Deploying IP Office in a Cloud Environment

Release 9.0.3
Issue 1
August 2014

© 2014 Avaya Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

“Documentation” means information published 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 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 OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

Licence types

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

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

with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

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

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

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

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

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products", or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

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 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.

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.

Contents

Chapter 1: Introduction 6
- Purpose 6
- Intended audience 6
- Documentation terminology 6
- Related resources 7
  - Documentation 7
  - Training 8
  - Finding documents on the Avaya Support website 8
  - Viewing Avaya Mentor videos 9
- Support 9
- Using the Avaya InSite Knowledge Base 10

Chapter 2: Overview of IP Office in a Cloud Environment 11
- Topology 12
- Components 14
- Interoperability 16
  - Product compatibility 16
  - Third-party requirements 17
  - Operating system compatibility 17

Chapter 3: Deployment process 18

Chapter 4: Planning and preconfiguration 19
- Checklist: Planning and preinstallation 19
  - Confirming system settings for virtualized deployments 20
  - Subscribing enterprises and ordering user subscription licenses for IP Office Cloud 20
  - Key configuration information 23
  - Required skills and knowledge 24

Chapter 5: Initial setup and connectivity 25
- Checklist: Initial setup and connectivity 25
  - Setting up network connectivity 25
  - Deploying the OVA file for virtualized deployments 26
  - Installing solution components 27

Chapter 6: Configuration 28
- Checklist: Solution configuration 28
  - Launching IP Office Manager 30
  - Configuring your virtual machine 31
  - Configuring Linux Platform settings 32
  - Configuring Cloud settings in IP Office Manager 33
  - Adding a license 36
  - Adding an extension 37
  - Adding a hunt group 37

Comments? infodev@avaya.com

Creating a template..... 38
Applying a template..... 39
Configuring alarms..... 39
Configuring the XMPP domain name in Avaya one-X® Portal for IP Office..... 40
Network and quality of service configuration..... 40
Security..... 42
Chapter 7: Administration..... 45
Monitoring IP Office systems using the System Status application..... 45
Routine maintenance..... 47
Backup and restore policy..... 47
Backing up IP Office components..... 48
Restoring IP Office servers..... 49
Chapter 8: Post-installation verification..... 50
Chapter 9: Troubleshooting..... 51
Glossary..... 53

Chapter 1: Introduction

Purpose

This document contains planning details as well as checklists and procedures for installation, configuration, and administration of IP Office Cloud.

Intended audience

This document is intended for providers to install, configure, and administer the IP Office Cloud solution.

Documentation terminology

The IP Office Cloud documents use the following terminology.

Product names

The following names are used to refer to the Cloud solution.

- IP Office Cloud
- IP Office in a Cloud Environment

Customers

The IP Office Cloud documentation avoids using the term “customer”. Instead, the documentation uses the following terms.

- Enterprise: The organization that consumes the IP Office functionality. IP Office Cloud is targeted for small and medium enterprises.
- Provider: The party hosting the IP Office equipment in the Cloud. The provider supplies the enterprise with the IP Office functionality as a service.

Related resources

Documentation

The following tables list the documents for this solution and other related documents for other products and solutions. Download the documents from the Avaya Support website at support.avaya.com.

Table 1: Related documents for IP Office in a Cloud Environment

Title	Use this document to:	Audience
Overview		
IP Office Server Edition Solution Overview	Obtain a high level functional and technical description of IP Office Server Edition.	• Sales engineers
Reference configuration		
IP Office in a Cloud Environment Reference Configuration	Understand system architecture and network engineering requirements for IP Office Cloud.	• Sales engineers • Architects
IP Office Server Edition Reference Configuration	Understand system architecture and network engineering requirements for IP Office Server Edition.	• Sales engineers • Architects
Implementing and administering		
Deploying IP Office in a Cloud Environment	Understand planning requirements and procedures for installation, configuration, and administration.	• Architects • Implementation engineers • System administrators
Deploying IP Office Server Edition	Understand planning requirements and procedures for installation, configuration, and administration.	• Architects • Implementation engineers • System administrators
Deploying IP Office Server Edition Servers as Virtual Machines	Understand planning requirements, compatibility requirements, and procedures for installation and configuration.	• Architects • Implementation engineers
IP Office Manager	Understand administration tasks performed on IP Office Manager for IP Office Standard Mode and Server Edition.	• Architects • System administrators
Administering Avaya one-X® Portal for IP Office	Understand administration tasks performed on Avaya one-X® Portal for IP Office.	• Architects

Title	Use this document to:	Audience
		• System administrators
Implementing Voicemail Pro on Linux	Understand how to install Voicemail Pro on Linux systems. TheVoicemail Pro server can be installed as part of the IP Office Application Server.	• Architects • Implementation engineers
Administering Voicemail Pro	Understand Voicemail Pro administration tasks.	• Architects • System administrators
IP Office Web Manager for Server Edition and Standard Mode	Understand administration tasks performed on IP Office Web Manager.	• Architects • System administrators

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. 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.

Table 2: Training courses related to IP Office in a Cloud Environment

Course code	Course title
Avaya Implementation Professional Specialist (AIPS) certification	
10S00005E	SMB Implementation ONLY
Avaya Certified Support Specialist (ACSS) certification	
5S00004E	Knowledge Collection Access: SMB Support ONLY
0S00010E	Knowledge Collection Access: SMB Implementation and Support

Finding documents on the Avaya Support website

About this task

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

Procedure

1. Navigate to the Avaya Support website at http://support.avaya.com/.
2. Select the **Downloads & Documents** tab, and select **Documents**.
3. In the **Product** search box, type the product name.
4. Select the appropriate release number from the **Choose Release** drop-down menu.

5. If necessary, use the Content Type filter on the left to select the type of document you are looking for.

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

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 web site, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support web site, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://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 site.

Note:

Videos are not available for all products.

Support

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

Using the Avaya InSite Knowledge Base

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

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

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base at no extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base to look up potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya Web site with a valid Avaya User ID and Password.

   The Support page appears.
3. Enter the product in the **The InSite Knowledge Base** text box.
4. Click the red arrow to obtain the Search Results.
5. Select relevant articles.

Chapter 2: Overview of IP Office in a Cloud Environment

IP Office in a Cloud Environment offers core IP Office telephony and Unified Communications (UC) features to users in small and medium enterprises. Providers host the IP Office equipment in a Cloud data center, and supply IP Office functionality to enterprises as a service. Providers centrally deploy, administer, and maintain the equipment in the Cloud data center, minimizing the equipment required at the enterprise premises.

The IP Office Cloud solution provides the following key benefits:

- Cost savings by reducing the IT complexity of equipment maintenance and operational costs. Virtualization and shared infrastructure also lower the cost to deliver services.
- Flexible delivery options. The enterprise can upgrade or downgrade IP Office telephony and UC services on demand.
- Ability to add and remove users at any time.
- Ease of upgrade. As technology evolves, the enterprise can upgrade without having to purchase and maintain costly equipment.

Multi-instance architecture

IP Office Cloud adheres to a multi-instance architecture for full separation between different enterprises. With the multi-instance architecture in the Cloud, a separate IP Office system is dedicated to each enterprise. The multi-instance architecture provides the following advantages:

- Improved security for the enterprise with partitioned data for voice messages, instant messages, and dial-plans.
- Flexibility for upgrades, maintenance, and Service- Level Agreements (SLAs).
- Enhanced customization options such as scalability and performance.
- Industry-standard resilience through virtualized VMware tools.

Related Links

Topology on page 12
Components on page 14
Interoperability on page 16

Topology

IP Office in a Cloud Environment supports the following deployment models:

- Hosted over Private Network: Requires an MPLS or VPN network connection between the Cloud data center and the enterprise premises. You can optionally deploy an expansion system in the enterprise network. With the survivability option in this deployment model, phones fail over from the expansion system to the primary server when the connection to the expansion system fails. With the IP500 V2 expansion system, you can also use analog and digital endpoints.
- Hosted over Public Network: Uses a public over-the-internet connection between the Cloud data center and the enterprise premises. This deployment includes the following limitations:
  - Expansion systems are not supported.
  - SoftConsole and certain endpoints are not supported.
  - All users connecting to the IP Office Cloud over the Public Network are considered Remote Workers.

