Office Server Edition server manually](#) on page 20

[Adding a license](#) on page 55

[Configuring IP Office Server Edition systems in Avaya one-X Portal for IP Office](#) on page 72

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:**

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

Chapter 5: Converting a Standard Mode IP500 V2 System to Server Edition

Related links

[Converting an IP500 V2 System Using the ICU](#) on page 41

[Manually Converting an IP500 V2 System](#) on page 43

[Converting an IP500 V2 to a Server Edition Expansion System \(V2\)](#) on page 47

[Converting an IP500 V2 to a Server Edition Primary Server](#) on page 47

[Converting an IP500 V2 to a Server Edition Expansion System \(L\)](#) on page 49

Converting an IP500 V2 System Using the ICU

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

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

Configuration Area	Retain Configuration Data	
	Off	On
System	Numerous changes to: <ul style="list-style-type: none">• Licensing• LAN1/2• DHCP• DNS• Directory	Numerous changes, same as default

Table continues...

Converting a Standard Mode IP500 V2 System to Server Edition

Configuration Area	Retain Configuration Data	
	Off	On
	<ul style="list-style-type: none"> • Voicemail • Auto user/ extrn. • Time • Server Edition Flag • Syslog 	
Line	<ul style="list-style-type: none"> • All IP trunks removed • IP Office trunks added 	All previous IP Office trunks removed IP Office trunks added
Control Unit	No	No
Extension	<ul style="list-style-type: none"> • IP extensions deleted • Analog/digital extensions un-numbered 	No changes
User	All users deleted	No changes
Group	All groups deleted	No changes
Short codes	All feature short codes deleted except on Primary	No changes
Service	No changes	No changes
RAS	No changes	No changes
ICR	Delete all	No changes
WAN Port	No changes	No changes
Directory	Delete all except on Primary	No changes
Time Profile	All time profiles deleted	No changes
Firewall Profile	No changes	No changes
IP Route	Add gateway route	Add gateway route
Account Code	Delete all	No changes
License	Delete all	No changes
Tunnel	No changes	No changes
User Rights	All user rights deleted	No changes
E911	E911 extension list deleted	No changes
ARS	Add default entry for primary/secondary	Add default entry for primary/secondary
Location	Delete all	No changes
Authorization Code	No changes	No changes
Security Settings	Configuration, Security and Web Services security level Medium	Configuration, Security and Web Services security level Medium
Call log	No changes	No changes
DHCP allocation	No changes	No changes

Related links

[Converting a Standard Mode IP500 V2 System to Server Edition](#) on page 41

Manually Converting an IP500 V2 System

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

*** Note:**

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

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

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

Table continues...

Configuration Area	Migration allowed	Potential migration issues	Manager Detect/ Correct?	Comments
		<ul style="list-style-type: none"> Duplicate user extensions. CCR Agent settings 	<ul style="list-style-type: none"> Yes 	<ul style="list-style-type: none"> Resolvable in Manager
Group	Yes	Non network advertised groups not supported	Yes	Non network advertised groups cannot be resolved.
Short codes	Yes	<ul style="list-style-type: none"> Existing global short codes are no longer global. Existing Call routing 	<ul style="list-style-type: none"> Varies Yes 	<ul style="list-style-type: none"> Any common feature short code that is not part of the migrated configuration will disappear from the top level but is resolvable in SE manager. If Manager is in Consolidated mode, a prompt to harmonize to the Primary common items is offered. Resolvable in Manager.
Service	Yes V2 Expansion only	Linux only supports the SSLVPN service	Yes	Only for IP500 V2 to V2 Expansion System migrations.
RAS	Yes V2 Expansion only			Only for IP500 V2 to V2 Expansion System migrations. No Linux support
ICR	Yes	Existing global ICRs are no longer global.	Varies	Any common feature short code that is not part of the migrated configuration will disappear from the top level but is resolvable in SE manager. If Manager is in Consolidated mode, a prompt to harmonize to the Primary common items is offered.
WAN Port	Yes V2 Expansion only	No Linux support.		Only for IP500 V2 to V2 Expansion System migrations.
Directory	Yes	Expansion directory entries cannot be deleted.	Yes	Use CSV export/import to migrate to Primary.

Table continues...

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

Table continues...

Converting a Standard Mode IP500 V2 System to Server Edition

Configuration Area	Migration allowed	Potential migration issues	Manager Detect/ Correct?	Comments
E911	No	No support.	No	Enhanced 911 not supported.
ARS	Yes	Existing Call routing	No	Resolvable in Manager
Location	Yes	Existing global locations stop being global.	Varies	Manager allows per system locations. Any that map to common locations will make that user right disappear from the top level but it is resolvable in Manager. If Manager in Consolidated mode, a prompt to harmonize to the Primary common items is offered.
Authorization Code	Yes			
Security Settings	Yes V2 Expansion only	Can only migrate using SD card. ICU may not work if PKI trust domain active.	Yes	PC running ICU must be in PKI trust domain. May have to be changed manually if security settings extensively modified.
Call log	Yes V2 Expansion only		No	Internal configuration file on SD Card mapped to users. Not deleted on upgrade or change of mode from Standard to Server Edition.
DHCP allocation	Yes V2 Expansion only		No	Internal configuration file on SD Card containing DHCP allocations. Not deleted on upgrade or change of mode from Standard to Server Edition.

Related links

[Converting a Standard Mode IP500 V2 System to Server Edition](#) on page 41

Converting an IP500 V2 to a Server Edition Expansion System (V2)

The supported conversion areas are:

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

Before you begin

You must have:

- the correct target software version installed
- valid configuration data

Procedure

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

Related links

[Converting a Standard Mode IP500 V2 System to Server Edition](#) on page 41

Converting an IP500 V2 to a Server Edition Primary Server

The supported Configuration conversion areas are:

- Trunks, except analogue/digital
- Extensions, except analogue/digital
- Users
- Groups, except non-advertised
- Short Code
- Incoming Call Route
- Time Profile

- Account Code
- User Rights
- Location
- Authorization Code

The following Configuration areas are not supported:

- Security settings
- Call logs
- DHCP allocations

Before you begin

You must have:

- the correct target software version installed
- valid configuration data

Procedure

1. Back up the configuration before making any changes.
2. Run the ICU on the Server Edition Primary server.
3. Read the IP500 V2 configuration into IP Office Manager.
4. Use IP Office Manager to delete analogue/digital trunks/extensions and any other entries not required.
5. Convert any hunt groups to network advertised.
6. Save as offline file in case of errors.
7. Use CSV or binary export to extract required areas of configuration to local files. Do not use the whole configuration option.
8. Use IP Office Manager to read the Server Edition Primary server configuration.
9. Use CSV or binary import to include required areas.
10. Manually update any System attributes required.
11. Resolve all warnings and errors before saving to the Server Edition Primary server.
12. Save to the Server Edition Primary server.
13. Review and test the resulting configuration.
14. Back up the configuration.

Related links

[Converting a Standard Mode IP500 V2 System to Server Edition](#) on page 41

Converting an IP500 V2 to a Server Edition Expansion System (L)

The supported Configuration conversion areas are:

- Trunks, except analogue/digital
- Extensions, except analogue/digital
- Users
- Groups, except non-advertised
- Short Code
- Incoming Call Route
- Time Profile
- Account Code
- User Rights
- Location
- Authorization Code

The following Configuration areas are not supported:

- Security settings
- Call logs
- DHCP allocations

Before you begin

You must have:

- the correct target software version installed
- valid configuration data
- ICU run on Linux Expansion

Procedure

1. Back up the configuration before making any changes.
2. Read the IP500 V2 configuration into IP Office Manager.
3. Use IP Office Manager to delete analogue/digital trunks/extensions and any other entries not required.
4. Convert any hunt groups to network advertised.
5. Save as offline file in case of errors.
6. Use CSV or binary export to extract required areas of configuration to local files. Do not use the whole configuration option.
7. Use IP Office Manager to read the Server Edition Expansion System (L) configuration.

Converting a Standard Mode IP500 V2 System to Server Edition

8. Use CSV or binary import to include required areas.
9. Manually update any System attributes required.
10. Resolve all warnings and errors before saving to Linux Expansion.
11. Save to Server Edition Expansion System (L).
12. Review and test the resulting configuration.
13. Back up the configuration.

Related links

[Converting a Standard Mode IP500 V2 System to Server Edition](#) on page 41

Chapter 6: 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 Manager and IP Office Web Manager to manage and configure additional settings. Refer to

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

 **Warning:**

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

IP Office Server Edition LAN support

 **Warning:**

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

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

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

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

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

- A One-X Portal client cannot listen to voicemail messages.

- You cannot launch the Server Edition Manager and other clients from Web Control.
- External MAPI and SMTP voicemail servers cannot be accessed via LAN2.

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

Feature	IP500 V2 LAN1	IP500 V2 LAN2	Linux LAN1	Linux LAN2	Notes
Interface Layer1 - Layer4					
Interface Support	Yes	Yes	Yes	Yes	
Physical<>logical interface mapping	Fixed: 'LAN'	Fixed: 'WAN'	Yes	Yes	
Speed	10/100	10/100	10/100/ 1000	10/100/ 1000	
Duplex	Full/half	Full/half	Full/half	Full/half	
802.1Q VLAN support	No	No	Yes	Yes	Static o/g VLAN assignment via administration IP500 V2 strips any received VLAN tag, all o/g packets have no VLAN tag
DSCP/ToS	Yes	Yes	Yes	Yes	Linux LAN2 uses LAN1 DSCP settings – any LAN2 settings are ignored
Default gateway/route	Yes	Yes	Yes	Yes	Linux via ignition or Web Control
Proxy ARP	Yes	Yes	No	No	IP500 V2 acts as an L3 router
IP Multicast	Yes	Yes	No	No	
Inter LAN					
Firewall	Yes	Yes	Yes	Yes	A Linux ingress/egress firewall can be activated, with further controls for specific unsecure ports such as TFTP and HTTP. No differentiation between LAN1 and LAN1
IP Routes	Yes	Yes	No	No	No configurable IP routing between Linux LAN interfaces All received Linux LAN traffic that is not destined for the node is discarded except VoIP media which is allowed to traverse with NAT
NAT/NAPT	Yes	Yes	No	No	
PPP	Yes	Yes	Yes	No	
Clients					

Table continues...

Feature	IP500 V2 LAN1	IP500 V2 LAN2	Linux LAN1	Linux LAN2	Notes
1XP client – basic	n/a	n/a	Yes	Yes	
1XP client – VM listen	n/a	n/a	Yes	No	
One-X Mobile Preferred	n/a	n/a	Yes	Yes	
One-X Mobile Preferred – VM listen	n/a	n/a	Yes	No	
Avaya Communicator	Yes	Yes	Yes	Yes	
One-X Plugins	n/a	n/a	Yes	Yes	
SoftConsole	Yes	Yes	Yes	Yes	
VMPPro – MAPI Link	n/a	n/a	Yes	Yes	Two way MS Exchange VM Integration via MAPI or EWS
VMPPro – SMTP	n/a	n/a	Yes	No	One way IMAP/Exchange VM integration
Administration					
IP Office Manager	Yes	Yes	Yes	Yes	Also accessible via IPOSS remote tunnel (SSLVPN)
Server Edition Manager	Yes	Yes	Yes	Yes	Access should be the same LAN1/2 interface as the inter-node connections Also accessible via IPOSS remote tunnel (SSLVPN)
SSA	Yes	Yes	Yes	Yes	Also accessible via IPOSS remote tunnel (SSLVPN)
SysMon	Yes	Yes	Yes	Yes	Also accessible via IPOSS remote tunnel (SSLVPN)
Web Manager	Yes	Yes	Yes	Yes	Cannot launch other clients (including Manager and Linux Platform Management) when not accessed via LAN 1 Also accessible via IPOSS remote tunnel (SSLVPN)
VMPPro Client	n/a	n/a	Yes	Yes	Also accessible via IPOSS remote tunnel (SSLVPN)
Linux Platform Management	n/a	n/a	Yes	Yes	Was Web Control in Server Edition Release 8.1 Also accessible via IPOSS remote tunnel (SSLVPN)
Admin launch from Web Manager	n/a	n/a	Yes	Yes	Launch of IP Office Manager, SSA, Voicemail Pro client,

Table continues...

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

Table continues...

