Avaya IP Office™ Platform Security Guidelines

Release 9.1
Issue 01.05
October 2015

Notice

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

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

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

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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 computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

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

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

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

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

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

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

Heritage Nortel Software

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

Copyright

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

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

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

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

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

Purpose

This document provides guidelines for implementing and maintaining IP Office Platform security. It contains an overview of security policy and describes the security tools available to an IP Office Platform solution.

Intended Audience

This document is intended for administrators and support personnel who required knowledge of the available IP Office security tools and information on how to implement an IP Office security policy.

Document Changes Since Last Issue

This is a new document.

Related Resources

Documentation

See the related documents at the Avaya support web site at support.avaya.com and at the IP OfficeKnowledge Base at marketingtools.avaya.com/knowledgebase

- *Avaya IP Office™ Platform Documentation Catalog*
- *Avaya IP Office™ Platform Solution Description*
- *Avaya IP Office™ Platform Feature Description*
- *Administering Avaya IP Office™ Platform with Manager*
- *Administering Avaya IP Office™ Platform with Web Manager*

- *Administering Avaya IP Office™ Platform Voicemail Pro*
- *Administering Avaya IP Office™ Platform Contact Recorder*
- *Administering Avaya one-X® Portal for IP Office™ Platform*
- *Using Avaya IP Office™ Platform System Status Application*
- *Deploying Avaya IP Office™ Platform SSL VPN Services*

Finding documents on the Avaya Support website

About this task

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

Procedure

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

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

Training

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

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

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

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

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

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

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Additional resources

You can find information at the following additional resource websites.

Avaya

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

Avaya Enterprise Portal

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

Avaya IP Office Knowledge Base

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

Avaya maintenance, lifecycle and warranty information

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

Avaya Community

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

Non-Avaya websites

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

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

Product compatibility

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

Support

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

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 website with a valid Avaya User ID and password.

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

Accessing Avaya DevConnect Application Notes

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

Procedure

1. Go to http://www.devconnectprogram.com/site/global/compliance_testing/application_notes/index.gsp.
2. Sign in or register.
3. Click a timeframe to search within.

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

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

   A list of relevant Application Notes appear.

Chapter 2: Overview

The following document is a practical guide to planning, checks, and configuration changes required to help secure the IP Office solution. All IP Office existing and new installations, regardless of usage, must be assessed with the following sections and immediate action taken where indicated.

Implementing these recommendations will substantially reduce the risk of compromise from security threats such as Denial of Service, Toll Fraud and theft of data.

This document does not provide an analysis of security-related topics, define security policy or discuss theory – it also cannot guarantee security. This document does however aim to provide useful and understandable information that can be used by installation, service and support personnel as well as customers to help harden IP Office against attacks.

Disclaimer

Avaya has used reasonable commercial efforts to ensure that the information provided here under is accurate at this date. Avaya may change any underlying processes, architecture, product, description or any other information described or contained in this document. Avaya disclaims any intention or obligation to update or revise the document, whether as a result of new information, future events or otherwise. This document is provided "as is," and Avaya does not provide any warranty of any kind, express or implied.

Information classifications and NDA requirements

Avaya provides security-related information according to the following information classifications.

Classification	Description
Avaya Restricted	This classification is for extremely sensitive business information, intended strictly for use within Avaya. Unauthorized disclosure of this information can have a severe adverse impact on Avaya and the customers, the Business Partners, and the suppliers of Avaya
Avaya Confidential	This classification applies to less sensitive business information intended for use within Avaya. Unauthorized disclosure of this information can have significant adverse impact on Avaya, and the customers, the Business Partners, and the suppliers of Avaya. Information that can be private for some people is included in this classification.
Avaya Proprietary	This classification applies to all other information that does not clearly fit into the above two classifications, and is considered sensitive only outside of Avaya. While disclosure might not have a serious adverse impact on Avaya, and the customers, Business Partners, and suppliers of Avaya, this information belongs to Avaya, and unauthorized disclosure is against Avaya policy.
Public	This classification applies to information explicitly approved by Avaya management as non-sensitive information available for external release.