Note:

Avaya Session Border Controller for Enterprise is not currently supported in either deployment model.

Figure 1: Hosted over Private Network Topology on page 12 shows a Hosted over Private Network deployment with an MPLS or VPN network connection. This diagram also shows an enterprise site with an expansion system.

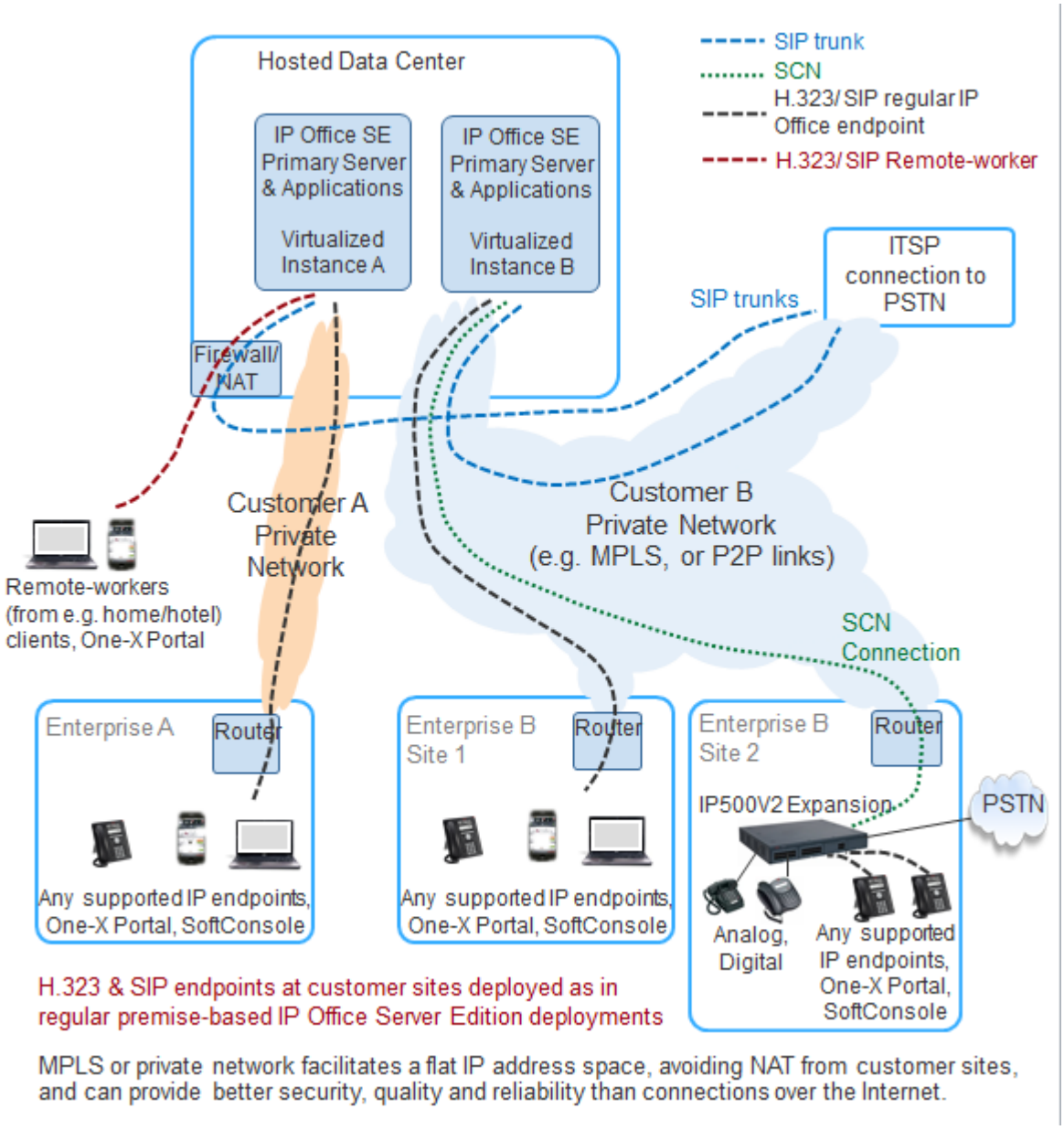


Figure 1: Hosted over Private Network Topology

Figure 2: Hosted over Public Network Topology on page 13 shows the Hosted over Public Network deployment with an over-the-internet connection using NATs. The IP Office Cloud solution supports a one-to-one NAT, which translates IP addresses, but not TCP or UDP ports. The solution supports any kind of NAT at the enterprise site.

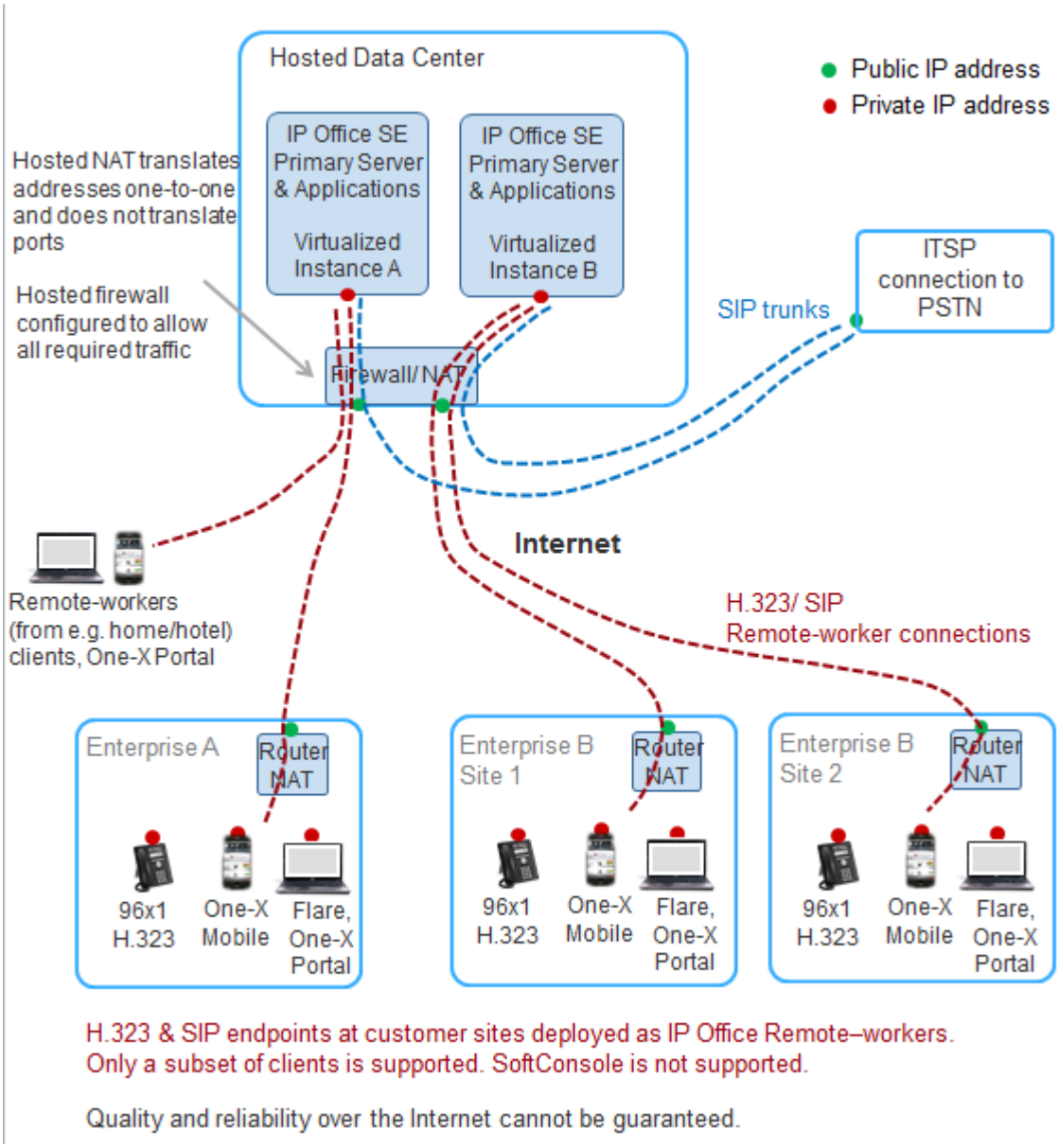


Figure 2: Hosted over Public Network Topology

Related Links

Overview of IP Office in a Cloud Environment on page 11

Components

The following table describes the main components of IP Office in a Cloud Environment. You must use the latest version of all IP Office components listed. For information about the latest supported

version of components, see the Avaya Support Interoperability Matrix at http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Table 3: Components of IP Office in a Cloud Environment