Feature	IP500 V2 LAN1	IP500 V2 LAN2	Linux LAN1	Linux LAN2	Notes
					access LAN2 registrar via LAN1
H.323 Remote worker phone	Yes	Yes	Yes	Yes	
IP DECT	Yes	Yes	Yes	Yes	
SIP trunks	Yes	Yes	Yes	Yes	
SIP phones	Yes	Yes	Yes	Yes	
STUN	Yes	Yes	Yes	Yes	
IP Office Softphone	Yes	Yes	Yes	Yes	
Avaya Communicator Essential	Yes	Yes	Yes	Yes	

Adding a license

Before you begin

1. Start IP Office Manager.
2. Get one IP Office Server Edition license for Server Edition Primary and Server Edition Secondary, and one license for each Server Edition Expansion System (L) and Server Edition Expansion System (V2). 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. License keys are unique strings based on features that are activated and the unique identity of the system. The unique identity of the IP500 V2 expansion system is the Feature Key serial number and the System ID for a Linux system.

Procedure

1. In the navigation pane, select the system for which you want to add the license.
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. In the License Key field, type the license key.
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.

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 31

[Adding a Server Edition Expansion System \(L\)](#) on page 38

[Adding a Server Edition Expansion System \(V2\)](#) on page 36

[Installing IP Office Server Edition server manually](#) on page 20

[Configuring IP Office Server Edition systems in Avaya one-X Portal for IP Office](#) on page 72

Activating resilience

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.

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 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 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 also add users using the auto create feature in IP Office Manager.

For information on capacity, see [Capacity Planning](#) on page 116.

Before you begin

Log in to Web Manager as Administrator.

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.

Adding an extension

An extension is associated with a base extension or 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.

You can also add extensions using the auto create feature in IP Office Manager.

For information on capacity, see [Capacity Planning](#) on page 116.

Before you begin

Start IP Office 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.
4. Click **OK**.

Result

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

Adding a hunt group

You can add a maximum of 300 hunt groups in an IP Office in a Cloud Environment with a maximum of 3000 users across these hunt groups. In each hunt group, you can add a maximum of 750 users.

Before you begin

Start IP Office Manager.

About this task

Add a hunt group using IP Office Manager. 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 also set the order in which calls are presented to the users.

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 about the configuration settings for the 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

Before you begin

Start IP Office Manager.

About this task

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.

Procedure

1. In the navigation pane, select the profile that you want to create.
2. Right-click the profile and select **New**.
3. In the detailed pane, enter the details of the profile that you selected.

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

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

The default location is `C:\Program Files\Avaya\IP Office\Manager\Manager_files\template`.

Applying a template

Before you begin

1. Start IP Office 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

Use this procedure to apply the templates that you created for the profiles using IP Office Server Edition Manager. 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.

Procedure

1. In the navigation pane, select the profile that you want to create.
2. Right-click the profile, and select **New from Template (Binary)**.

3. Select the template that you want 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

The components of IP Office in a Cloud Environment forward the alarms using Syslog to the 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 Manager.

Before you begin

Start IP Office Manager.

About this task

Use the following steps to configure alarms using IP Office Manager.

The system reports events occurring on the various IP Office applications and 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 the following:

- Events and alarms to include
- Method of reporting to use, such as SNMP, Syslog, or Email
- 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.

Procedure

1. In the navigation pane, click **System**.
2. Click the **System Events** tab.
3. In the **Configuration** tab, type the configuration details.
4. In the **Alarms** tab, add the destination for the events.

For more information about the fields and configuration settings, see “System events” in the *IP Office Manager* document.

5. Click **OK**.

Configuring the Linux Platform settings

Before you begin

1. Start Web Manager.

Or, 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

Use this procedure to configure the Linux Platform settings for an IP Office in the Cloud Environment system using Web Manager. You can monitor and configure the log files and download and update the applications using the Linux Platform settings.

Procedure

1. Click **Platform**.

The system displays the Systems window.

2. In **Control Units**, click the IP Office Server Edition for which you want to set the Linux Platform settings.

Result

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

Note:

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

Related links

[Configuring a VLAN](#) on page 61

[Viewing system information](#) on page 62

Configuring a VLAN

Before you begin

Open IP Office Web Manager and navigate to **Platform Settings**.

About this task

Use this procedure to create a Virtual LAN (VLAN).

Procedure

1. Click **Settings > System**.

2. In the Network section, in the Network Interface field, click the network interface where you want to create a VLAN.
3. Click **Create Subinterface**.
The system displays the **Create New Subinterface** dialog box.
4. In the **VLAN Id** field, type the VLAN ID.
The VLAN ID 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.
6. Click **Create**.

Related links

[Configuring the Linux Platform settings](#) on page 61

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

[Configuring the Linux Platform settings](#) on page 61

[System](#) on page 62

System

Navigation: **Server Menu > Platform View > System**

The **System** page provides a status overview of the server. 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. You can also use the Start All and Stop All buttons.
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.

Table continues...

Field	Description
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.
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 62

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

[Configuring the Linux Platform settings](#) on page 61

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

[Configuring the Linux Platform settings](#) on page 61

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

[Configuring the Linux Platform settings](#) on page 61

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

[Configuring the Linux Platform settings](#) on page 61

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

[Configuring the Linux Platform settings](#) on page 61

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

[Configuring the Linux Platform settings](#) on page 61

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.

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

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

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

About this task

By default Avaya one-X[®] Portal for IP Office is installed on the Server Edition Primary server. To support additional users, you can install Avaya one-X[®] Portal for IP Office as a standalone server. For capacity information, see [Capacity Planning](#) on page 116.

Procedure

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

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

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

To ensure that the all users can use the services of Avaya one-X[®] Portal you need to configure all the Server Edition Expansion Systems and Server Edition 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 31

[Adding a Server Edition Expansion System \(L\)](#) on page 38

[Adding a Server Edition Expansion System \(V2\)](#) on page 36

[Installing IP Office Server Edition server manually](#) on page 20

[Adding a license](#) on page 55

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. n
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/onexpportal-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

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

Before you begin

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

Procedure

1. In the **Settings** tab select **General**.
2. In the **one-X Portal Settings** section clear **Use Local IP**.
3. Select **System > Services**.
4. Click **Stop** to stop the services of Avaya one-X® Portal for IP 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 8: Configuring Voicemail Pro

Configuring Voicemail Pro

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

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

About this task

Add 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 81

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 80

[Restoring Voicemail Pro not stored on IP Office Server Edition server](#) on page 81

[Backup and restore limitations](#) on page 82

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 80

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 80

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 80

Chapter 9: 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 the Services window.
2. Click **Preferences** .
The system displays the Preferences dialog.
3. Type the new password in the **Password** field.
4. Retype the new password in the **Confirm Password** field.

 **Note:**

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

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

5. Click **Save**.

Result

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

Changing the Administrator password using Linux Platform settings

Procedure

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

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

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

 **Note:**

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

You can configure the password complexity rules for IP Office *Administrator* account using IP Office Server Edition Manager. For more information, see the *Security Mode* section of the *IP Office Manager* document.

5. Retype the new password of the *Administrator* in the **Confirm Password** field.
6. Click **Ok**.

Next steps

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

Changing the root user password

Before you begin

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

About this task

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

Procedure

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

*** Note:**

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

3. Retype the password in the **Confirm New Password** field.
4. Click **Save**.

Changing the Security Administrator password for Server Edition server

Before you begin

Start IP Office Server Edition Manager.

About this task

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

*** Note:**

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

To change the password:

Procedure

1. Select **File >Advanced > Security Settings**.
2. In the Select IP Office window select the server for which you want to change the *Security Administrator* password.
3. Click **OK**.
4. Type the name of the *Security Administrator* in **Service User Name** field.
5. Type the password of the *Security Administrator* in **Service User Password** field.
The default user name is *security* and password is *securitypwd*.
6. Select **General** in the navigation pane.
7. In the **Security Administrator** section, click **Change**.
8. Type the current password of the *Security Administrator* in the **Old Password** field.
9. Type the new password of the *Security Administrator* in the **New Password** field.
10. Retype the new password in the **Re-Enter Password** field.
11. Click **OK**.

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

Changing the passwords of common configuration Administrator

Before you begin

Note:

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

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

About this task

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

Procedure

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

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

To use different user name and password for each of the selected systems, clear **Use above credentials for all remaining, selected IPOs**.

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

Next steps

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

Chapter 10: Backup and restore

Backup overview

Related links

- [Backup and restore policy](#) on page 89
- [Backup and Restore location](#) on page 90
- [Backup data sets](#) on page 91
- [Disk Usage](#) on page 92
- [Managing Disk Space for Backup and Restore](#) on page 93

Backup and restore policy

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

The following IP Office Server Edition aspects must be considered as part of such a policy:

- Ignition settings. These must 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. If not saved earlier, this file can be retrieved from the file system:
 - IP500 V2: `primary\ws\onb\onb_<date>T<time>.xml`
 - Linux: `system\ws\onb\onb_<date>T<time>.xml`
- License key data: All ADI and PLDS license key files must 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 – Server Edition Primary server and Application Server only
- Periodic configuration backup for Voicemail Pro – Server Edition Primary server only

- Periodic voice mailbox and recording data backup – Server Edition Primary server only
- The timing of backup operation: This should be done when little or no traffic is present on the target system(s), but the backup process itself is not service-affecting.
- The timing of restore operation: This should be done when no traffic is present on the restored system(s). 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 that backup of an Avaya Linux server does not include any locally-stored backup data. For example, if using the Server Edition Primary server as a backup destination for an Expansion, then performing a backup of the Server Edition Primary server will not create a backup of the whole solution; only the Server Edition Primary servers’s data will be saved.
- Security of backup data communication
- Backup prior to and after any software upgrade; in general it is not possible to restore backup data set onto a different software version.
- Backup prior to and after any hardware upgrade.

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 (plus a single manual backup instance), after which the oldest set is overwritten. These instances are per backup server and regardless of the backup data set; for example two weekly separate backup tasks of all IP Office configurations and Voicemail configuration will overwrite the first set after 7 weeks.

Related links

[Backup overview](#) on page 89

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. Disabled by default. [1]
HTTPS	5443	/avaya/backup	none	HTTPS supported by all IP Office components. Enabled by default.
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)	Enabled by default.
SCP	22	/var/www/html/avaya/backup	Any service user with WebControl Admin rights, Root (not recommended)	SCP supported by Linux-based components. Enabled by default.

1. To enable HTTP, use the Web Control application. Go to **Settings > System > HTTP Server** and select the check box for **Enable HTTP file store for backup/restore**.

*** Note:**

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

Related links

[Backup overview](#) on page 89

Backup data sets

The following table provides information about the backup data sets:

Data Set	Content	Notes
IP Office Configuration (V2)	<ul style="list-style-type: none"> • Configuration • Security Settings • DHCP Allocations • Call log 	When selected for IP500 V2 Expansion systems
IP Office Configuration (L)	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Voicemail Pro server preferences • Call flows 	
Messages & Recordings	<ul style="list-style-type: none"> • Voice mailbox contents • Call recordings 	
Voicemail Pro Full	<ul style="list-style-type: none"> • Voicemail Pro server preferences 	

Table continues...

	<ul style="list-style-type: none"> • Call flows • Voice mailbox contents • Call recordings 	
Selective Voicemails		

Related links

[Backup overview](#) on page 89

Disk Usage

The tables below can be used to calculate the required disk space for backups.

Example:

A Server Edition deployment has 2500 users with 150 nodes and 500 hunt groups. The Primary Server is an R620 machine.

From the server disk usage table, the Primary Server occupies 170 GB of space. A solution backup requires 189 GB. The total is 359 GB.

Since the server disk capacity is 600 GB, the Primary Server has the capacity to act as the backup server.

Table 1: Server disk capacity

Server	R620	DL360	DL120	R210	OVA (default)	OVA (max supported) [1]
Nominal disk capacity (GB)	600	300	250	500	100	166
Max solution users	3,000	2,000	1,500	1,500	750	3,000

1. Requires disk size increase.

Table 2: Primary / Secondary / Expansion server disk usage

Solution	Max No. of users	100	750	1500	2000	2500
	Max No. of nodes	5	50	100	125	150
	Max No. of groups	20	150	300	400	500
Primary / Secondary max disk usage (no backup, one-X collocated) (GB)		75	100	130	150	170
Expansion max disk usage (no backup) (GB)		48	48	48	48	48

Table continues...

one-X standalone max disk usage (no backup) (GB)		49	49	49	49	49
Solution Max backup size (GB)	Configuration only	2	13	25	31	37
	All data	35	78	127	158	189

Table 3: Application Server disk usage

No. of VMPro users	20	50	100	150
No. of Hunt Groups	4	12	20	30
Application Server max disk usage (GB)	117	117	117	118
Max backup size config only (GB)	1	1	1	1
Max backup size all data (GB)	30	32	34	37

Related links

[Backup overview](#) on page 89

Managing Disk Space for Backup and Restore

Any Server Edition server can be used as a backup server, if there is sufficient disk space. The minimum available disk space required in order to use a Server Edition server or Application Server as a backup server is 60 GB or 120 GB if VMPro is installed. Information on the disk space available for backup is displayed in the Web Control application. On the **System** page, see **Quota available for backup data**.