As this document is generally available, the information herein is considered *Public*. This document contains references to additional information sources that may disclose both confidential and proprietary information and require a non-disclosure agreement (NDA) with Avaya.

Intended Audience

This document is intended for IP Office customers, installation, administration, service and support personnel.

Applicability

The following information is applicable to IP Office IP500 V2, IP Office Server Edition, IP Office applications and endpoints for release 9.1.

IP Office Technical Bulletin 169 covers releases 9.0 and earlier. The document is available from the Knowledge Base at http://marketingtools.avaya.com/knowledgebase/businesspartner/ipoffice/mergedProjects/bulletins/techbulls/tb169.pdf.

The following areas are not covered:

- Physical security
- Non-Avaya component security
- Security policy definition
- Regulatory compliance

Responsibility for IP Office Security

Avaya is responsible for designing and testing all Avaya products for security. When Avaya sells a product as a hardware/software package, the design and testing process of the Avaya product also includes the testing of the operating system.

The customer is responsible for the appropriate security configurations of data networks. The customer is also responsible for using and configuring the security features on IP Office systems, gateways, applications and telephones.

Responsibility for Security Updates

Avaya notifies customers of the availability of security updates through Security Advisories. Customers can subscribe to receive notification about Security Advisories by email. For more information, see Appendix A Security Advisories on page 102.

When IP Office software security updates become available, the customer can install the update or employ an installer from the customer services support group to install the updates. When Avaya installs the updates, the installer is responsible for following best security practices for server access, file transfers, and data backup and restore.

Chapter 3: IP Office Security Fundamentals

All telephony, management, data, services and interfaces offered by the IP Office solution have security features to help prevent security threats such as:

- unauthorized access or modification of data
- theft of data
- Denial of Service (DoS) attacks
- viruses and worms
- web-based attacks such as cross-site scripting and cross-site forgery
- detect of attempted attacks

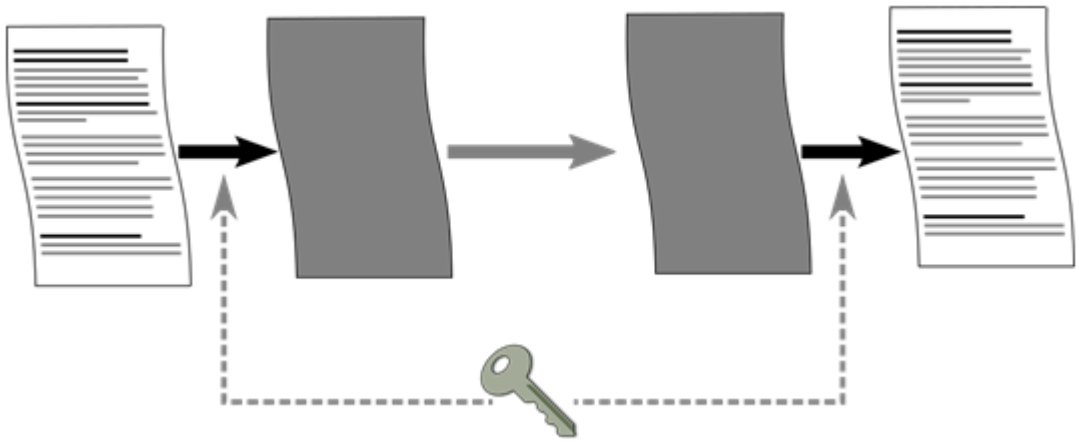
The following table lists methods and techniques used to help counter security threats.