Component	Description
IP Office Cloud Primary server	The primary server for IP Office Cloud. This server provides the following: • IP Office server • Voicemail Pro server • Avaya one-X® Portal and Mobility server • IP Office Manager, including System Status Application • Voicemail Pro client • Client and DevConnect applications such as IP Office Softphone and DevLink • Acts as a central host for licensing, solution directory and time server • Supports remote worker including Avaya one-X® Portal, Avaya one-X® Mobile, and Flare Experience clients • Conference resources for ad-hoc and meet-me conferences • Avaya SoftConsole • Microsoft Office Outlook plugin • Microsoft Lync plugin • Salesforce plugin • Call Assistant
IP500 V2 Expansion System	IP500 V2 expansion system optimized for hybrid analogue or TDM deployments and IP deployments. **Important:** Expansion systems can only be deployed at the enterprise site over a Private Network deployment. You cannot deploy expansion systems in the provider network.
Expansion System on Linux	Expansion System for the IP Office Linux server optimized for IP only deployments. **Important:** Expansion systems can only be deployed at the enterprise site over a Private Network deployment. You cannot deploy expansion systems in the provider network.
IP Office Manager	A Windows software program for IP Office management and configuration. For more information about using IP Office Manager for Server Edition, see *IP Office Manager*.
IP Office Web Manager	Web-based program for IP Office management and configuration. IP Office Web Manager only offers a subset of the IP Office Manager options. You must

Component	Description
	perform most management and configuration tasks in IP Office Manager. You can launch IP Office Manager directly from IP Office Web Manager.

Related Links

Overview of IP Office in a Cloud Environment on page 11

Interoperability

The following sections describe the compatibility requirements for IP Office Cloud. For information about supported releases for products, applications, and endpoints that can interwork with IP Office Cloud, see http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Related Links

Overview of IP Office in a Cloud Environment on page 11
Product compatibility on page 16
Third-party requirements on page 17
Operating system compatibility on page 17

Product compatibility

IP Office in a Cloud Environment requires the following components:

- IP Office Cloud Primary server: The only server deployed in the Cloud.

  You can deploy expansion systems at the enterprise site with the Hosted over Private Network deployment.
- IP Office Manager: A Windows software program for IP Office management, configuration, and user administration.
- IP Office Web Manager: Web-based program for IP Office management and configuration. IP Office Web Manager only offers a subset of the IP Office Manager options.
- IP Office endpoints: IP Office desk phones and soft phones. IP Office Cloud supports both H.323 and SIP endpoints. For example, the 96xx IP desk phones are H.323 endpoints supported in the Cloud, and Avaya one-X® Mobile is an example of a SIP endpoint.

Supported endpoints in the Cloud

All IP Office hard and soft endpoints are supported in the Private Network deployment.

The following endpoints are supported in the Public Network deployment.

- 9608, 9611, 9621, and 9641 series IP desk phones (H.323)
- Avaya one-X® Mobile for iOS and Android (SIP)
- Avaya Flare® Experience for iOS and Windows (SIP)

For details about supported IP Office endpoints, see *Installing IP500 and IP500 V2*, document number 15-601042.

Related Links

Interoperability on page 16
Components on page 14

Third-party requirements

- VMware vSphere: Required for deploying IP Office Cloud with an IP Office Cloud OVA file image in a virtualized VMware vSphere environment. The virtualized server is based on a CentOS Linux server.
- Computer with a compatible operating system and web browser: Required for using IP Office Manager and IP Office Web Manager.

Operating system compatibility

IP Office Manager support

The following server operating systems support IP Office Manager

- Windows Server 2012 (64 – bit only)
- Windows Server 2008/2008R2 (32 – bit and 64 – bit)

The following client operating systems support IP Office Manager:

- Windows 7 (32 – bit and 64 – bit)
- Windows 8 (32 – bit and 64 – bit)

Virtualized Environment support

IP Office in a Cloud Environment can work on a VMware vSphere virtual server platform.

- The minimum required vSphere version is 4.1 Update 2. IP Office supports up to the latest VMware vSphere ESXi 5.5.
- Support includes the Standard, Enterprise, and Enterprise Plus variants of vSphere.

For more information about deploying IP Office Cloud in a Virtualized Environment, see *Deploying IP Office Server Edition Servers as Virtual Machines*, document number – 15-601011.

Related Links

Interoperability on page 16

Chapter 3: Deployment process

The following table shows the high level order of tasks you must perform to deploy and administer IP Office Cloud.

Table 4: Deployment process for IP Office Cloud

No.	Deployment task	Reference
1	Planning tasks, including: • Understanding pre-sales engineering. • Completing required site preparation. • Confirming system settings for VMware. • Obtaining components and licenses. • Ensuring you have all required skills and knowledge before deploying IP Office Cloud.	For detailed information on tasks, see Checklist: Planning and preinstallation on page 19.
2	Initial setup and connectivity tasks, including: • Setting up network connectivity. • Deploying the OVA file and install components.	For detailed information on tasks, see Checklist: Initial setup and connectivity on page 25.
3	Configuration tasks, including: • Configuring your virtual machine. • Completing required configuration tasks in IP Office Manager, IP Office Web Manager, and Avaya one-X® Portal for IP Office. • Configuring network and quality of service settings. • Configuring ports and firewalls.	For detailed information on tasks, see Checklist: Solution configuration on page 28.
4	Additional administration tasks, including: • Monitoring systems. • Backing up and restoring components.	For detailed information on tasks, see Administration on page 45.

Chapter 4: Planning and preconfiguration

Checklist: Planning and preinstallation

The following checklist describes the planning tasks you must perform before installing and configuring the solution.

No.	Task	Notes	✔
1	Understand pre-sales engineering.	You must have an idea of enterprise requirements and the number of users within each enterprise. You can assign users with basic telephony or UC privileges. However, the user must have a license for both the feature packages.	
2	Complete any required site preparation.	Set up the Cloud data center, and make sure your network infrastructure setup allows you to connect the Cloud data center with the enterprise network.	
3	Confirm system settings for virtualized deployments.	None.	
4	Obtain required components.	For information about IP Office Cloud components, see Components on page 14.	
5	Ensure all users are licensed to use IP Office Cloud.	All users must be licensed with a manual subscription process. To obtain licenses, fill out an order spreadsheet and send the completed spreadsheet to productops@avaya.com. **Important:** Finalize the Host name, IP address, and Time zone parameters before ordering licenses.	
6	Understand key configuration details and required skills.	• Review key configuration details forIP Office Cloud. • Ensure you have all required skills and knowledge before deploying IP Office Cloud. You should not attempt to deploy this solution unless you meet all prerequisite requirements defined.	

Related Links

Confirming system settings for virtualized deployments on page 20
Subscribing enterprises and ordering user subscription licenses for IP Office Cloud on page 20
Key configuration information on page 23
Required skills and knowledge on page 24

Confirming system settings for virtualized deployments

About this task

Use the following procedure before you deploy servers for IP Office in a Cloud Environment in a virtualized VMware environment.