You can use an Application Server solely as a backup server if the one-X Portal and Voicemail Pro applications are not installed. The disk capacity (total disk space) must be at least 60 GB.

*** Note:**

The backup and restore process uses the OS disk. The additional disk is for Contact Recorder only.

Using a virtual Server Edition machine as a backup server

To use a Primary, Secondary, or Application server as a backup server, you must increase the disk size or uninstall Voicemail Pro. For information on increasing the available disk size, see *Deploying Avaya IP Office™ Platform Server Edition Servers as Virtual Machines*.

A virtual Server Edition expansion system can be used as a backup server without increasing the disk size since by default, Voicemail Pro is not installed.

You can use an Application Server solely as a backup server if the one-X Portal and Voicemail Pro applications are not installed. The disk capacity (total disk space) must be at least 60 GB.

Related links

[Backup overview](#) on page 89

Backing up an IP Office Server Edition server

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

- You can schedule a backup, set the proxy, and a remote server using Web Manager **Solution Settings**.
- 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 the Web Manager menu bar, click **Solution**.
2. In the Solution page, select the component or components that you want to backup.
To select all the components, click the **Actions** check box .
3. Click **Actions** and select **Backup**.
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. Under **Proxy Settings**, enable **Use Proxy**.
 - c. In the **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. Under **Schedule Options**, enable **Use Schedule**.
 - c. In the **Select Schedule** list, select the schedule option that you created.
 - d. Set a **Start Date** and a **Start Time**.
 - e. To configure a recurring backup, set **Recurring Schedule** to **Yes** and then set the **Frequency** and **Day of Week**.
 - To backup the IP Office sets:
 - a. In the **Select Remote Server** drop down list, select the remote server that you have set.
 - b. In the **Select IP Office Sets** list, select the IP Office set that you want to backup.

- To backup one-X Portal sets:
 - a. In the **Select Remote Server** drop down list, select the remote server that you have set.
 - b. In the **Select one-X Portal Sets** list, select the one-X Portal set that you want to backup.
 - To backup Voicemail Pro sets:
 - a. In the **Select Remote Server** drop down list, select the remote server that you have set.
 - b. In the **Select Voicemail Pro Sets** list, select the Voicemail Pro set that you want to backup.
 - To backup Contact Recorder sets:
 - a. In the **Select Remote Server** drop down list, select the remote server that you have set.
 - b. In the **Select Contact Recorder Sets** list, select the CSIPO set that you want to backup.
5. In the **Backup Label** field, type a label for the backup.
 6. Click **OK**.

Restoring an IP Office Server Edition server

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

Note:

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

Before you begin

Warning:

Close any Voicemail Pro client before restoring.

The restoration process requires the voicemail service to shutdown and restart. This does not occur if any Voicemail Pro client is connected to the service during the restore and leads to an incorrect restoration of files.

Procedure

1. In the Web Manager menu bar, click **Solution**.
2. In the Solution window, select the component that you want to restore.

To backup all the components, select the **Actions** check box .

3. Click **Actions** and select **Restore**.
4. Do one of the following:
 - To restore from a remote server:
 - a. In the **Select Remote Server** drop down list, select the remote server that you have set.
 - To restore using a proxy:
 - a. In the **Select Remote Server** drop down list, select the remote server that you created.
 - b. Enable **Use Proxy**.
 - c. In the **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**.

Restoring a failed IP Office Server Edition server

Before you begin

 **Note:**

You cannot restore the backup the data of one 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.

Procedure

1. Install the IP Office Server Edition server.

For information about installing IP Office Server Edition, see [Installing IP Office Server Edition Server](#) on page 17.
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 11: Upgrading

Server Edition upgrade policy

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

Minor Upgrades

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

Major Upgrades

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

Upgrades with Patches Present

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

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

Upgrade Licenses

- To upgrade from one Server Edition release to another, for example, from 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.
- 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.

Upgrading IP500 V2 Expansion Systems to Release 9.1

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

Server Edition downgrade policy

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

1. Review the release notes of the current version before you downgrade.
2. Take a backup of the solution backup from Web Manager of Server Edition Primary before you downgrade. The backup should include all systems, components and configuration data sets.
3. Perform downgrade when there is no traffic on the system because it affects the service of the system.
4. *Minor* downgrade is a downgrade from one previously installed minor release to another in the same series. For example: 8.1 SP to 8.1 SP or 8.1 SP to 8.1 GA
5. *Minor* Linux server downgrade can be performed using the Web Manager package manager by qualified personnel only for the following IP Office components: IP Office, Jade Media Server, Avaya one-X[®] Portal for IP Office, Voicemail Pro Server or client, Web Control and Web Manager. You cannot downgrade any other component.
6. You can perform a *Minor* Linux server downgrade by performing a complete reinstallation and re-ignition.
7. You can perform a *Major* Linux server downgrade, for example, a downgrade from 9.0 to 8.1 or from 9.1 to 9.0 GA only by reinstallation and re-ignition. Do not attempt to downgrade a component through the Web Manager. In addition, all servers require downgrade because IP Office Server Edition Solution does not support mixed versioning.
8. You can downgrade Server Edition Expansion System through the IP Office Manager memory card Restore command.

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

*** Note:**

For Release 8.1 when you restore the system through Web Control, the system does not restore IP Office Security settings for any device other than Server Edition Primary . To restore the IP Office configurations, use the configuration synchronization feature of IP Office Manager .

9. Ensure that all components of a Server Edition deployment have the same software version.
10. Subsequent upgrade of a *Minor* or *Major* downgrade are supported

*** Note:**

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

Downgrade configuration data

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

Upgrade Process 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

- Ensure that all components of a Server Edition deployment have the same software version.
- This is policy not an absolute guarantee; if for example Avaya fix a bug in a Service Pack that corrects an upgrade or configuration error, the policy may not apply, and would be highlighted in the release notes

*** Note:**

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

Upgrade Procedures

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

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

*** Note:**

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

Downloading ISO using Web Manager

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

Before you begin

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

About this task

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

Procedure

1. Log in to Web Manager.
2. In Solution window, click **Actions** and select **Transfer ISO**.

3. In the Transfer ISO window, do one of the following:

- Download from a remote server.
 - a. In **Transfer from** field, select **Remote Location**.
 - b. In **File path** field, type the path where the ISO file is located on the remote server.
 - c. In **Select Remote Server**, choose the remote server where the latest ISO is located.

If you want to set a proxy server, enable **Use Proxy** and select the proxy server in **Select Proxy** field.


- Download from primary server path.
 - a. In **Download from** field, select **Primary Server Path**.
 - b. In **File path** field, type the path where the ISO file is located in the primary server.
- Download from the client machine.
 - a. In **Download from** field, select **Client Machine**.
 - b. In **Select ISO** field, browse to the location where the ISO file is located on the client machine.
- Download from DVD of Primary server.
 - a. Insert the installation DVD in the DVD drive of the Primary server.
 - b. In **Download from** field, select **DVD Primary Server**.
- Download from USB of Primary server.
 - a. Insert the installation USB in the USB port of the Primary server.
 - b. In **Download from** field, select **USB Primary Server**.

4. Click **OK**.

Result

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

Upgrading using Web Manager

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

Note:

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

Before you begin

Download the latest ISO using Web Manager.

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

About this task

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

* Note:

You cannot upgrade IP Office Server Edition systems directly from a remote server.

Procedure

1. Log in to Web Manager.
2. In the server list on the Solution page, select the Primary Server.
Click **Actions** and then select **Upgrade**.
3. In the Upgrade window, ensure that the Primary server is selected and click **OK**.
Note that you can opt to schedule the upgrade at a later time by selecting **Schedule job** and defining a scheduled time.
4. You receive a prompt regarding upgrade licenses. Click **Yes**.
5. You receive a prompt for the License Agreement. Click **Accept** and then **Next**.
6. Click **Close** to close the Upgrade window.
7. You receive a prompt to confirm the upgrade. Click **OK**.
The upgrade process begins.
8. After 30 minutes, log in to Web Manager.
9. You receive a prompt regarding background synchronization. Click **Yes**.
10. You receive a prompt that an additional upgrade is required for the Primary Server. Click **Yes** to perform the upgrade immediately.
The upgrade continues and the server is rebooted. The server can take up to 20 minutes to completely restart.

* Note:

You can select **No** and continue with the upgrade at a later time. On the Solution page, the server displays a warning that the upgrade needs to be completed.

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

The upgrade process begins.

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

Upgrading the system using an installation DVD or USB drive

Before you begin

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

Procedure

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

 **Note:**

To restart a Server Edition server, always use Web Manager. For more information, see [Restarting a Server using Web Manager](#) on page 108. For a new installation, power cycle the server.

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

 **Note:**

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

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

The system prompts you to install or upgrade. If you are installing Server Edition on a server in which Server Edition is already installed, then the system displays the details of the

applications that are already installed. The system also displays the details of the applications that the system will install.

11. Select **Upgrade** and then click **Next**.
12. You receive a prompt regarding licenses. Click **Next**.
13. Click **Next** to start the upgrade. The upgrade process can up to one hour to complete.
14. You receive a prompt that the system has been successfully upgraded. Click **Next**.
15. You receive a prompt to install additional TTS languages. Click **Next**.
16. Remove the installation DVD or the installation USB drive and click **Reboot**.

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

17. Log in to Web Manager.
18. You receive a prompt regarding background synchronization. Click **Yes**.

Next steps

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

Upgrading the system automatically

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

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

Before you begin

Server Edition installation USB drive. For more information, see [Creating an installation USB drive for automatic upgrade](#) on page 19.

Procedure

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

Note:

To restart Server Edition server, always use Web Manager. For more information, see [Restarting a Server using Web Manager](#) on page 108. For a new installation, turn off the power supply to the server.

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

*** Note:**

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

Result

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

*** Note:**

When you upgrade Server Edition to 9.1, the system upgrades the version of CentOS to 6.4. For more information, see [Checking the version of CentOS](#) on page 151.

Next steps

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

*** Note:**

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

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

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

Before you begin

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

About this task

You can upgrade only a local server using this procedure.

Procedure

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

The default port number is 7071.

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

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

 **Note:**

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

4. Do one of the following:

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

Chapter 12: Shutting down a system

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

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

About this task

Warning:

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

Procedure

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

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

4. Click **OK**.

Shutting Down a Linux Server Using Web Manager

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

Procedure

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

Shutting down a Linux server using Linux Platform settings

About this task

To shut down a server using Linux Platform settings:

Procedure

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

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

Chapter 13: Changing the IP Address of a Server Edition Server

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

Related links

[Changing the IP Address of the Primary Server](#) on page 110

[Changing the IP Address of a Secondary or Expansion Server](#) on page 111

Changing the IP Address of the Primary Server

Procedure

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

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

- a. Enter the new Server Edition Primary server IP address/Netmask. This may require a different Gateway IP Route.
 - b. Save the configuration to the system. This results in the system going offline from the Server Edition Primary server and Manager.
 - c. Once the ICU has been run on each system, close Manager.
2. Use IP Office Web Manager to log in to the Server Edition Primary server and change the IP address.
 3. Restart the Server Edition Primary server.
 4. Use Manager to log in to the Server Edition Primary server and check that all the IP Office systems are online.
 5. Review and test the configuration.
 6. Perform a backup.

Related links

[Changing the IP Address of a Server Edition Server](#) on page 110

Changing the IP Address of a Secondary or Expansion Server

Procedure

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

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

2. Change the IP address.
3. Save the configuration to the system. This results in the system going offline from the Server Edition Primary server and Manager.
4. Log in to the Server Edition Primary server and remove the Server Edition Secondary or Server Edition Expansion System from the solution.
5. Run the ICU and add the Server Edition Secondary or Server Edition Expansion System to the solution.

If requested, use the consolidate from Primary (Replace option).

6. Launch one-X Portal administration and configure the DSML and CSTA providers with the new IP address. The one-X Portal service may require a restart.
7. Review and test the configuration.
8. Perform a backup.