Mechanism	Usage	IP Office Examples
Identification and Authentication	**Identification** is the ability to uniquely identify a user, system or application of a system or an application that is running in the system. **Authentication** is the ability to prove that an entity is genuinely who they claim to be.	Telephony and Service User accounts Message authentication X509 digital certificates
Authorization	**Authorization** protects resources by limiting access only to authorized users, systems or applications.	Telephony and Service User accounts' access controls
Auditing	**Auditing** is the process of recording and checking events to detect whether any unexpected activity or attempt has taken place.	Audit trail System Status Application Alarms Syslog reports
Confidentiality	**Confidentiality** keeps sensitive information private, protecting from unauthorized disclosure.	TLS/SRTP encryption Security database encryption
Data integrity	**Data integrity** detects whether there has been unauthorized modification of data.	TLS/SRTP Message authentication

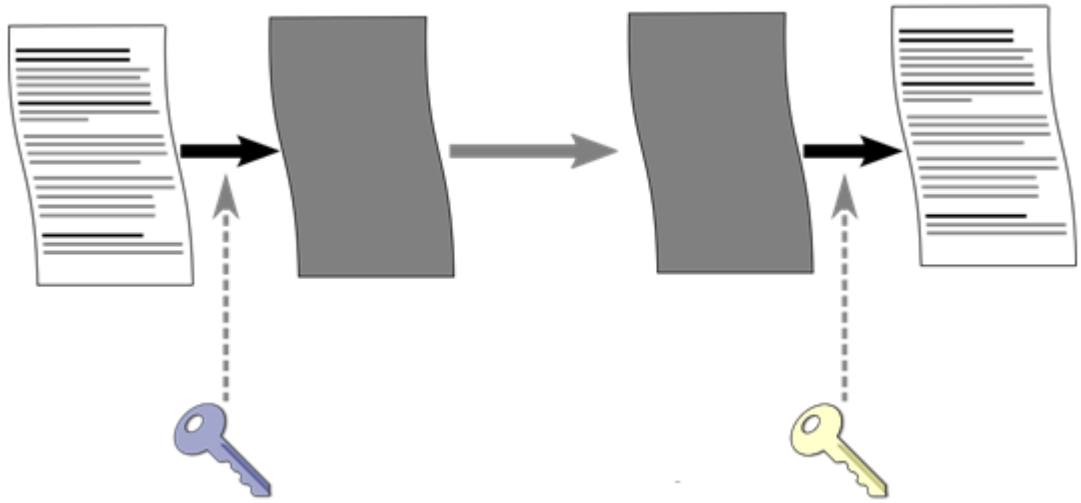
Encryption

Encryption ensures that all data stored on a system or sent by one system to another cannot be "read" by anyone else. There are two main types of encryption.

Symmetric encryption: The application of a mathematical process at the originating end, and a reverse process at the receiving end. The process at each end uses the same 'key' to encrypt and decrypt the data.



Asymmetric encryption: Uses different keys for encryption and decryption. A common usage is a certificate authority's private and public key. For more information, see Certificates and Trust on page 36.



Most message data encryption is symmetric. The data sent may be optionally encrypted using a number of well-known algorithms.

Algorithm	Effective key size (bits)	Use
DES-40	40	Insufficient security.
DES-56	56	Insufficient security.
3DES	112 (AKA two key DES)	Insufficient security.
3DES	168 (AKA three key DES)	'Low' security.
RC4-128	128	'Low' security.

Table continues…

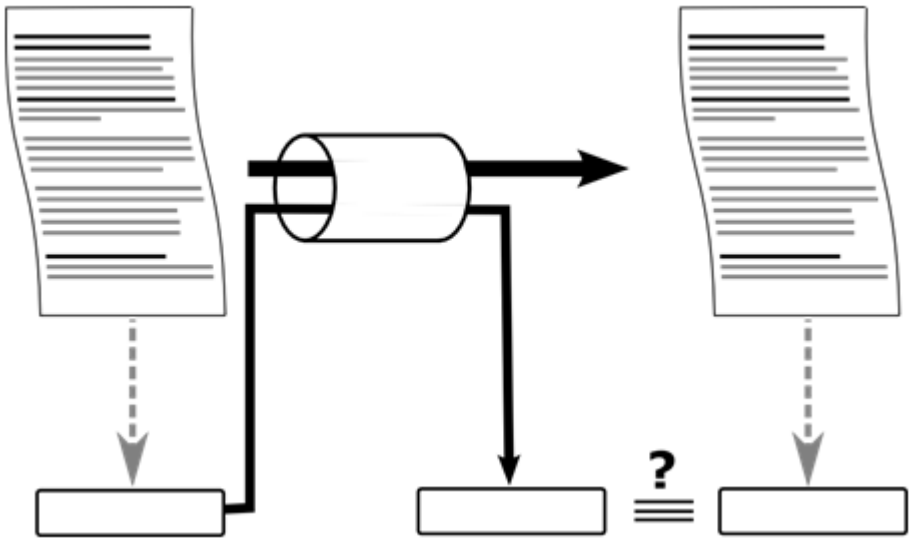
Algorithm	Effective key size (bits)	Use
AES-128	128	‘Medium’ security.
AES-256	256	‘Strong’ security.