Procedure

Before deploying the virtual machine, confirm the following values:

- The host name
- The IP address for LAN 1
- The time zone setting

Important:

Changing the Host name, IP address, and Time zone parameters changes the System ID and affects security settings. If you make any changes to these parameters, you must get new licenses. To avoid this situation, ensure that you decide on these parameters before ordering licenses.

Related Links

Checklist: Planning and preinstallation on page 19

Subscribing enterprises and ordering user subscription licenses for IP Office Cloud

About this task

As a service provider, you need to sign up customers for IP Office Cloud manually. The following procedure provides guidelines on the manual subscription process for this release.

Procedure

1. Work with Avaya Product Management to obtain an order spreadsheet form.
2. Populate the spreadsheet with the required information about the enterprise or customer, and the licensing requirements for each user within the enterprise.

   The spreadsheet includes the following fields:

   - System ID

- Number of Telephony Users and UC Users
- Sold To
- Customer Details

3. Send the completed spreadsheet to productops@avaya.com.

   You can only use a limited number of server provider email addresses to place an order. You must provide the email addresses you will use to productops@avaya.com. Avaya will not honor orders from any other email address.

4. Order the required number of subscription licenses from Avaya.

   Avaya generates the required number of subscription licenses. Avaya will send a manual invoice bill based on the number of subscribed users at the end of every month.

   Note:

   You will still be billed for unused subscription licenses. Licenses cannot be transferred from one enterprise to another.

Next steps

Provision licenses in IP Office as described in Adding a license on page 36.

Packaging and order codes

All IP Office Cloud users must be licensed. Licenses are not applied until you add them in IP Office Manager.

Note:

- Licensing is centralized in the Primary IP Office virtual instance in the Cloud.
- Licenses are unique for Cloud and on-premise deployments, and you cannot reuse licenses across these environments.

Each IP Office Cloud license is generated based on the IP Office System ID. The System ID for virtualization is based on the following parameters:

- Host name
- IP address for LAN 1
- Time zone setting

Important:

Changing the Host name, IP address, and Time zone parameters changes the System ID and affects security settings. If you make any changes to these parameters, you must get new licenses. To avoid this situation, ensure that you decide on these parameters before ordering licenses.

The System ID is displayed in the IP Office Manager Solution view under **System**, and in Web Manager under **Platform**.

The following table describes the IP Office Cloud license packages. You must order the IP Office Cloud bundle and either a UC User or Telephony User license subscription for every user.

Table 5: Material codes and license packages for IP Office Cloud

Material code	License package and name	Available features and supported services	Licenses mapped to the IP Office Cloud license package
None	IP Office in the Cloud base bundle	System-level features: • Audio conferencing with 128 ports • Voice Mail Pro ports • SIP Trunking • SoftConsole Services: One-time, up front, non-refundable, non-cancellable fee per customer to start support services coverage. Avaya provides these licenses for each enterprise with either UC User or Telephony User licenses for each user.	• IP Office Server Edition Quantity – 32 • SIP trunks Quantity – 250 • SoftConsole Quantity – 10 • Voicemail Pro ports Quantity - 200 • CTI Link Pro Quantity - 1 • Third-party endpoints **Note:** Any deployment scenarios that include third-party endpoints require a special request.
307472	IPO CLOUD PRTNR HSTD TELE USR SUBSC Telephony User	Features: • Basic telephony services, such as making and receiving calls • Advanced telephony features, including park and page, call transfer, call forwarding, and voicemail. Services: • 24 x 7 remote technical support including software upgrades	• Avaya IP Endpoint license Quantity - 1
307473	IPO CLOUD PRTNR HSTD UC USR SUBSC Unified Communications User	This package includes the Telephony User features and the following additional features: • Advanced mobile applications • Voice mail to email notifications • Windows and iPad soft phones • Video calling • Instant Messaging and Presence	• Avaya IP Endpoint license Quantity - 1 • Power User license Quantity - 1

Material code	License package and name	Available features and supported services	Licenses mapped to the IP Office Cloud license package
		• SFDC Plug-in • Outlook Plug-in • Lync Plug-in Services: • 24 x 7 remote technical support including software upgrades	

Key configuration information

IP Office security settings contain service users, rights groups, and password complexity rules. These security settings are stored separately from the system configuration settings.

You must implement a DHCP server for IP Office Cloud deployments. IP Office Cloud simplifies system deployment by automatically performing initial start up, ignition, and configuration. As part of the automatic system deployment, the system removes service users that are not required for Cloud. The system also resets the *Administrator* and *security* service user passwords from the standard defaults. After the automatic configuration, the following service users remain in the system security settings:

- security
- Administrator
- EnhTcpaService
- IPDECTService

The new *Administrator* and *security* service user passwords are based on the LAN 1 DHCP address obtained at system launch. The new passwords contain the first four letters of the service user name followed by the LAN 1 DHCP IP address without the dots.

Example

If the LAN 1 DHCP IP address is 192.168.10.25, then the *Administrator* and *security* service user passwords are as follows:

Service user name	Service password
Administrator	Admi1921681025
security	secu1921681025

System ID

The system ID for IP Office Cloud is based on the following configuration information:

- IP Office LAN 1 IP address
- Host name

Comments? infodev@avaya.com

- Time zone

The system ID affects a number of system functions, including licensing. If you change any field used to generate the system ID, all existing licenses in the system become invalid. When the system ID changes, security settings are also reset, and this affects defined service users and their initial passwords.

Required skills and knowledge

You must have the following skills and knowledge to install and configure IP Office Cloud.

- Understand how to use IP Office configuration tools, such as IP Office Manager and IP Office Web Manager.
- Be familiar with virtualized machine deployments and OVA images.
- Be able to set up and use a Dynamic Host Control Protocol (DHCP) server in the provider network. The DHCP server provides the IP address for the primary IP Office Cloud server.
- Know how to deploy IP Office endpoints and applications, such as Voicemail Pro, Avaya one-X® Portal for IP Office, and SoftConsole. This document does not cover installation and configuration of endpoints and applications.

  In a Private Network deployment, endpoints are configured the same way as in a standard on-premise deployment. In a Public Network deployment, you must configure endpoints as Remote Workers. For information about installing and configuring H.323 and SIP endpoints as Remote Workers, see the following documents:

  - *IP Office H.323 Telephone Installation* at http://marketingtools.avaya.com/knowledgebase/businesspartner/ipoffice/mergedProjects/ipphoneinst/index.htm.
  - “VoIP client” in *Administering Avaya one-X® Mobile for IP Office* at http://support.avaya.com/.

Chapter 5: Initial setup and connectivity

Checklist: Initial setup and connectivity

You must install components in your data center and set up connectivity between the data center in the Cloud and the enterprise network. The following checklist outlines installation and network connectivity tasks for IP Office in the Cloud Environment.

No.	Description	Notes	✔
1	Set up network connectivity.	Set up connectivity between the data center in the Cloud and the enterprise site.	
2	Install required virtual machine software and deploy the OVA file.	These tasks are required if you are deploying IP Office in the Cloud with a virtual machine. For more information about virtualized IP Office deployments, see *Deploying Server Edition Servers as Virtual Machines*.	
3	Install solution components.	None.	

Related Links

Setting up network connectivity on page 25
Deploying the OVA file for virtualized deployments on page 26
Installing solution components on page 27

Setting up network connectivity

Before you begin

Complete required site surveys and network infrastructure assessments.

About this task

The following procedure provides guidelines for setting up network connectivity between the provider network and the enterprise site.

Procedure

1. Set up the Cloud data center in the provider network.

2. Install required solution components in the provider network.

   You can optionally install expansion systems at the enterprise site over a Private Network deployment with MPLS or VPN.

3. Make sure you have a Dynamic Host Configuration Protocol (DHCP) server in your network.

   The DHCP server provides the LAN 1 IP address for the virtual primary IP Office. LAN 2 is not currently available in the virtualized image.