Related links

[Changing the IP Address of a Server Edition Server](#) on page 110

Chapter 14: Replacing the hardware of IP Office Server Edition

Replacing IP500 V2 system

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

Before you begin

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

Procedure

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

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

Replacing System SD Card

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

Before you begin

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

Procedure

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

You do not need to shutdown the system.

2. Remove SD card.
3. Insert replacement SD card in System SD slot and wait for System SD LED to be constant green.

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

*** Note:**

Any local licenses will fail in 2-4 hours if not failed already. All Server Edition central licenses remain valid.

4. Using IP Office Manager, administer new local licenses and delete old.
5. Validate status and configuration with IP Office Manager, Web Manager, , and SSA.
6. Take a backup using Web Manager and an SD card backup using IP Office Manager, SSA or system phone.

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

Replacing an IP 500 V2 Field Replacable Unit

Procedure

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

Replacing a Linux server

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

Before you begin

- At all times follow the relevant safety and static handling procedures.
- The HP DL360/Dell R620 hard drives and power supplies are hot swap. There is no need for chassis replacement. These items should be replaced while the system is running. For further information see document IP Office Installation guide of the Avaya Common Server installation guides.

- If viable and appropriate, take server backup using Web Manager. Take a backup of all components, all data sets, and to a remote server. Note any parameters required for the new server's ignition process
- If not down already, shut down the server using Web Manager, then power off.
- Ensure any resilient switch over of phones, hunt groups, VMPro has taken place. There is currently no force fail-over command.
- Remove and replace chassis with same variant. You can replace:
 - an HP DL120 with a Dell R210
 - an HP DL360 with a Dell R620

About this task

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

Procedure

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

The system restores all configuration and data saved in the original backup except security settings. If this is an Application Server that is not a part of Server Edition, use Web Manager to restore.

6. Reconstitute the security settings as these will be default.
 - If the system is supported through IPOSS and SSL VPN, see [Restoring SSLVPN/ IPOSS](#) on page 115
 - If you are replacing a Server Edition Primary server, set all the non-default security settings using IP Office Manager.
 - If you are replacing a Server Edition Secondary server, a Server Edition Expansion System, or an Application Server, use the **Synchronize Security** feature of Web Manager.
7. Validate status and configuration with Web Manager, Manager, and SSA.
8. Perform a backup using Web Manager.
9. Using IP Office Manager, administer new local licenses and delete old.

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

Restoring SSLVPN or IPOSS

About this task

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

Procedure

To restore either the 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 certificate at [Appendix A: Certificate Text](#) on page 154 to IP Office's Trusted Certificate Store using IP Office Manager. The certificate expires in 2020.

Chapter 15: Capacity Planning

This covers various aspects of 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 *Avaya IP Office™ Platform Solution Description* gives a high level view on deployment components.
- 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: The 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 behavior or errors in the published documentation. They can be found at: <http://marketingtools.avaya.com/knowledgebase/businesspartner/caveats/index.php>
- Virtualized Deployments: Server Edition components are supported in a virtualized environment using VMware. The performance and capacity is directly governed by static and dynamic resource assignments which are not covered here. For more information, see *Deploying Avaya IP Office™ Platform Server Edition Servers as Virtual Machines*.
- Avaya Contact Center Applications: Server Edition supports differing capacity and performance levels when IP Office Contact Centre (IPOCC) or Avaya Contact Center Select (ACCS) are attached. Refer to the relevant application documentation.
- Other attached Avaya DevConnect applications: Refer to the relevant application documentation

The *Avaya IP Office™ Platform Solution Description* 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 (IP500 V2) because of the combination of VoIP with digital and analogue, and the flexibility of constructs.

The Linux components (Server Edition Primary, Server Edition Secondary and Linux Server Edition Expansion System) are VoIP only and single construct, save for the decision whether to move the one-X Portal for IP Office server from the Server Edition Primary to a separate platform for capacity.

Releases of IP Office Server Edition prior to release 9.1.2 have differing capacities and performance limits and the corresponding release documentation should be used.

Virtualized Deployments

Server Edition components are supported in a virtualized environment using VMware technologies. This document refers to the option as Open Virtual Appliance (OVA) and assumes that the necessary host and Virtual Machine (VM) resources have been assigned.

In general, OVA is regarded as the Dell R620 for whatever Server Edition component, noting that the support capacities and performance of a Server Edition Expansion System differs from a Server Edition Primary or Server Edition Secondary regardless of the platform.

For further information about VM resourcing and OVA-specific planning, see *Deploying Avaya IP Office™ Platform Server Edition Servers as Virtual Machines*.

IP Office Select

Avaya IP Office Select is new premium Server Edition offer providing extended capacity, performance and features over basic Server Edition. Where Select is required, it is indicated in the relevant section. Where not indicated, either basic Server Edition or Select can be used.

In summary, IP Office Select offers the following increased capacities on the Dell R620 and OVA platforms only:

- Users/extensions per server (1500 > 3000)
- Users/extensions per solution (2000 > 3000)
- Expansion systems (30 > 148)
- Power User/UC clients (750 > 3000)
- Hunt Groups (300 > 500)
- Voicemail/Attendant/Recording channels (150 > 500)
- Conference channels (256 > 512)
- SIP trunk calls (512 > 1024)
- Inter IP Office line channels (250 > 500)
- Solution SoftConsole instances (32 > 50)

Select offers increased performance, on the Dell R620 and OVA platforms only: Peak call Rate (18,000 > 20,000).

Select offers the following additional features:

- Expansion to Expansion Inter IP Office lines
- Location based phone resilience
- Expansion to Expansion phone and hunt group resilience
- VMWare HA
- Active Directory/LDAP integration

The decision to deploy basic Server Edition or Select should be made at the outset. However, it is possible to convert a basic Server Edition to a Select solution at a later date without loss of configuration or data. Moving from Select to basic Server Edition requires re-configuration.

Avaya Contact Center Applications

Server Edition supports both IP Office Contact Centre (IPOCC) and Avaya Contact Center Select (ACCS). When either is connected, certain aspects of Server Edition capacity and performance are determined by that application. These include:

- Maximum agents
- Supported call rate
- Maximum Conference channels
- Maximum Recording channels

These are irrespective of whether the IP Office system is Select or basic Server Edition. Maximum conference and recording channels are covered in this document. Refer to the relevant application documentation for all other aspects.

Related links

- [Primary and Secondary Server Capacity Planning](#) on page 118
- [Avaya one-X Portal Server Capacity Planning](#) on page 123
- [IP500 V2 Expansion System Capacity Planning](#) on page 124
- [Linux Server Edition Expansion System Capacity Planning](#) on page 131
- [Conferencing Capacity Planning](#) on page 132
- [Voicemail, Auto Attendant, and IVR Capacity Planning](#) on page 133
- [Voice Recording Capacity Planning](#) on page 134
- [Multi-Site Network Link Capacity Planning](#) on page 135
- [Call Destination Server](#) on page 136
- [IP infrastructure, bandwidth, and VoIP Quality of Service](#) on page 137
- [Call Traffic Profile](#) on page 138
- [Resilience and Failover](#) on page 139
- [Startup and Availability](#) on page 140
- [Capacity planning for over 3000 users](#) on page 140

Primary and Secondary Server Capacity Planning

When designing a Server Edition Solution, many aspects need to be considered for capacity. These include:

- Maximum extension, user capacity; both per server and solution
- Maximum anticipated site/node capacity
- Maximum trunk capacity
- The total concurrent VoIP call capacity
- Call media destination location and type; both intermediate and final
- Direct/indirect/secure VoIP media
- Conference, and recording capacity

- Multi-Site Network link capacities
- Call Destination
- IP Infrastructure & VoIP QoS
- Trunk utilization and call traffic profile
- Resilience and failover requirements
- Available licenses

All of the above must be assessed, as one factor may limit another.

Related links

[Capacity Planning](#) on page 116

[Maximum Extension, User, and Site Capacity](#) on page 119

[Maximum Trunk Capacity](#) on page 120

[Server Concurrent Call Capacity](#) on page 121

[Call Media Path](#) on page 122

Maximum Extension, User, and Site Capacity

The server platform type should be selected to support the maximum potential users/extensions/sites according to the following table.

Primary/ Secondary Server Type	Maximum Server Users/ Extensions	Maximum Solution Users/ Extensions	Maximum Expansion Systems	Maximum Solution Call Rate, BHCC	Notes
HP120G7/Dell R210 II	750	1500	30	7,200	
HP DL360G7	1500	2000	30	18,000/9,000	[1]
Dell R620	1500	2000	30	18,000/9,000	[1], [2]
OVA	1500	2000	30	18,000/9,000	[1]
Dell R620 — IP Office Select	3000	3000	148	20,000/10,000	[1]
OVA — IP Office Select	3000	3000	148	20,000/10,000	[1], [2]

Notes:

1. Lower call rate when one-X Portal users active.
 2. Assumes sufficient VM resources assigned.
- The Server Edition Secondary server platform must match the Server Edition Primary server. For example a Dell R620 when the Primary is a Dell R620. A mix of native and virtualized is supported, providing the resources assigned to the virtual server match the other.
 - Maximum users and extensions are the configuration limits, not a currently active/registered limit.
 - The special user 'NoUser' is not counted.

- Certain types of extension are supported at a lower capacity. For example DECT R4 and 11xx/12xx phones.
- Maximum Solution Call Rate can be further reduced by the presence of Call recording, CTI or Contact Center application such as IPOCC or ACCS.

The following occurs if the maximum numbers are exceeded:

- Manager does not permit the administration of more than 2000 extensions/users if the solution is not Select.
- Manager does not permit the administration of more than 1500 per server extensions/users if the solution is not Select.
- Manager does not permit the administration of more than 30 expansion systems if the solution is not Select. It will always reserve one for a Server Edition Secondary server.
- The Server Edition Primary server does not accept phone registrations from more than the above per-server quantity of extensions. Additional phone registrations are rejected. This is important when considering fall back scenarios.
- If the call rate is exceeded, there may be disruption to recordings, or a general slowdown in other operation such as UC or management clients.

Related links

[Primary and Secondary Server Capacity Planning](#) on page 118

Maximum Trunk Capacity

The Primary/Secondary server supports three types of trunks:

- SIP
- H.323
- IP Office

Primary/Secondary Server Type	Maximum Registered SIP Trunks	Total SIP Trunk calls (direct/indirect media)	Maximum IP Office (SCN) Trunks	Maximum calls per SCN Trunk
HP120G7/Dell R210 II	125	256/128	32	250
HP DL360G7	250	512/256	32	250
Dell R620	250	512/256	32	250
OVA	250	512/256	32	250
Dell R620 — IP Office Select	250	1024/512	150	500
OVA — IP Office Select	250	1024/512	150	500

Notes:

- The **Total SIP Trunk Calls** figure is the maximum number of concurrent SIP trunk calls/session. They can be distributed over one or more trunks on the same system.

- SIP trunk concurrent call capacity is also limited by available licenses and the **SIP Line | SIP URI | Max Calls per Channel** setting.
- The number of SIP trunk session licenses requested by each system is defined by the **System | Telephony | Maximum SIP Sessions** setting. One available SIP Trunk session license enables one concurrent SIP session/call.
- The maximum number of configured URIs per SIP trunk is 150. This is not correlated with maximum SIP trunks or concurrent calls.
- The Maximum Calls per SCN Trunk figure is the maximum number of concurrent sessions supported on a single inter-node link whether WebSocket or Proprietary type. Note that the number of SCN channels is controlled by the **Line | IP Office Line | Number of Channels** setting.
- H323 trunks are distinct from SCN, but are taken from the same capacity pool.
- The above figures are a theoretical maximum. Other factors can reduce what can be utilized on a concurrent basis:
 - Available licenses
 - Trunk configuration
 - Maximum server call capacity

The following occurs if the maximum numbers are exceeded:

- Manager does not permit the administration of more than 30 Expansion Systems if the solution is not Select.
- Unless administered, IP Office does not limit the number of concurrent trunk calls and makes a best effort to service all. VoIP voice quality will degrade as load increases. High overload conditions will cause the server to perform poorly in general.

Related links

[Primary and Secondary Server Capacity Planning](#) on page 118

Server Concurrent Call Capacity

Each server type is rated to support every single extension engaged in a call providing it is direct media and regardless of security settings. If the media stream passes through the server some way, the capacity is reduced.