In general the larger the key size, the more secure the encryption. However smaller key sizes usually incur less processing.

IP Office supports encryption using the Transport Layer Security (TLS), Secure Shell (SSH), Secure RTP (SRTP) and IPsec protocols.

Message Authentication

Message authentication ensures that all data sent by either the system or Manager cannot be tampered with (or substituted) by anyone else without detection. For message authentication to occur, the originator of the data produces a signature (termed a hash) of the data sent and sends both. The receiver gets the data and the signature, and checks that both match.



Any data sent may be optionally authenticated using a number of well-known and cryptographically secure algorithms.

Algorithm	Effective hash size (bits)	Use
MD5	128	Not supported – insufficient strength
SHA-1	160	‘Low/Medium’ security for message authentication.
SHA-2	224, 245, 384,512	‘Strong’ security

In general the larger the hash size, the more secure the signature. However smaller hash sizes usually incur less processing. IP Office supports message authentication using Transport Layer Security (TLS), Secure Shell (SSH), Secure RTP (SRTP) and IPsec protocols.

Security Database

The IP Office security database controls all local access, plus remote access to other IP Office components. The security settings contained in the database have initial default values and cover the following areas:

- Administrative accounts
- An inviolate security administration account
- Users' password and account policy
- Trusted Certificate Store (TCS)
- Identity certificates
- Received certificate checks
- Service interface security controls
- Legacy interface controls

The security settings are separate from the IP Office configuration settings. They are always secured and cannot be saved or edited offline. The Manager and Web Manager applications can be used to edit the security settings.

In addition to the IP Office security settings, one-X Portal for IP Office, Voicemail Pro, Contact Recorder, WebLM and Web Control have local administrative accounts used under fall-back conditions. See User Accounts and Rights of Access on page 24.

Authentication and Authorization Framework

IP Office has its own Authentication and Authorization (AA) framework, and requests to IP Office services are routed through the AA framework. The AA framework prevents unauthenticated, unauthorized access to IP Office services and data. The following diagram shows the service interfaces covered by this framework.