4. Connect your provider network to the enterprise site.

   The following network connection options are available for IP Office Cloud:

   - Over a Private Network: This is a secure network connection over MPLS or VPN. You can optionally deploy an expansion system at the enterprise site. Survivability is also supported with this network deployment. With the survivability option, phones fail over from the expansion system to the primary server.
   - Over the Public Network: This network connection only includes the basic IP Office Cloud OVA. Expansion systems cannot be deployed with this network connection. All users are connected to IP Office Cloud over an unsecured public internet connection, and are considered Remote Workers. Signaling and media streams are not encrypted in this deployment.

5. Provide enterprises with required endpoints and equipment that need to be configured at the enterprise site.

Deploying the OVA file for virtualized deployments

Before you begin

- Ensure your virtual machine meets the requirements defined in *Deploying IP Office Server Edition Servers as Virtual Machines*.
- Obtain the required OVA file software for the virtualized machine installation.
- Configure the DHCP server in your network. The OVA instance obtains the IP address for LAN 1 from the DHCP server.

Procedure

1. Access the virtual server from your VMware client.
2. Select **File** > **Deploy OVF Template**.
3. Click **Browse** to navigate to the OVA image file.
4. Select the OVA image file and click **Open**.

   Important:

   You must use an IP Office Cloud OVA image.

5. Click **Next**.

   The system displays the OVF Template Details screen.

6. Use the navigation pane on the left to view the remaining screens.
7. Check the details on each screen and update the details as required.
8. When you are ready to complete the installation, the Ready to Complete screen displays a summary of the deployment settings you selected during the installation.
9. Click **Finish** to complete the installation.

   Once deployment is complete, the new virtual machine appears in the inventory of virtual machines.

Related Links

Checklist: Initial setup and connectivity on page 25

Installing solution components

About this task

The following procedure outlines general steps for installing IP Office Cloud components.

Procedure

1. Install the IP Office Cloud Primary server.
2. Optionally, install expansion systems in the enterprise network over MPLS or VPN.
3. Install IP Office Manager.

   For information about installing and using IP Office Manager, see *IP Office Manager*, document number 15-601011.
4. Install endpoints.
5. Install any other required applications.

Related Links

Checklist: Initial setup and connectivity on page 25

Chapter 6: Configuration

You can complete most IP Office configuration using IP Office Manager and IP Office Web Manager. This document describes the main configuration tasks you can perform in IP Office Manager and IP Office Web Manager. For information about additional tasks you can perform with these tools, see the following documents:

- *IP Office Manager*
- *IP Office Web Manager for Server Edition and Standard Mode*

Important:

Before configuring IP Office Cloud, you must have a DHCP server set up in your network. The DHCP server provides the LAN 1 IP address, which is required for auto-ignition.

The system automatically configures the following parameters:

- LAN 1 network topology public IP address is set to `LAN 1 Address`.
- LAN 1 network topology public UDP port is set to `5056`.
- LAN 2 DHCP Mode is set to `Disabled`.
- System Telephony Maximum SIP Sessions is set to `100`.

The system also configures the following ignition values:

- Host name is set to `ipo90FP<LAN 1 dhcp ip address without dots>`.

  For example: If the LAN 1 IP address is 192.168.10.125, then the host name is `ipo90FP19216810125`.
- Time zone is set to `America/New_York`.
- NTP server is set to `0.pool.ntp.org`.
- Companding law is set to `MULaw`.

Related Links

Checklist: Solution configuration on page 28

Checklist: Solution configuration

The following checklist outlines configuration tasks for IP Office in a Cloud Environment.

No.	Description	Notes	✔
1	Understand how to launch IP Office Manager and IP Office Web Manager.	You must perform most configuration tasks using IP Office Manager and IP Office Web Manager.	
2	Configure your virtual machine.	You must deploy a DHCP server in your network. As part of the virtual machine configuration, the DHCP server performs automatic ignition.	
3	Configure Linux platform settings.	Configure the Linux platform settings for IP Office Cloud using IP Office Web Manager.	
4	Configure settings specific to IP Office Cloud in IP Office Manager.	Verify configuration settings for the Cloud in IP Office Manager. These settings include the following: • Enable H.323 and SIP • Update domain names • Enable ports and modify port numbers as required • Update and manage passwords	
5	Add licenses.	Add user licenses for Cloud using IP Office Manager.	
6	Add extensions.	Add user extensions for each user in the enterprise.	
7	Add hunt groups.	Add required hunt groups using IP Office Manager. A hunt group is a collection of users who are accessible through a single directory number.	
8	Create and apply the required templates.	Create the required profile templates for your server using IP Office Manager.	
9	Configure alarms.	Configure alarm destinations for system events. The system reports events occurring on the various IP Office applications and the control units. You can create multiple event destinations. On each destination, you can specify events and alarms, the method of reporting, and where to send events. Methods of reporting include SNMP, Syslog, or Email.	
10	Configure the XMPP domain name in Avaya one-X® Portal for IP Office.	You must configure the XMPP domain name for mobility applications and Instant Messaging and Presence functionality with Avaya one-X® Portal for IP Office.	

No.	Description	Notes	✔
11	Configure VLAN.	Configure the required VLAN IDs for your network.	
12	Configure quality of service.	Ensure your Cloud network and the enterprise network meet the minimum voice and video quality requirements for: • Network delay • Network jitter • Network packet loss	
13	Configure ports and firewalls.	Port and firewall configurations vary depending on your network connection and the deployment model. This configuration task does not apply if you have an MPLS or VPN connection.	

Related Links

Configuration on page 28
Launching IP Office Manager on page 30
Configuring your virtual machine on page 31
Configuring Linux Platform settings on page 32
Configuring Cloud settings in IP Office Manager on page 33
Adding a license on page 36
Adding an extension on page 37
Adding a hunt group on page 37
Creating a template on page 38
Applying a template on page 39
Configuring alarms on page 39
Configuring the XMPP domain name in Avaya one-X Portal for IP Office on page 40
Configuring VLAN on page 40
Configuring quality of voice requirements on page 41
Configuring the quality of video requirements on page 42
Configuring ports and firewalls on page 42

Launching IP Office Manager

Before you begin

- Start Web Manager.
- Log in as *Administrator*.
- To start Manager using Web Manager, install the Java Runtime Environment (JRE) Oracle version 1.6. or 1.7.x

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 your virtual machine

Before you begin

- You must have a basic understanding of how to deploy IP Office servers on virtual machines. For more information, see *Deploying IP Office Server Edition Servers as Virtual Machines*.
- Configure a DHCP server in your network. The DHCP server provides the IP address for the primary Cloud server. This IP address is required for the system to perform auto-ignition.

About this task

The following procedure provides an overview of the Cloud configuration tasks for virtual machines. The system automatically performs server ignition and sets the following ignition values:

- Host name is set to `ipo90FP<LAN 1 dhcp ip address without dots>`.

  For example: If the LAN 1 IP address is 192.168.10.125, then the host name is `ipo90FP19216810125`.
- Time zone is set to `America/New_York`.
- NTP server is set to `0.pool.ntp.org`.
- Companding law is set to `MULaw`.

Procedure

- Complete the virtual machine profiling.

Profiling allows you to optimize the following resources, which are allocated to meet the actual requirements of the virtual machine.

- Memory: You can set the maximum amount of RAM memory that the virtual machine can use. You can also set how much of that RAM memory the platform guarantees for the virtual machine.
- CPUs: You can configure virtual processors (vCPUs) for a virtual machine. A virtual machine cannot have more vCPUs than the maximum number of logical CPUs on the host virtual server platform. The number of logical CPUs is the number of physical processor cores.
- CPU Clock Cycles: You can set the maximum number of CPU clock cycles that the virtual machine can use. You can also set the number of CPU clock cycles guaranteed for the virtual machine.

For more information, see the Virtual Machine Profiling section in *Deploying IP Office Server Edition Servers as Virtual Machines*.

- Configure IP Office on the virtual machine.