Primary/Secondary Server Type	Concurrent Calls, direct media	Concurrent Calls, indirect media	Concurrent Calls (Secure), indirect media
HP120G7/Dell R210 II	750	128	64
HP DL360G7	1500	256	128
Dell R620	2000	1024	512
OVA	2000	1024	512

Table continues...

Primary/Secondary Server Type	Concurrent Calls, direct media	Concurrent Calls, indirect media	Concurrent Calls (Secure), indirect media
Dell R620 — IP Office Select	3000	1024	512
OVA — IP Office Select	3000	1024	512

Notes:

- Direct media is RTP/SRTP data directly between VoIP endpoints, not through IP Office. There are some IP Office networking constraints to achieve direct media. See [Call Media Path](#) on page 122.
- Direct media with SRTP does not reduce the direct media capacity.
- One SRTP direct media call reduces the available RTP call capacity by 2 (and vice versa).
- If SRTP transcoding is present (for example where the security parameters are mismatched between two phones), the capacity is reduced by a further 50%.
- OVA capacities assume sufficient VM resources assigned.

Concurrent call maximum capacity can be administered using Manager in a number ways to ensure limits are not exceeded:

- The **Number of Channels** and **Outgoing Channels** setting on the **Line | IP Office Line VoIP** tab.
- The **Max Calls per Channel** setting on the **SIP Line | SIP URI** tab.
- The **Call Admission Control** area of the **Location** settings.
- The **VoIP Security** area of the **System** settings.
- The **Media Security** area in the **VoIP Settings** tab for Lines.
- The **Media Security** area in the **VoIP** tab for Extensions.

The following occurs if the maximum numbers are exceeded:

- Unless administered, IP Office does not limit the number of concurrent calls and makes a best effort to service all.
- VoIP voice quality will degrade as load increases. High overload conditions will cause the Server to perform poorly in general.

Related links

[Primary and Secondary Server Capacity Planning](#) on page 118

Call Media Path

There are two options for where calls go between VoIP endpoints (e.g. SIP trunk to H.323 extension): direct and indirect media. Direct media does not use the server's routing engine and hence, the base capacity for concurrent calls applies.

Direct media is a configurable parameter for VoIP trunks and extensions with a default of active.

Indirect media will occur either where configured, or if direct media is not possible (even if configured). Some causes are:

- VoIP traffic routed between the LAN1 and LAN2 interface.
- Unsuccessful codec negotiation (including silence suppression, DTMF transport as well as basic codec support).
- A VoIP endpoint that does not support direct media.
- Mismatched SRTP or SRTCP security settings such as no common cipher suite.
- Network Address Translation (NAT) traversal usually associated with Remote Worker phone deployments.

The above should be avoided if at all possible due to the limited indirect media capacity.

Related links

[Primary and Secondary Server Capacity Planning](#) on page 118

Avaya one-X® Portal Server Capacity Planning

The following Avaya one-X® Portal client capacity numbers are supported with two main options:

- The Avaya one-X® Portal server running on the Server Edition Primary.
- A standalone server with increased capacity.

Primary Server Type	Maximum one-X Portal Clients – Primary	Maximum one-X Portal Clients – Stand Alone	Maximum Solution Call Rate, BHCC
HP120G7/Dell R210 II	375	750	7,200
HP DL360G7	750	750	9,000
Dell R620	750	750	9,000
OVA (Assumes sufficient VM resources assigned.)	750	750	9,000
Dell R620 — IP Office Select	1500	3000	10,000
OVA — IP Office Select (Assumes sufficient VM resources assigned.)	1500	3000	10,000

Notes:

- The maximum supported total solution call rate is 7,200/9,000/10,000 BHCC when Avaya one-X® Portal users are active.
- The Avaya one-X® Portal client types can be of any mix, including plug-ins. HTTP or HTTPS can be used. Not more than 50% can be Avaya Communicator for Windows.

- With Avaya one-X[®] Portal users active, a solution-wide limit of 750 conference channel participants applies, but this limit does not include recording channels.
- It is possible to migrate from a Avaya one-X[®] Portal server located on the Server Edition Primary to a stand alone server at a later date. See the Avaya one-X[®] Portal documentation for the migration process.

Related links

[Capacity Planning](#) on page 116

IP500 V2 Expansion System Capacity Planning

When planning for a Server Edition Expansion System (IP 500), you must consider the following:

- Maximum trunk and extension capacity
- The total concurrent VoIP call capacity
- The VCM channel capacity
- Call media destination location and type; both intermediate and final
- Direct/indirect/secure VoIP media
- Conference, and recording capacity
- Multi-Site Network link capacities
- Call Destination
- IP Infrastructure & VoIP QoS
- Trunk utilisation and call traffic profile
- Resilience and Failover

All the above must be assessed, as one factor may limit another.

Related links

[Capacity Planning](#) on page 116

[Maximum Extension/User Capacity](#) on page 124

[Maximum trunk capacity](#) on page 125

[Concurrent Call Capacity](#) on page 126

[VCM Channel Capacity](#) on page 128

[Call Media Path](#) on page 130

Maximum Extension/User Capacity

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

- 384 Analog extensions
- 384 Digital extensions

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

The total may not exceed 384 extensions. The capacity of analog 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	Max VoIP
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

[IP500 V2 Expansion System Capacity Planning](#) on page 124

Maximum trunk capacity

A single Server Edition Expansion System (IP 500) 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 concurrent calls
- 32 H323/SCN trunks with 250 concurrent calls per trunk

This is the theoretical maximum number of trunk channels that can be supported. Other factors will reduce what can be utilized on a concurrent basis.

- Available licenses
- Trunk configuration
- VCM channels
- Maximum server call capacity

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

*** Note:**

All variants are not listed in the tables. 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	Max BRI	Max PRI E1/T1	Max Analog
Dual PRI	Dual PRI	Dual PRI	Dual PRI	ATM 16		0	240/192	128
ATM 4	ATM 4	ATM 4	4 Port Exp	ATM 16	ATM 16	0	0	204
BRI 8	BRI 8	BRI 8	BRI 8	ATM 16		32	0	128
						0	0	0

Server Type	Maximum Registered SIP Trunks	Total SIP Trunk Calls (direct/ indirect media)	Maximum IP Office (SCN) Trunks	Maximum Calls per SCN Trunk
IP500 V2	125	128/120	32	250

- The Total SIP Trunk Calls figure is the maximum number of concurrent SIP trunk calls/session and can be distributed over one or more trunks on the same system.
- SIP trunk concurrent call capacity is also limited by available licenses and the **SIP Line | SIP URI | Max Calls per Channel** setting.
- The number of SIP trunk session licenses requested by each system is defined by the **System | Telephony | Maximum SIP Sessions** setting. One available SIP Trunk session license enables one concurrent SIP session/call.
- The maximum number of configured URIs per SIP trunk is 150. This is not correlated with maximum SIP trunks or concurrent calls.
- The Maximum Calls per SCN Trunk figure is the maximum number of concurrent sessions supported on a single inter-node link whether WebSocket or Proprietary type. Note that the number of SCN channels is controlled by the **Line | IP Office Line | Number of Channels** setting.
- H323 trunks are distinct from SCN, but are taken from the same capacity pool.
- The PRI trunk capacity is also limited by available licenses. One available PRI Trunk Channel license enables one concurrent PRI call.

Related links

[IP500 V2 Expansion System Capacity Planning](#) on page 124

Concurrent 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. A Server Edition Expansion System (IP 500) has a number of concurrent call capacities that can influence the design of the 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. Limited by the available VCM channel capacity.
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. A VCM channel is always required during call setup.
Concurrent VoIP calls (secure): indirect media, IP500 V2	40	The value is per call leg. This means 40 VCM calls or 20 indirect media calls if some SRTP settings demand decoding, then re-encoding. In a mixed RTP/SRTP call environment, each SRTP leg removes three from the RTP call capacity.

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, the 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 the Server Edition Expansion System (V2) in general.

Concurrent call maximum capacity can be administered using 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.
- **VoIP Security** area of the System settings.
- **Media Security** area in the **VoIP Settings** tab of Lines.
- **Media Security** area in the **VoIP** tab of Extensions.

The following occurs if the maximum numbers are exceeded. Unless administered, the Server Edition Expansion System (V2) does not limit the number of concurrent calls and makes a best effort to service all. VoIP voice quality will degrade as load increases. High overload conditions will cause the Server Edition Expansion System (IP 500) to perform poorly in general.

Related links

[IP500 V2 Expansion System Capacity Planning](#) on page 124

VCM Channel Capacity

Voice compression (VCM) channels enable the 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 analog/digital 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.

Local V2 Expansion conferences and music on hold use the digital domain. Therefore, all VoIP parties (trunk or extension) require a VCM channel.

VCM channels are also used to perform VoIP 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 only G.711. This case will use two VCM channels and should be avoided wherever possible.

The following table summarises VCM channel usage.

Endpoint A	Endpoint B	VCM channels used [1]	Notes
Analog/Digital trunk or extension	Analog/Digital trunk or extension	None	DECT endpoints are VoIP
	Local Conference	None	Conference hosted on the IP500 V2
	Local Music on Hold	None	
	Embedded Voicemail	None	Includes voicemail, attendants, announcements Embedded Voicemail not supported in Server Edition
Analog/Digital trunk or extension	VoIP trunk or extension	1	
	Central Voicemail	1	Includes voicemail, IVR attendants, announcements
	Remote Conference	1	
	Remote Music on Hold	1	Maximum of 3 MOH sources streamed from Primary Server using a maximum of 3 VCM channels
	Call recording	1	Using Voicemail Pro, ACCS or IPOCC

Table continues...

Endpoint A	Endpoint B	VCM channels used [1]	Notes
VoIP trunk or extension	VoIP trunk or extension	None [2]	VoIP endpoints includes IP Office Line (AKA SCN line), DECT endpoints
	Central Voicemail	None [2]	Includes voicemail, IVR attendants, announcements
	Remote Conference	None [2]	
	Remote Music on Hold	None [2]	Streamed from Primary Server
	Call recording	None [2]	Using Voicemail Pro, ACCS or IPOCC
VoIP trunk or extension	Analog/Digital trunk or extension	1	
	Local Conference	1	Conference hosted on the IP500 V2
	Local Music on Hold	1 per MOH source [2]	Maximum of 4 MOH sources. One VCM channel will be used per codec type per source.
	Embedded Voicemail	1	Includes voicemail, attendants, announcements Embedded Voicemail not supported in Server Edition

Notes:

1. Unless otherwise specified, the VCM channel is used for the duration of the call and the VCM resource is always local.
2. Assumes both endpoints' VoIP codecs match, if they do not match 2 VCN channels are used.

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 but 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 and 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.

If VCM channels are used to convert SRTP media, a maximum of 40 calls per system are supported regardless of codec type.

When the system runs out of VCM resources, the Server Edition Expansion System (V2) manages this common resource as efficiently as possible but if there are insufficient resources 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.

Related links

[IP500 V2 Expansion System Capacity Planning](#) on page 124

Call Media Path

Where calls start and remain in the digital and or analogue domain, the VCM and VoIP capacities of Server Edition Expansion System (IP 500) systems are not affected. The base non-blocking capacity applies.

Where calls go between VoIP and digital or analogue domains within the Server Edition Expansion System (IP 500), 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 the Server Edition Expansion System (IP 500) 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
- A VoIP endpoint that does not support direct media
- Mismatch of RTP and SRTP
- Mismatched SRTP or SRTCP security settings such as no common cipher suite. These should be avoided if at all possible due to the limited indirect media SRTP capacity.

Related links

[IP500 V2 Expansion System Capacity Planning](#) on page 124

Linux Server Edition Expansion System Capacity Planning

When designing a Server Edition Solution that includes an Server Edition Expansion System (L), the aspects that are covered for an 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 750, except DECT R4 which is 384
- Maximum trunk capacity for each Server Edition Expansion System (L)
 - No digital or analog trunks
 - Maximum SIP sessions/calls 256 total
- The concurrent call capacity of Server Edition Expansion System (L)
 - No analog or digital calls
 - Indirect media capacity 128
 - Direct media capacity 750
- The VCM channel capacity for each Server Edition Expansion System (L)
 - Only transcoding is relevant; 128 channels
 - There is no capacity difference due to codec type
- Call media path
 - Same as Server Edition Expansion System(V2)
- The server type can be an HP DL360G7, a Dell R620 or OVA. However, the supported capacities and performance are not increased.

All the above must be assessed, as one factor may limit another.

Related links

[Capacity Planning](#) on page 116

Conferencing Capacity Planning

Each Server Edition Primary, Server Edition Secondary, and Server Edition Expansion System supports a local conference capability with the following capacities.