  During this initial configuration, you must ensure that the required settings match the virtual machine and IP Office. The system sets the following parameters:

  - LAN 1 network topology public IP address is set to `LAN 1 Address`.
  - LAN 1 network topology public UDP port is set to `5056`.
  - LAN 2 DHCP Mode is set to `Disabled`.
  - System Telephony Maximum SIP Sessions is set to `100`.

  For more information, see the IP Office Initial Configuration section in *Deploying IP Office Server Edition Servers as Virtual Machines*.

- Copy the required IP Office certificates to the virtual machine.

  1. In IP Office Web Manager, select **Platform** > **Settings** > **General**.

     The **Web Control** section indicates whether an IP Office certificate is available.

  2. Click **Copy Certificate from IP Office**.
  3. Accept the prompts that appear.

     The next time you log in, the **Web Control** section under **Platform** > **Settings** > **General** should indicate that all certificates are up to date.

Related Links

Checklist: Solution configuration on page 28

Configuring Linux Platform settings

Before you begin

Log in to IP Office Web Manager as *Administrator*.

About this task

Use the following procedure to update Linux Platform Settings in IP Office Web Manager. Examples of platform settings you can update are the login banner, host name, and date and time settings.

Important:

Changing the Host name, IP address, and Time zone parameters changes the System ID and affects security settings. If you make any changes to these parameters, you must get new licenses. To avoid this situation, ensure that you decide on these parameters before ordering licenses.

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

Checklist: Solution configuration on page 28

Configuring Cloud settings in IP Office Manager

Before you begin

Log in to IP Office Manager as *Administrator*.

About this task

Use the following procedure to configure settings specific to IP Office Cloud in IP Office Manager. For more information about the IP Office Manager tool, see *IP Office Manager*.

Procedure

- To enable H.323, click **System** > **LAN 1** > **VoIP** > **H.323 Remote Extn Enable**.
- To use SIP hard and soft phones, including mobility applications, click **System** > **LAN 1** > **VoIP** > **SIP Remote Extn Enable**.
- To update the domain name for SIP endpoints, click **System** > **LAN 1** > **VoIP** > **Domain Name**.
- To enable the TCP and TLS ports, click **System** > **LAN 1** > **Network Topology** > **Public Ports needed for TCP/TLS**.

- To change the port number to 5056 for TCP for extra protection against known SIP attacks, click **System** > **LAN 1** > **VoIP** > **Change UDP/TCP Ports**.
- To configure additional alarms, click **System** > **SMTP** > **SMTP Server Configuration for Email for Alarms**.
- To change and control passwords:
  1. To update the security service user password, click **File** > **Advanced** > **Security Settings** > **Security** > **General** > **Security Administrator Password Change**.
  2. To change the security service user password complexity, click **File** > **Advanced** > **Security Settings** > **Security** > **General** > **Service User Details** > **Minimum Password Complexity**.

     Change the security service user password complexity setting to **Medium** or **High**.
  3. Update **File** > **Advanced** > **Security Settings** > **Security** > **General** > **Service User Details** > **Password Reject Action**.
  4. To change the IP Office user password complexity, click **File** > **Advanced** > **Security Settings** > **Security** > **General** > **IP Office User Details** > **Minimum Password Complexity**.

     Change the IP Office user password complexity setting to **Medium** or **High**.
  5. Update **File** > **Advanced** > **Security Settings** > **Security** > **General** > **IP Office User Details** > **Password Reject Action**.
  6. To update the Administrator password, click **File** > **Advanced** > **Security Settings** > **Security** > **Service Users** > **Administrator** > **Change Password**.

Related Links

Checklist: Solution configuration on page 28
Password management best practices on page 34

Password management best practices

Use the following best practices when setting and changing passwords for IP Office Cloud.

- Change default account passwords to be different on all installed systems using IP Office Manager or IP Office Web Manager.
- Set the default password complexity rules to at least Medium. The Low setting does not provide adequate security for the Cloud environment.

Changing the Administrator password using Web Manager

Before you begin

Login as *Administrator* into Web Manager

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**.

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

Before you begin

Start IP Office Manager.

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.

Adding a license

Before you begin

- Ensure that you have received the required Cloud licenses from Avaya.

  Important:

  Changing the Host name, IP address, and Time zone parameters changes the System ID and affects security settings. If you make any changes to these parameters, you must get new licenses. To avoid this situation, ensure that you decide on these parameters before ordering licenses.

- Start IP Office Manager.

About this task

The following procedure describes how to add licenses for IP Office Cloud in IP Office Manager.

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

Checklist: Solution configuration on page 28
Subscribing enterprises and ordering user subscription licenses for IP Office Cloud on page 20
Packaging and order codes on page 21

Adding an extension

Before you begin

Start IP Office Manager.

About this task

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.

Procedure

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

   For more information, see the Configuration Settings section of the *IP Office Manager* document.
4. Click **OK**.

Result

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

Related Links

Checklist: Solution configuration on page 28

Adding a hunt group

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.

Related Links

Checklist: Solution configuration on page 28

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`.

Related Links

Checklist: Solution configuration on page 28

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.

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**.

Related Links

Checklist: Solution configuration on page 28

Configuring alarms

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**.

Related Links

Checklist: Solution configuration on page 28

Configuring the XMPP domain name in Avaya one-X® Portal for IP Office

About this task

Configure the XMPP domain name for mobility applications, and Instant Messaging and Presence in Avaya one-X® Portal for IP Office. For more information about Avaya one-X® Portal for IP Office configuration and administration, see *Administering Avaya one-X® Portal for IP Office*.

Procedure

Click **Configuration** > **IM/Presence** > **XMPP Domain Name**.

Related Links

Checklist: Solution configuration on page 28

Network and quality of service configuration

Configuring VLAN

Before you begin

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

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

Checklist: Solution configuration on page 28

Quality of service requirements

Configuring quality of voice requirements

Before you begin

Set up your network and the enterprise network.

About this task

To get good voice quality, the enterprise network and the provider network must meet certain requirements . If these requirements are met, other factors might still prevent enterprises from getting the voice quality you want. Optimal voice quality is toll quality, but business communication quality is suitable for most enterprises. Business communication quality is not as high as toll quality, but is still better than cell phone quality.

For more information about Quality of Service (QoS) settings, see the Network and quality of service configuration section in *IP Office in a Cloud Environment Reference Configuration*.

Procedure

1. Configure the connection between your network and the enterprise network.
2. Check the voice delay between your network and the enterprise network:
   - Delay of 80 ms or less: Voice is of toll quality
   - Delay between 80 ms to 180 ms: Voice is of business communication quality.
   - Delays exceeding 180 ms: Voice is of lower quality than business communication quality, but this delay might still be acceptable depending on enterprise requirements.
3. To achieve optimal voice quality, ensure that the average jitter is less than half the network packet payload.

   Note:

   This value can vary depending on the service that the jitter buffer has in relation to other buffers and to the packet size used. Assuming the packet size is 20 ms, to prevent problems with voice quality, the network jitter must not exceed 20 ms.
4. Check the network packet loss requirements between your network and the enterprise network:
   - To get toll quality, the packet loss must not exceed 1%.
   - To get business communication quality, the packet loss must not exceed 3%.
   - A packet loss exceeding 3% provides a lower quality than business communication quality. This loss might result in signaling interferences.

Related Links

Checklist: Solution configuration on page 28

Configuring the quality of video requirements

Before you begin

Set up your network and the enterprise network.

About this task

The user network and your network must meet certain requirements to obtain high definition (HD) video quality with IP Office in a Cloud Environment. If these requirements are met, other factors might still prevent user enterprises from getting HD video quality.

For more information about Quality of Service (QoS) settings, see the Network and quality of service configuration section in *IP Office in a Cloud Environment Reference Configuration*.

Procedure

1. Establish a connection between your network and the enterprise network.
2. Ensure that the one-way network delay between the enterprise network and your network is between 80 ms to 180 ms.
3. Ensure that the network packet loss between the enterprise network and your network is less than 0.2 %. A packet loss of 0.2 % or higher negatively affects video quality.
4. Ensure that the network jitter between the enterprise network and your network is less than 20 ms.

Related Links

Checklist: Solution configuration on page 28

Security

Configuring ports and firewalls

Before you begin

Ensure that required firewalls are set up in your network. Firewalls are not part of the IP Office systems.

About this task

Use the following steps to configure ports and firewalls for IP Office in a Cloud Environment. For more information about the ports associated with each IP Office deployment, see the “Port assignments” section in *IP Office in a Cloud Environment Reference Configuration.*

Important:

You must have a firewall to protect your network unless you are using MPLS or VPN. The following procedure does not apply if your network connection uses MPLS or VPN.

Procedure

1. Ensure that the H.323 sets remain connected by setting **NAT UDP Session Timeout** to more than 60 seconds.

2. Open the required ports in your network firewall depending on your deployment model.

   Note:

   If you change these port settings from the defaults, you must also adjust the firewall accordingly.

3. Disable ports that are not secured.

Related Links

Required ports on page 43

Required ports

Table 6: Standard ports in the provider data center

The following table describes the main ports that you should open in the provider data center with a Public Network deployment.

If you choose to configure firewalls in a Private Network deployment, you might need to open additional ports in the provider data center. If you have an expansion system at the enterprise site, you might also need to open ports at the enterprise site network. With a Private Network deployment, additional port configuration is the same as for a standard on-premise deployment. For more information about ports in a Private Network deployment, see the “IP Office Port Matrix” on the Avaya Product Port Matrix Page.

Ports	Direction	Protocol	Description
25	Out	UDP	IP Office Manager email integration. This port depends on the email provider. Some providers operate on different ports.
53	Out	UDP	Domain Name Server (DNS) for name service.
80	In or Out	TCP	Phone configuration, backup, and restore.
123	Out	UDP	Network Time Protocol (NTP).
443	In or Out	TCP	HTTPS for provisioning Avaya soft phone and file transfer.
1718	In	TCP	H.323 Discovery Use this port for remote H.323 client support.
1719	In	UDP	H.323 Status Use this port for remote H.323 client support.
1720	In	TCP	H.323 Signaling Use this port for remote H.323 client support.
5056	In or Out	TCP or UDP	SIP Signaling.
5061	In or Out	TCP	SIP TLS Signaling.
5222	In	TCP	XMPP port for Instant Messaging or for Mobility.
5269	In or Out	TCP	XMPP port for Server to Server Federation.
7070	In	TCP	IP Office Solution Web Manager.
7071	In	TCP	IP Office Solution Web Control.

Ports	Direction	Protocol	Description
8063	In	TCP	Secure web socket-based delivery for Avaya Flare® Experience.
8069	In	TCP	Web socket-based delivery for Avaya Flare® Experience, Outlook plug-in, and Salesforce plug-in.
8443	In	TCP	System Status Application secure access.
8444	In	TCP	One-X Mobility and Flare.
9443	In	TCP	Secure access to Avaya one-X® Portal – Management and User.
47000-54000	In or Out	UDP	The RTP or RTCP ports used for SIP or H.323 media.
50791	In	TCP	Centralized Voicemail Pro.
50794	In	TCP	IP Office Monitor.
50802	In	TCP	TCP Discovery – IP Office Manager.

Chapter 7: Administration

This chapter describes the following administration tasks:

- Monitoring and analysis
- Component backup and restore

You can also perform certain configuration tasks in IP Office Manager on an ongoing basis if required. The tasks you can perform on an ongoing basis include the following:

- Adding and updating licenses
- Adding and updating extensions
- Updating hunt groups
- Creating, applying, and editing templates
- Editing alarms

For more information about IP Office Manager configuration and administration, see the *IP Office Manager* document.

Related Links

Adding a license on page 36
Adding an extension on page 37
Adding a hunt group on page 37
Creating a template on page 38
Configuring alarms on page 39
Monitoring IP Office systems using the System Status application on page 45
Backing up IP Office components on page 48
Restoring IP Office servers on page 49

Monitoring IP Office systems using the System Status application

Before you begin

Ensure System Status is installed and configured.

About this task

Use IP Office System Status to monitor and check the status of systems. System Status connects to systems running IP Office with an IP connection. For more information about deploying and using System Status, see *Using System Status*, document number 15-601758.

Procedure

1. Launch the System Status application.

   You can launch System Status in the following ways:

   - Directly from the **Start** menu on your Windows computer.
   - From IP Office Manager under **File** > **Advanced** > **System Status**.
   - From a web browser, you can enter the IP address for the system and then select the **System Status** link.
   - From IP Office Web Manager.

2. Select the system information you want to view.

   System Status provides information about:

   - System resources, including Voicemail Channels, Conference Channels, Data Channels, VCM Channels, and Modem Channels.
   - Alarms: System Status displays all alarms for any system components. It shows the number of such alarms and the date and time of the last occurrence.
   - Call Details: Information on incoming and outgoing calls; including call length, call reference and routing information.
   - Extensions: System Status lists all extensions on the system, including device type, port location and status.
   - Trunks: System Status lists all system trunks and connections, and shows their status.

   For information about navigating through System Status, see “Screens” in *Using System Status*.

3. Take a snapshot if required.

   Taking a snapshot allows you to capture the System Status details to a file. You can then use System Status to view the saved snapshot. You can take one of the following types of snapshots:

   - Simple Snapshot: This type of snapshot captures the status details that System Status provides. System Status gives this type of snapshot an SSH file extension.
   - Continuous Log: This type of snapshot captures the system's status details over a period of time. System Status gives this type of snapshot an SLO file extension.

Routine maintenance

Backup and restore policy

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

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

  Note:

  backup of an Avaya Linux server does not include any local backup data.
- Security of backup data communication
- Backup prior to any software upgrade
- Retention of backup data for older software versions should a *downgrade* need to be considered.

The period and number of unique instances selected should reflect the frequency of change, the consequence due to data loss, and the storage capacity of the backup data server. Periodic backups using Web Manager have up to 14 instances and a single manual backup instance, after which thesystem overwrites the oldest set. These instances are for each backup server and regardless of the backup data set; for example two weekly separate backup tasks of all IP Office configurations and Voicemail configuration overwrite the first set after 7 weeks.

Backing up IP Office components

About this task

You can back up IP Office servers using Web Manager.

Procedure

1. Log in to Web Manager as an administrator.
2. In the Solution window, select the components you want to back up.
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. Enter a label for the backup if required.

Restoring IP Office servers

Before you begin

Back up the servers.

About this task

You can restore IP Office servers using the backup file of a remote file server in IP Office Web Manager.

Procedure

1. In the Solution window, select the component you want to restore.
2. Click **Actions** and select **Restore**.
3. 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.
4. Under **Get Restore Points**, select the appropriate restore point for the server.

Chapter 8: Post-installation verification

You can use IP Office System Status to verify user extensions, alarms, and trunks that you configured. You should also use System Status to monitor systems on an ongoing basis. For information about monitoring with System Status, see Monitoring IP Office systems using the System Status application on page 45.

System Status provides the following information:

- System resources, including Voicemail Channels, Conference Channels, Data Channels, VCM Channels, and Modem Channels.
- Alarms: System Status displays all alarms for any system components. It shows the number of such alarms and the date and time of the last occurrence.
- Call Details: Information on incoming and outgoing calls; including call length, call reference and routing information.
- Extensions: System Status lists all extensions on the system, including device type, port location and status.
- Trunks: System Status lists all system trunks and connections, and shows their status.

For more information about deploying and using System Status, see *Using System Status*, document number 15-601758.

Chapter 9: Troubleshooting

You can use IP Office System Monitor to assist in the diagnosis of system problems. Through the configuration of settings, the IP Office System Monitor application displays information on a specific area of IP Office operation. You can also capture the information provided to log files for later analysis.