Platform	Total Conference Channels	Maximum conference size	Total conference channels with ACCS	Total conference channels with IPOCC
HP DL120 / Dell R210	128	128	414	414
HP DL360	256	256	825	825
Dell R620	256	256	825	825
OVA	256	256	825	825
Dell R620 — IP Office Select	512	256	825	825
OVA — IP Office Select	512	256	825	825
IP500 V2	128	64	128	128

Notes:

- OVA will always advertise these figures. However, performance and capacity is dependent on VM resources assigned.
- The figures cover both ad-hoc and meet-me conference types.
- With one-X Portal users active, a solution-wide limit of 750 conference channel participants applies, but this does not include conferences used for call recording.
- The increased capacities for Avaya Contact Center Select (ACCS) and IP Office Contact Center (IPOCC) are only supported when the applications are actively connected to the host IP Office.
- No dynamic solution-wide conference allocation supported, only static via call flows or Conference Meet Me short code Line Group ID.
- V2 Expansion conferences exist in the digital domain. Therefore, all VoIP parties (trunk or extension) will require a VCM channel for the duration. See [VCM channel capacity](#) on page 128.
- Further information on conferences can be found at http://marketingtools.avaya.com/knowledgebase/businesspartner/ipoffice/mergedProjects/manager/_frame2.html?Conferencing.Overview.html.

The location of the conference resource used is determined by a number of factors:

- A user performing an ad-hoc conference will use the system's conference capacity on which they are logged in to.
- A meet-me conference using a user's personal meet-me bridge will use the system on which they are logged in to.
- A meet-me conference created by Voicemail Pro call flows, or the Conference meet-me short code feature will use the system on which the feature was invoked.

- To invoke a meet-me Conference on a remote system, use the Line Group ID field of the Conference Meet Me short code feature. By default this is set to 0, for local system.

Recording a conference requires an additional conference channel, as well as an SCN trunk channel to the recording destination (Primary or Secondary server, alternate during fail over operation). Neither IP Office nor Voicemail Pro can automatically link or move conference locations, but existing conferences can be connected together.

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

Related links

[Capacity Planning](#) on page 116

Voicemail, Auto Attendant, and IVR Capacity Planning

Leaving a voicemail for a user or hunt group uses one licensed (and available) voicemail channel and an SCN trunk channel, as the recording destination is on the Server Edition Primary (or Server Edition Secondary during fail over operation). If the source of the caller is digital or analog, a VCM channel is required.

Voicemail collect operation uses one licensed voicemail channel and an SCN trunk channel. If the destination of the caller is digital or analog, a VCM channel is required on the Server Edition Expansion System (IP 500).

Invoking an Auto Attendant, Announcement, or IVR script uses the same resources as voicemail, and is taken from the same pool of licenses and voicemail channel capacity. One active Auto Attendants, IVR, or Announcement takes one channel and license.

The total solution voicemail channel capacity is determined by a number of factors:

- The number of per-serve supported voicemail channels, which can be up to 250 for Dell R620, 150 for HP DL360, or 75 for the HP DL120/Dell R210 server.
- Whether the Dual VMPro feature is active (IP Office Select only) – this doubles the maximum capacity to 500 channels.
- The number of licensed voicemail channels: Each active master VMPro must have its own licenses. It inherits the other set when active as a backup.
- Recording also uses licensed voicemail channels. One active recording channel consumes one voicemail/AA channel.

If voicemail resources run out:

- Calls continue to alert and do not switch to voicemail.
- Voicemail collect will fail to connect to the Voicemail server.
- Calls to Attendants will continue to alert.
- Text To Speech (TTS) will not be output during call flows.
- Note that the TTS channel capacity is 250. As the TTS channel is utilized for a very short periods, this capacity should not prove a limitation

To ensure voicemail channel capacity is available for voicemail collect and leave, the Manager setting **Voicemail Channel Reservation** on the Server Edition Primary's **System | Voicemail** tab can be used 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 the Voicemail Pro documentation for more information.

If recording storage resources run out:

- Voicemail leave operations receive an announcement that the user/group's mailbox is full.
- Voicemail collect continues to function.

Related links

[Capacity Planning](#) on page 116

Voice Recording Capacity Planning

Each Server Edition Primary and Server Edition Secondary supports a voice recording capability with the following capacities.

Server	Server Recording Channels	Solution Recording Channels	Solution Recording Channels with ACCS	Solution Recording Channels with IPOCC
HP DL120/ Dell R210	75	75	175	175
HP DL360	150	150	350	350
Dell R620	150	150	350	350
OVA	150	150	350	350
Dell R620 — IP Office Select	250	500	350	350
OVA — IP Office Select	250	500	350	350

Notes:

- OVA always advertises these figures. However, performance and capacity is dependent on vCPU and vRAM assigned.
- Call recording uses a 3 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 (for the IP 500 Expansion), and SCN trunk channel as the recording destination is on the Server Edition Primary or Server Edition Secondary.
- The increased capacities for Avaya Contact Center Select (ACCS) and IP Office Contact Center (IPOCC) are only supported when the application is connected to the host IP Office.

- If the Dual Voicemail Pro feature is active (Select only) the maximum solution capacity is doubled to 500 channels.
- One active recording channel consumes one voicemail/AA channel.

The location of conference resource used is determined by point of recording.

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

The maximum supported voice recording call rate is 3,600 BHCC for an Expansion, 10,000 BHCC for a Linux Server.

If recording channel resources run out, further attempts to record calls or conferences are not successful.

To ensure channel capacity is available for recordings, the Manager setting **Voicemail Channel Reservation** on the Primary Server's **System | Voicemail** tab can be used to reserve channels exclusively for recording use.

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

If recording storage resources run out, further attempts to record calls or conferences are not successful and receive announcements to that effect.

Related links

[Capacity Planning](#) on page 116

Multi-Site Network Link Capacity Planning

A multi-site network link is the IP Office Line (SCN trunk) connection between each Server Edition node. The links are arranged in a star topology with the Server Edition PrimaryServer at the centre (or double star when a Server Edition Secondary server is present).

Regardless of direct/indirect media, VCM or codec used, a further capacity consideration is the multi-site network links between all Server Edition nodes. Each IP500 V2 or Linux link has a maximum capacity of 250 channels/calls (500 for Select Linux servers). The maximum total and outgoing channels are independently configurable in Manager using the **IP Office Line | VoIP** tab, and have a default of 128 for both.

This is per link, not a per system limit. For example, a Server Edition Primary or Server Edition Secondary may have up to 250/500 concurrent calls to each Server Edition Expansion System system. Due to the star topology of Server Edition, calls between Server Edition Expansion Systems go through the 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 between the Server Edition Primary, Server Edition Secondary, and Server Edition Expansion Systems. If the capacity is exhausted, an additional Server Edition Secondary or Server Edition Expansion System should be considered.

In release 9.1 and higher, it is possible to add IP Office Lines between Server Edition Expansion Systems. There is a limit of one between each pair of expansions. This link can be used to increase capacity and resilience.

If these figures are exceeded:

- Additional outgoing calls can be routed via 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 server is present.
- If no alternative route, incoming calls remain ringing until a channel is free and outgoing calls indicate busy.

Related links

[Capacity Planning](#) on page 116

Call Destination Server

When considering expansion or server planning from a media perspective, it is important to note that communication with any other Server Edition component will use VoIP and hence, is limited by the media, IP Office Line (SCN trunk) and VCM capacities. This includes:

- Calls to and from Server Edition Primary, Server Edition Secondary and Server Edition Expansion Systems.
- Call recording: one VoIP channel per recorded call. Destination will be the location of the active Voicemail Pro.
- Auto Attendants/IVR: one VoIP channel per call when connected to the Auto Attendant/IVR. Destination will be the location of the active Voicemail Pro.
- Conferencing when the conference focus is not the V2 Expansion: one VoIP channel per local member.
- Local conferences involving remote users: one VoIP channel per remote member when connected to the conference.
- Voicemail leave and collect: one VoIP channel per VM caller. Destination will be the location of the active Voicemail Pro.
- Announcements: one VoIP channel per call when generating announcements. Destination will be the location of the active Voicemail Pro.
- Centralized Music on Hold: one VoIP channel per central Music On Hold (MOH) source when playing to held calls. Destination will be the location of the MOH source.

For all VoIP connections between systems, the codec used will be according to the IP Office Line settings of those two nodes.

Consideration should also be given to intermediate destinations to ensure adequate capacity is present. For example, a consultation call will open a secondary channel for the consultation whilst keeping the initial call connected.

Any call on the IP Office Line takes into consideration administered channel limits and Call Admission Control (CAC) if active. Refer to the Manager documentation for behaviors when CAC limits are exceeded.

Related links

[Capacity Planning](#) on page 116

IP infrastructure, bandwidth, and VoIP Quality of Service

This document does not cover the detailed aspects of Ethernet and IP infrastructure.

For an IP Office bandwidth calculator, see <http://marketingtools.avaya.com/knowledgebase/tools/bandwidth/index.htm>.

Note that secure VoIP (SRTP) can increase the required bandwidth by up to 8%. See the “VoIP Security” chapter of *Avaya IP Office™ Platform Security Guidelines*.

In addition to the network requirements for VoIP calls, additional bandwidth must be reserved for the corresponding inter-node signalling and management paths. This includes any access using SSL VPN. The following suggested minimum bandwidths must be made available for these additional paths.

Table 4: Suggested bandwidths

Traffic	Suggested Minimum bandwidth	Comments
One-X Portal CTI	96 kbit per call or 192 kbit/s @ 7,200 BHCC	Between the one-X Portal server location and Expansion when one-X Portal server is active.
Web Manager	512 kbit/s	Between Web Manager PC and Primary (or Secondary under failover conditions) when a Web Management session is active
Manager	512 kbit/s	Between Manager PC and each node when a Manager session is active.
Upgrade	512 kbit/s	Between Primary and each node when upgrade is being performed.
Backup / Restore	256 – 2048 kbit/s	<p>Between Backup Server and each Expansion</p> <p>Between Backup Server and Primary</p> <p>Between Backup Server and Secondary</p> <p>An IP Office R9.1 Linux platform may be designated as the backup server.</p> <p>Bandwidth will only be required when a backup or restore operation is active, and only between participating nodes.</p> <p>The bandwidth required will be dependent upon backup/restore content.</p>

Table continues...

Traffic	Suggested Minimum bandwidth	Comments
Voicemail Pro Client	512 kbit/s	Between Voicemail Pro Client PC and IP Office Server when a Voicemail Pro server management session is active.
Between Voicemail Pro Server and Voicemail Pro Server	1024 kbit/s	Bursty traffic, peaking during start-up or loss of Server to Server connectivity.
Between Voicemail Pro Server and Contact Recorded Server	TBC	Between Primary and server running Contact Recorder.
Web Collaboration Client	128 – 256 kbit/s	Between each active Web Collaboration client and the Web Collaboration server.

Notes:

- These figures are for general guidance only as do not reflect the specific requirements for a given installation. For example:
 - Management operations are typically session based.
 - Backup and restore content and frequency are administrable.
 - Many are bursty in nature and might not coincide with others.
- Only the major signalling and management paths are included here. Further network bandwidth might be required for SSA, SysMonitor, syslog, SNMP or upgrade.
- For more information about possible IP communications, see *IP Office Port Matrix* at <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C201082074362003>.
- Server internal communications do not require bandwidth assessment.

Related links

[Capacity Planning](#) on page 116

Call Traffic Profile

General traffic engineering is outside the scope of this document. However the following Server Edition specific factors must be considered.

Server Type	Maximum Server Call Rate, BHCC	Maximum Solution Call Rate, BHCC	Notes
Primary/Secondary: HP120G7/Dell R210 II	7,200	7,200	Lower call rate when any one-X Portal user active.
Primary/Secondary: HP DL360G7	18,000/9,000	18,000/9,000	Lower call rate when any one-X Portal user active.
Primary/Secondary: Dell R620	18,000/9,000	18,000/9,000	<ul style="list-style-type: none"> Lower call rate when any one-X Portal user active. Assumes sufficient VM resources assigned.
Primary/Secondary: OVA	18,000/9,000	18,000/9,000	Lower call rate when any one-X Portal user active.
Primary/Secondary: Dell R620 — IP Office Select	20,000/10,000	20,000/10,000	Lower call rate when any one-X Portal user active.
Primary/Secondary: OVA — IP Office Select	20,000/10,000	20,000/10,000	<ul style="list-style-type: none"> Lower call rate when any one-X Portal user active. Assumes sufficient VM resources assigned.
Linux Expansion	7,200	N/A	
IP 500 V2 Expansion	3,600	N/A	

Notes:

- Total solution BHCC must not exceed 9,000/10,000 BHCC when one-X Portal users are active.
- Continuously running at the maximum supported solution call rate when one-X Portal users are active must not exceed 24 hours.
- one-X portal users include: Web Client, Call Assistant, Outlook Integration, Lync Integration, one-X Preferred Mobile Clients.
- Maximum recording call rate is 9,000/10,000 BHCC.