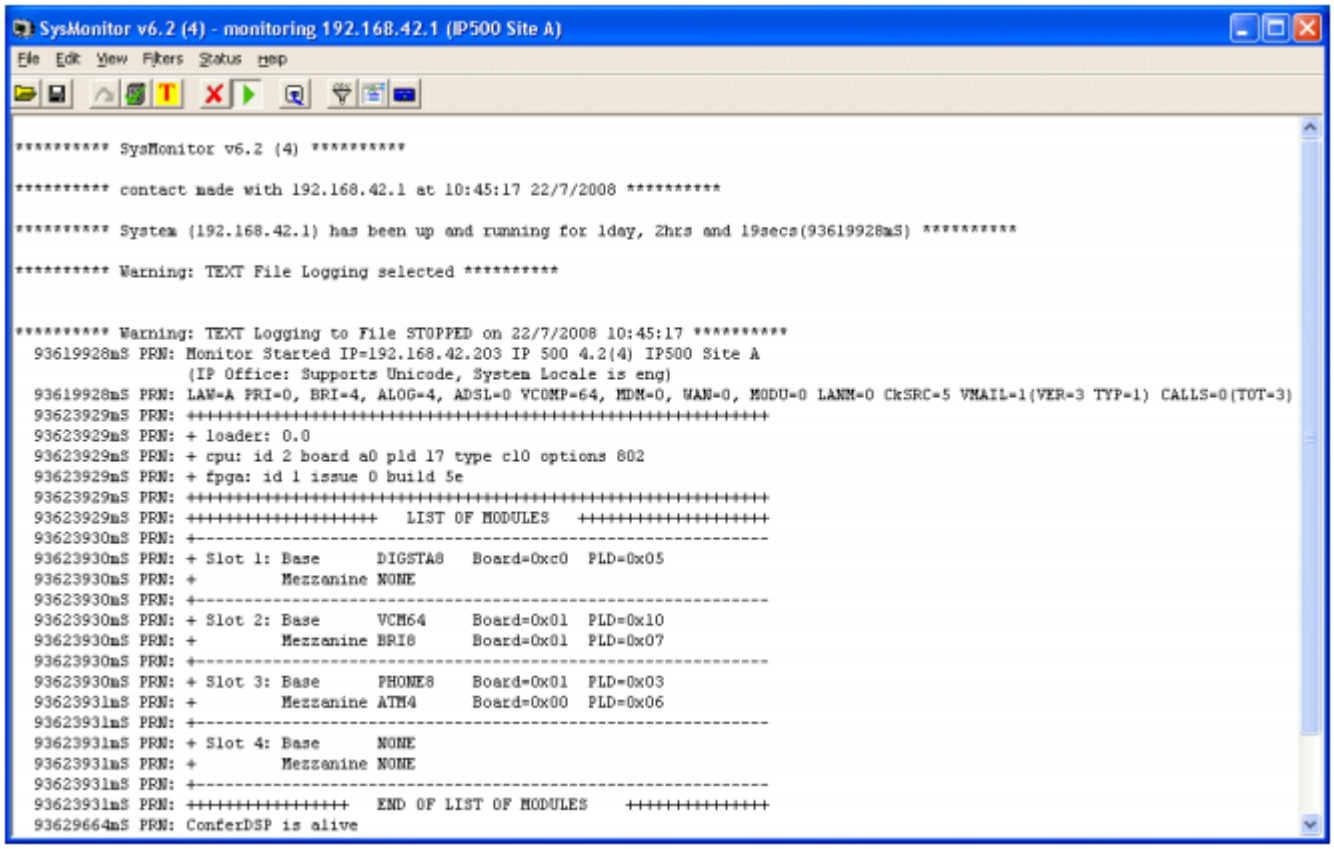


Figure 3: Example of information captured with System Monitor

Consider the following guidelines when using the System Monitor application to troubleshoot IP Office system issues:

- System Monitor is intended primarily for use and interpretation by Avaya support staff. The settings within System Monitor and the information shown in the monitor trace frequently change between IP Office software releases.

- Analysis of the information shown in monitor traces requires detailed data and telecommunications knowledge as well as IP Office knowledge and is not intended for the general user.
- Despite the above facts, if you are maintaining IP Office systems, you must be able to run System Monitor to capture traces for submission with escalated fault reports. You must be able to obtain this detail even if you cannot interpret the trace yourself.

For more information about using IP Office System Monitor, see *IP Office System Monitor*, document number 15-601019.

Glossary

Direct media	Voice travels directly between two endpoints. When direct media is not available, voice and other media elements are anchored through IP Office.
Enterprise	The organization that consumes the IP Office functionality supplied by the provider. IP Office Cloud is targeted for small and medium enterprises.
Hosted over Private Network	IP Office Cloud deployment model that uses an MPLS or VPN network connection between the provider data center and the enterprise premises. You can optionally deploy an expansion system at the enterprise premises. A survivability option also exists in this deployment model where phones fail over from the expansion system to the primary server. This deployment model is also referred to as a Private Network deployment.
Hosted over Public Network	IP Office Cloud deployment model that uses an unsecured over-the-internet connection between the provider data center and the enterprise premises. This deployment model contains only the basic IP Office Cloud OVA. This deployment model is also referred to as a Public Network deployment.
Hunt group	A hunt group is a collection of users who are accessible through a single directory number. Any available member of the group can answer the calls to the hunt group. You can set the order in which calls are presented to the users.
IaaS	Infrastructure as a Service. This is a Cloud computing service model in which the provider outsources required equipment. The equipment belongs to the provider, who stores, maintains, and runs the equipment, while the enterprise is billed based on usage.
MPLS	Multiprotocol Label Switching. A mechanism in high-performance telecommunications networks that directs data from one network node to the next. MPLS uses short path labels rather than long network addresses, avoiding complex lookups in a routing table.
NAT	Network Address Translation. A NAT works like a firewall to protect the internal IP address and differentiate this address from the external IP address.

Provider	The party that hosts IP Office equipment in a virtualized Cloud data center, and supplies IP Office functionality to small and medium enterprises as a service.
Remote Worker	In IP Office Cloud, the term “Remote Worker” refers to the following: • Users connected to IP Office over an unsecured Public Network. • Endpoints configured as remote endpoints. You must configure endpoints over a Public Network deployment as Remote Workers.
TCP	Transmission Control Protocol.
TLS	Transport Layer Security
UDP	User Datagram Protocol. This is a communication method, similar to TCP.
VPN	Virtual Private Network. The VPN extends a private network and its resources across public networks such as the Internet.

Index

A

adding
- extension ... 37
- hunt group ... 37
- license ... 36

administration ... 45
administration settings ... 33
alarms ... 39
applying
- template ... 39

B

back up ... 48
backup and restore policy ... 47

C

change password
- administrator ... 34

changing password
- security administrator ... 35

checklist
- planning ... 19

components ... 14
configuration ... 28
configuration information
- planning ... 23

configure firewalls ... 42
configuring
- alarms ... 39
- Linux Platform settings ... 32
- virtual machine ... 31

configuring video quality ... 42
configuring VLAN ... 40
configuring voice quality ... 41
creating
- template ... 38

D

deployment process ... 18
deploy OVA file ... 26

I

initial setup
- checklist ... 25

InSite Knowledge Base ... 10
install components ... 27
interoperability ... 16

L

launching IP Office Manager ... 30
license ... 36
licensing ... 20, 21
Linux Platform settings ... 32

M

monitoring ... 45

N

network connectivity ... 25

O

obtain subscription licenses ... 20
open ports ... 43
operating system ... 17
overview ... 11

P

packaging and order codes ... 21
passwords
- best practises ... 34

ports ... 42, 43
products
- IP Office ... 16
- third party ... 17

Q

quality of service
- configuration ... 42

Quality of Service
- configuration ... 41

R

related documentation ... 7
restore ... 49
root user ... 35

S

settings
- one-X Portal for IP Office ... 40
- virtualized deployments ... 20

sign up enterprises and users ... 20

Comments? infodev@avaya.com

subscriptions 20
support
    contact 9
System Monitor
    troubleshooting 51
System Status
    monitor IP Office 45

T

terminology 6
topology 12
training 8
troubleshooting 51

U

updating
    IP Office Manager settings 33

V

verification 50
videos 9
VLAN 40