Related links

[Capacity Planning](#) on page 116

Resilience and Failover

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

- The total extensions/users on any single Server Edition Primary, Server Edition Secondary, or Server Edition Expansion System must not exceed their supported limits. Any H.323 phones that exceed the limit will be ignored on a first come, first served basis.

- Server Edition Primary failure when a Server Edition Secondary is present routes all non-local expansion calls, Voicemail leave + collect, IVR and Auto Attendants to the Server Edition Secondary.
- Server Edition Primary failure when a Server Edition Secondary is present moves group processing and management access to the Server Edition Secondary. This increases the management bandwidth from the Server Edition Secondary to the Server Edition Expansion Systems.
- Any Power User or Office Worker licenses associated with fail-over users will move with that user; no separate license provision on the fall back server is required.
- Any Voicemail channel licenses (real or virtual) associated with the Server Edition Primary will move to the Server Edition Secondary on fail-over. No separate license provision on the fall back server is required.

Related links

[Capacity Planning](#) on page 116

Startup and Availability

Event	Startup / Availability	Notes
Phone service availability after restart, DL360	1000 in 10 minutes	Able to make calls. 96x1 phone with DHCP, no upgrade. No PoE or other data equipment startup times included.
Phone service availability after restart, DL120/R210	500 in 5 minutes	
Phone service availability after restart, IP500 V2	384 in 5 minutes	
Phone upgrade performance, DL360	200 per 50 minutes	For 96x1 phone types. 16xx and 94xx types are typically quicker.
Phone upgrade performance, DL120/R210	100 per 50 minutes	
Phone upgrade performance, IP500 V2	50 per 50 minutes	

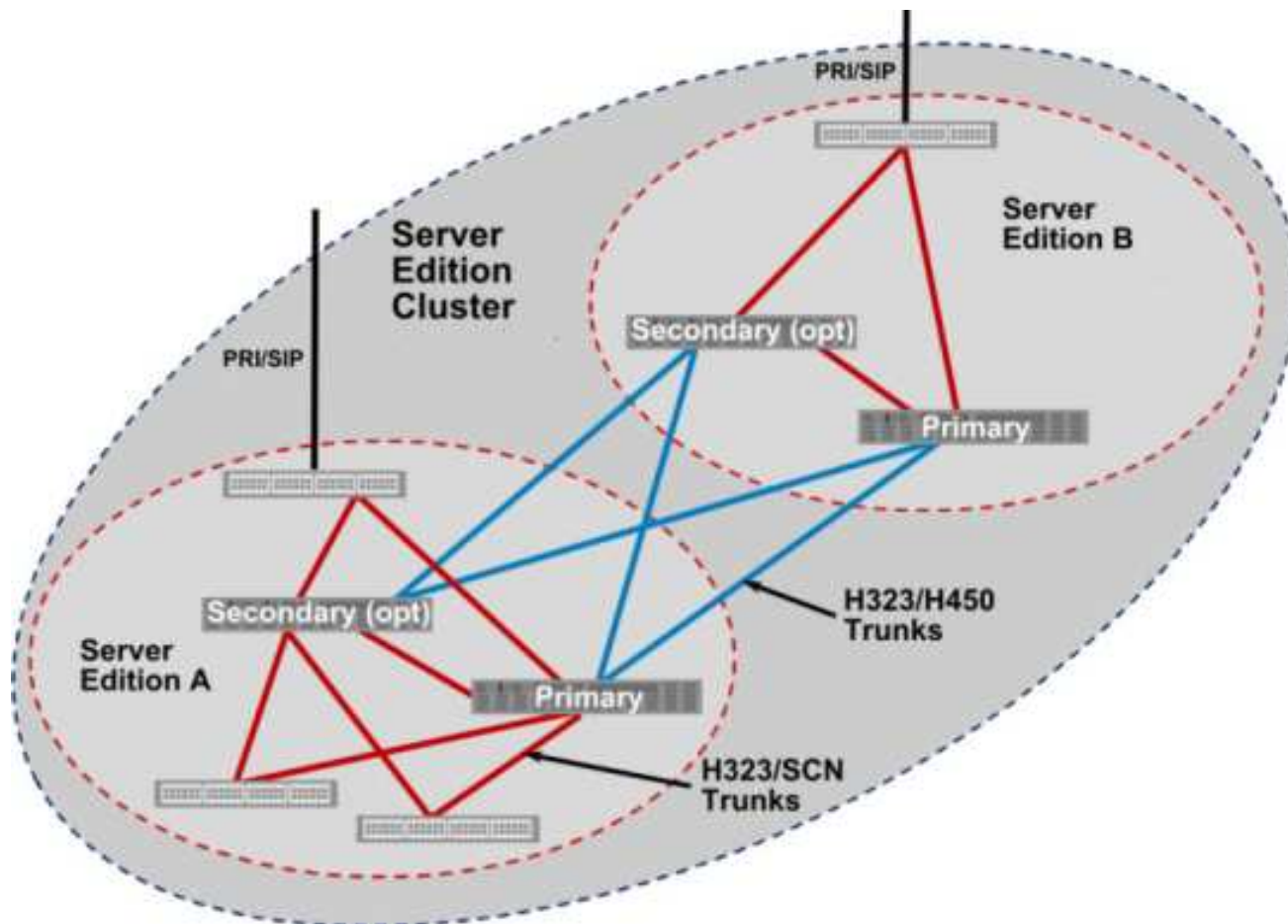
Related links

[Capacity Planning](#) on page 116

Capacity planning for over 3000 users

To provide a cost effective solution of more than 3000 users to larger customers, two IP Office Select systems can be federated together to support a total of 6000 users/extensions.

This construct may also be used when other per-solution capacities are exceeded. For example, one-X Portal users or Voicemail/recording channels.



You can create a cluster by linking two separate Server Edition systems using H.323 + H.450 trunks to provide a single system view to all users. 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 must be managed separately. The systems are configured to share a common dial plan and directory.

Feature	Server Edition	SE Federation	Comment
Maximum Users/ Extensions	300	6000	3000 per system
Directory	Single Directory	Common directory with manual synchronization between the two systems.	Can use auto synchronization for system directory.
Directory Size	7500	7500	
Dial Plan	Single dial plan	Single dial plan	For example, 21xxxx is on A and 22xxxx is on B.

Table continues...

Feature	Server Edition	SE Federation	Comment
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 a Server Edition 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 Server Edition Primary.
SMDR	Single stream per node	Single stream per node	
Voicemail	Single/Dual	Single/Dual 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 IP Office Lines with the following settings:

- Transport Type: WebSocket Client/Server
- Networking Leve: None
- 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. The WebSocket Server end for all lines should be the same Select system

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 Manager.

- Extract Full Name and Extension fields from each file into a single CSV directory file. See “Importing and Exporting Settings” in *Deploying Avaya IP Office™ Platform IP500/IP500 V2* for more information on the file formats.

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 using Manager.

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 see “Centralized System Directory” in *Administering Avaya IP Office™ Platform with Manager*.

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 and Server Edition Secondary.

PSTN/SIP trunks on one system can be accessed from the other using ARS 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 must be the same software version. Each should be upgraded separately from the associated Server Edition Primary server .

Related links

[Capacity Planning](#) on page 116

Chapter 16: Troubleshooting

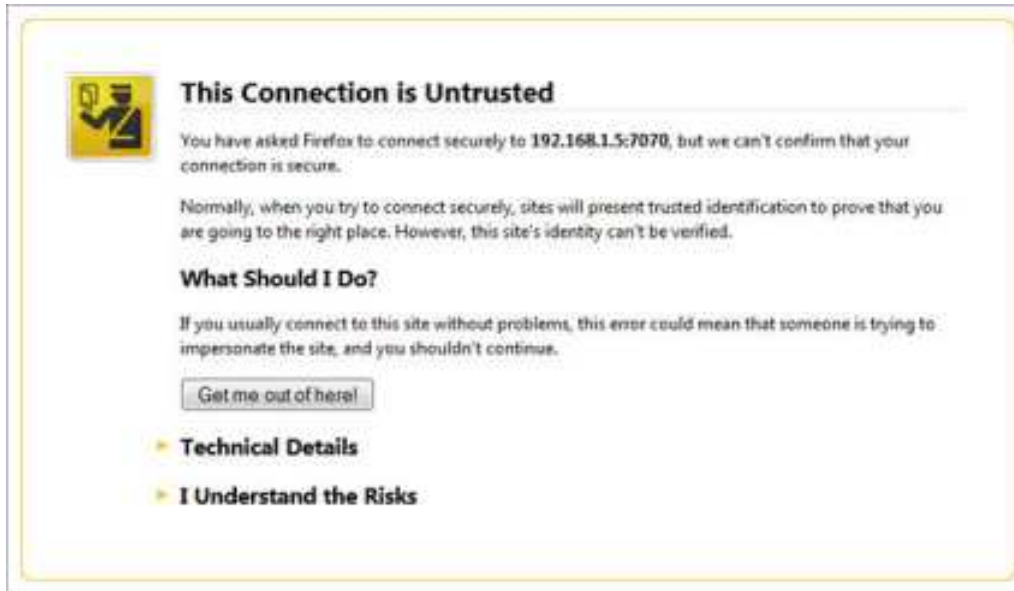
Warning message

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

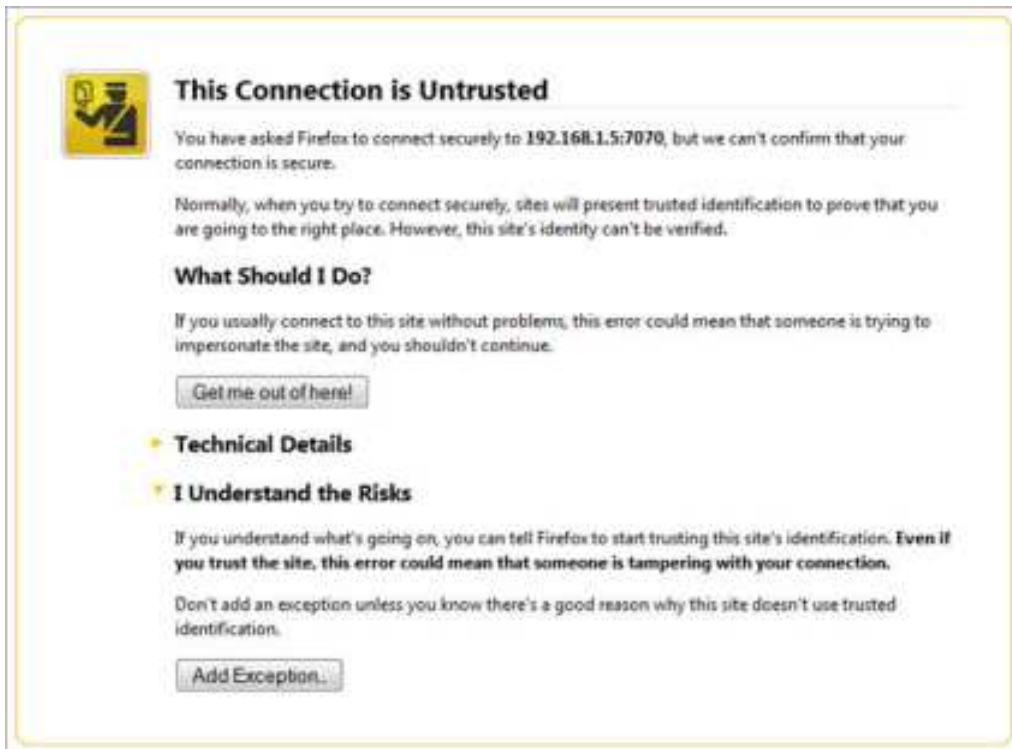
This Connection is Untrusted

*** Note:**

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



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



2. Click **Add Exception**.



3. Click **Confirm Security Exception**.

The system displays IP Office Server Edition login page.

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

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

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

1. Go to **File >Advanced > Security Settings**.
2. Select the IP Office Server Edition system, in the Select IP Office window.
3. Click **OK**.
4. Type the name of the *Security Administrator* in the **Service User Name** field.
5. Type the name of the *Security Administrator* in the **Service User Password** field.
The default user name is *security* and password is *securitypwd*.
6. Select **Services** in the navigation pane.
7. In the Service: Configuration section, set the **Service Access Source** field as *Unrestricted*.
8. Click **OK**.
9. Select **File > Save Security Settings**.
The system unlocks the access for the *Administrator*.
10. Open the configuration and log in as *Administrator*.

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

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

Solution:

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

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

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

Solution:

- Ensure that the password of the *Administrator* account on each of the Server Edition Expansion 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 148
- [Checking memory usage](#) on page 149
- [Checking the version of Linux OS](#) on page 151

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 147

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 62.

Before you begin

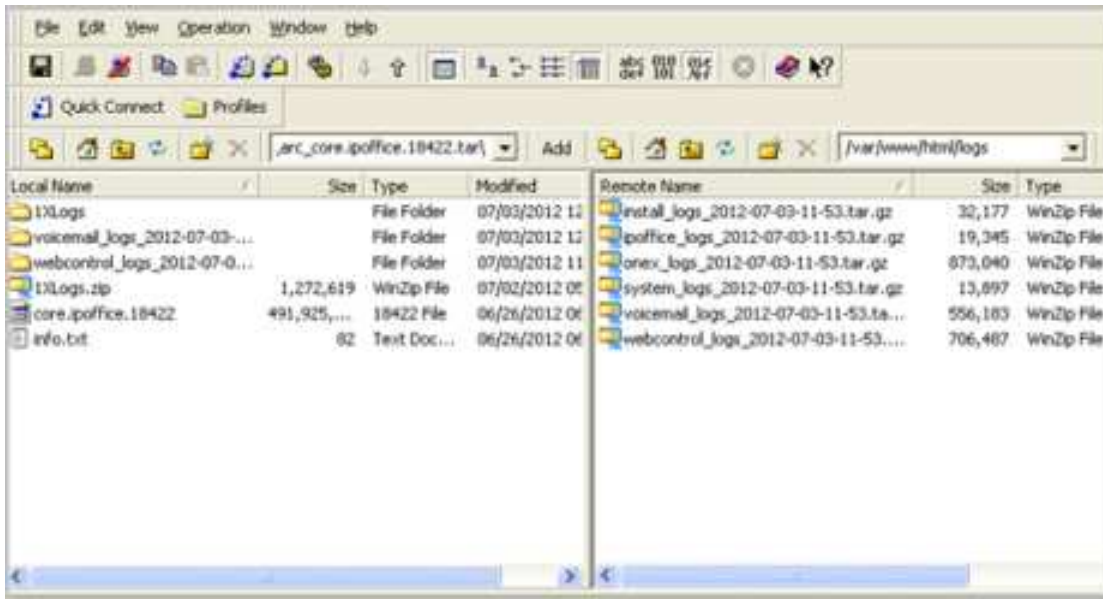
Log in as *Administrator* using SSH Secure File Transfer client

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
+ Tree
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 [ksftirqd/0]
0 [migration/0]
    
```

Related links

[Debugging steps](#) on page 147

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 148.

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 147

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. For information on certificates, see *Avaya IP Office™ Platform Security Guidelines*.

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

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

Solution

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

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

Manager: System | Telephony | Telephony | Phone Failback

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

Unable to export template

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

Solution

About this task

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

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

Procedure

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

For more information, see [Changing the Administrator password](#) on page 85.

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.

Possible reasons

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

Work around

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

Changing a System Configuration from Select to Non-Select

Condition

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

Remedy

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

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

Chapter 17: Appendix A: Certificate Text

Use this certificate when performing the procedure [SSLVPN/IPOSS Restoration](#) on page 115.

```

-----BEGIN CERTIFICATE-----
MIIGKTCCBRGgAwIBAgIQZBvoIM4CCBPzLU0tldZ
+ZzANBqkqhkIG9w0BAQFADCBYjELMAkGALUEBhMcvVMxwFzAVBgvNBVAoTD1Zlcm1TaWduLCBjbmMuMR8wHQYDVQQLE
xZWZxJpU2lnbiBucnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBwZXJpU2lnbiwgSW5jLiAtIEZvciBhdXR
ob3JpemVkiHVzZSBvbmx5MUUwQwYDVQQDEzxWZXJpU2lnbiBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IEENLcnRpZmljY
XRpb24gQXV0aG9yaXR5IC0gRzUwHhcNMTAwMjA4MDAwMDAwHhcNMjAwMjA3MjMlOTU5WjCBvDELMakGALUEBhMcvVM
xwFzAVBgvNBVAoTD1Zlcm1TaWduLCBjbmMuMR8wHQYDVQQLEzxWZxJpU2lnbiBucnVzdCBOZXR3b3JrMTswOQYDVQQLE
zJUZxJjtcyBvZiB1c2UgYXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYyYkxMDE2MDQGA1UEAxMtVmVyaVN
pZ24gQ2xhc3MgMyBjbnRlcm5hdGlvbmFsIFNlcnZlcjB1c2UgYXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYS
gKAQEAMdAcYvAV9IGaQqHzjxOdF8mfUdzasVLv/+NB3eDfxCjG4615HycQmLi7IJfBKERBD
+ppqFLPTU4bi7ulxHbZzFYG7rNVICreFY1xy1TIbxfNiQDk3P/
hwB9ocenHKS5+vDv85burJ1SLZpDN9pK5MSSAvJ5s1fx+0uFLjnx+c+kRLX/
gYtS4w9D0SmNniBXNUPpyiHb5SgzoHRsQ7AlYhv/JRT9Cm
mTnprqU/
iZucff5NYAc1lPe712mDK4KTQzfZg0EbawurSmaET0qO3n40mY5o1so5BptMs5pITRNGtFghBMT7oE2sLktiEuP7Tf
bJUQABH/weaoEqOOC5T9YtrQIDAQABo4ICFTCCAHEwEgYDVROTAQH/BAGwBgEB/
wIBADBwBGNVHSAEaTbnMGUGC2CGSAGG
+EUBBxcDMFYwKAYIKwYBBQUHAQgEWHGhOdBzOi8vd3d3LnZlcm1zaWduLmNvbS9jcHMwKgyIKwYBBQUHAQgIwHhocaH
ROcHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYTAObgNVHQ8BAf8EBAMCAQYwYwQYIKwYBBQUHAQgEYTBfoV2gWzBZMfcw
VRYJaW1hZ2UvZ22lmMCEwHZAHBGUrDgMCGgQUj
+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVyaXNpZ24uY29tL3ZzbG9nby5naWYwNAYDVRO1BC0
wKwYIKwYBBQUHAwEGCCsGAQUFBwMCBglghkgBhvhCBAAEGCmCGSAGG
+EUBCAEWNAyIKwYBBQUHAQEEDAMCQGccsGAQUFbZABhhodHRwOi8vb2Nzc5Z2XJpc2lnbi5jb20wNAYDVROfBC
0wKzApoCegJYyjaHR0cDovL2Nybc52Z2XJpc2lnbi5jb20vcGNhMy1nNS5jcmwwKAYDVRORBCEwH6QdMBSxGTAXBGNV
BAMTEFZlcm1TaWduTVBLS0yLTcwHQYDVRO0BBYEfNebfNgioBX33a1fzimWMO8RgC1MB8GA1UdIwQYMBaAFH/
TZafC3ey78DAJ80M5+gKvMzEzMA0GCSqGSIb3DQEBBQUAA4IBAQBxtX1zUkrd1000Ky6v1Ea1SVACT/
gvF3Dye9wfIYaqwk98NzzURniuXXhv0bpavBCrWDfjGIVRWAXIeLVQqh3oVXY
QwRR9m66SOzdtLdE0z6k1dyzmp8N5tdOlkSVWmzWoxZTDphDzqS4w2Z6BVxiEogbEtt9LnZQ/9/XaxvMisxx
+rNAVnwzeneUW/ULU/sOX7xo+68q7jA3eRaTjX9NEP9X+79uOzMH3nncHhdZLUNkt6Zmh
+q8lkyZGoaLb9e3SQBb26O/KZru99MzrqP0nkzKXmnUG623kHdq2FlveasB+lXwiiFm5WVu/
XzT3x7rfj8GkPsZC9MGAht4Q5mo
-----END CERTIFICATE-----

```

Index

A

- administering one-X Portal [76](#)
- administrator [85](#)
- Administrator [84](#), [86](#)
- AFA [74](#)
- alarms [60](#)
- application notes [14](#)
- audience
 - deployment [14](#)
- auto attendant
 - capacity planning [133](#)
- automatic
 - default paramaters [24](#)
 - install [23](#)
 - upgrade [105](#)

B

- backup [75](#), [79](#), [94](#)
 - overview [89](#)
- backup and restore
 - manage disk space [93](#)
- backup and restore policy [89](#)

C

- call media destination [136](#)
- call traffic profile [138](#)
- capacity planning [116](#)
- certificates [151](#)
- change history [10](#)
- changing the IP address [110](#)
- conferencing
 - capacity planning [132](#)
- configuration data [43](#)
- configurations
 - offline [146](#)
 - upload [146](#)
- configure [73](#)
- custom folder [82](#)

D

- data sets [91](#)
- debug [147](#)
- deploying [15](#)
- deployment
 - audience [14](#)
- DevConnect [14](#)
- disk usage [92](#)
- document purpose [10](#)

- downgrade [99](#)
- download [66](#)

E

- error [152](#)
- expansion system [34](#), [39](#)
- expansion system,
 - users [72](#)
- expansion system (L) [38](#)
- expansion system (V2) [36](#)
- extension [57](#)

F

- failed server
 - restore [96](#)

H

- hunt group [58](#)

I

- identity certificates [152](#)
- ignition process [24](#)
- infrastructure
 - bandwidth [137](#)
 - VoIP QoS [137](#)
- initial configuration utility [29](#)
- install [20](#)
 - Voicemail Pro [77](#)
- Install
 - automatic [19](#)
- installation USB drive [17](#)
- installing automatically [23](#)
- intended audience [10](#)
- IP 500 expansion system
 - capacity [124](#)
- IP 500 V2 capacity
 - call media path [130](#)
 - concurrent call capacity [126](#)
 - VCM channel capacity [128](#)
- IP500 V2 conversion
 - to Linux expansion [49](#)
 - to Server Edition primary [47](#)
 - to Server Edition V2 expansion [47](#)
- IP address
 - changing [110](#)
- IP Office
 - shutting down expansion server [108](#)
- ISO download [101](#)

Index

IVR		
capacity planning	133	
L		
LAN support	51	
license	55	
Linux expansion system		
capacity	131	
Linux Platform	61	
local server	106	
location	90	
lockout	146	
log files	64, 65	
logging in	78	
login	148	
M		
Manager	28	
memory	149	
migrate	80	
multi-site network		
capacity planning	135	
O		
offline	147	
on board	68	
one-X Portal	69, 72, 75	
capacity planning	123	
over 2000 users	140	
P		
password	85, 86	
platform		
system	62	
Platform	85	
primary server	17	
call media path	122	
concurrent call capacity	121	
maximum extension, user, and site capacity	119	
maximum trunk capacity	120	
primary server capacity	118	
product compatibility	13	
purpose of document	10	
R		
related documents	10	
remove	32, 39	
replace		
FRU	113	
IP500 V2	112	
Linux server	113	
SD card	112	
resilience	56	
failover	139	
H323	152	
resource websites	13	
restore	75, 80, 95	
restoring	81	
revision history	10	
root user	85	
S		
secondary server	31, 32	
Select license		
removing	153	
server menu		
platform		
system	62	
shut down	109	
shutting down		
expansion server	108	
SIP phones	153	
SSA	70	
SSLVPN		
IPOSS		
restore	115	
startup and availability	140	
support	14	
synchronize passwords	87	
syslog	65	
syslog records	66	
system information	62	
T		
template	59	
templates	59	
training	12	
trunk capacity	125	
U		
untrusted connection	144	
upgrade	101, 104	
automatic	19	
web manager	102	
upgrade policy	98	
USB		
manual	18	
USB installation	17	
user	57	
V		
version	151	
videos	12	

VLAN	61
voicemail	79, 80
capacity planning	133
Voicemail Pro	77
Voicemail Pro client	69
voice recording	
capacity planning	134

W

warning banner	67
Web Manager	
Administrator	84, 86
restarting server	108
starting	20