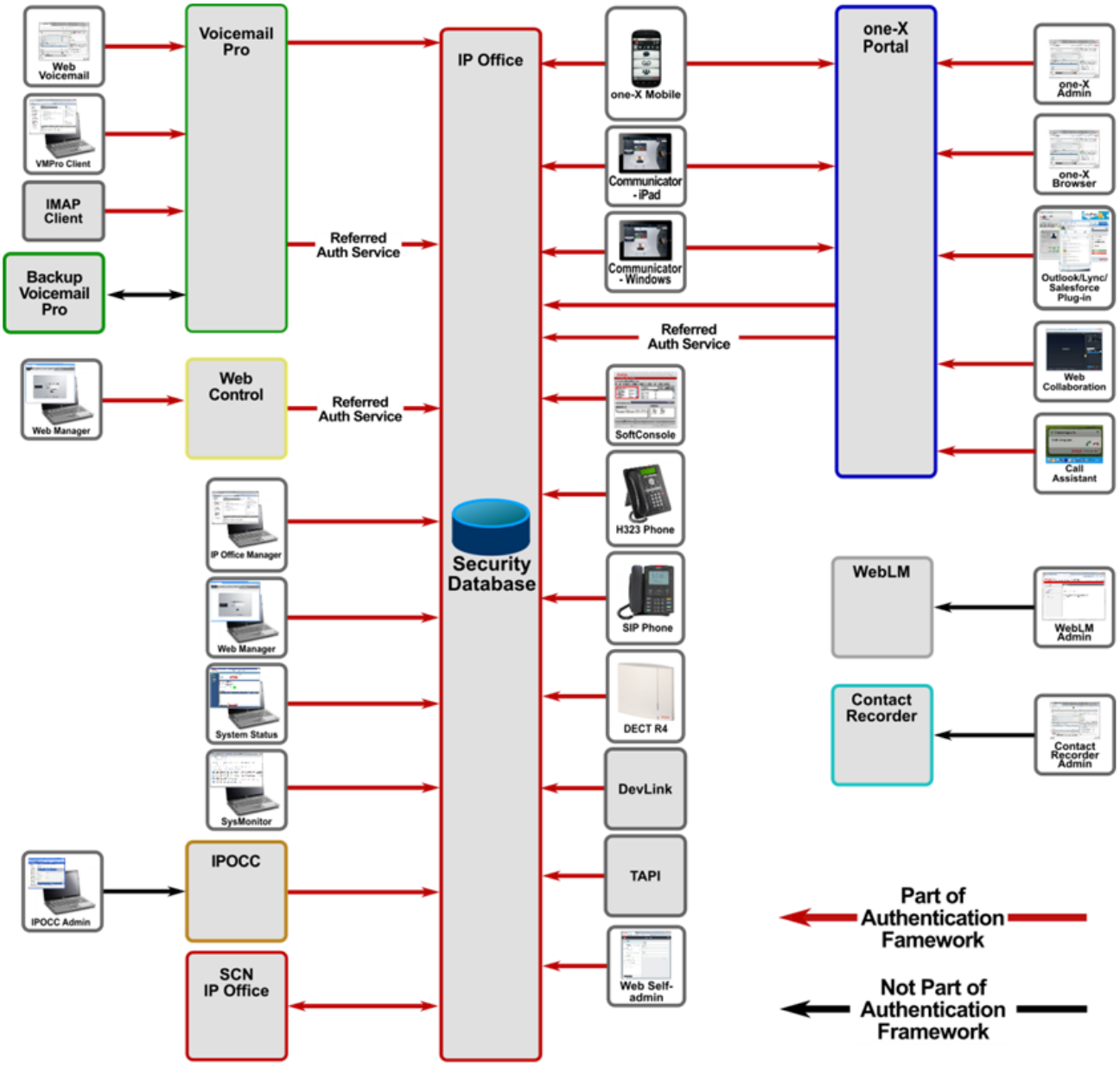


Figure 1: Authenticated Services

Linux one-X Portal, Linux Voicemail Pro, and Web Control refer any administrative login to IP Office via an authentication/authorization web service. Windows one-X Portal and VMPro do not participate.

The following legacy interfaces do not pass through the AA framework:

- TFTP user lists and directories
- TFTP file transfer
- SNMP (no SET operations supported)

These interfaces are disabled by default but can be enabled within an environment secured by other means.

Linux Platform Security

A number of IP Office products run on the Linux operation system. Avaya uses the open-source Linux operating system as a secure foundation for communications. The open source foundation is beneficial for following reasons:

- Security experts worldwide review the source code for defects or vulnerabilities.
- Avaya works diligently to monitor both the enhancements and improvements created by the Linux community and to carefully review the changes before incorporating them into Avaya products.
- Linux-based Avaya servers help protect against many DoS attacks such as SYN floods, ping floods, malformed packets, oversized packets, and sequence number spoofing, among others.

Avaya has modified or hardened the Linux operating system in the following ways to minimize vulnerabilities and to improve security.

- **Minimal installation:** All unnecessary RPMs are removed. In addition to making the software file images smaller and more manageable, the operating system is more secure because attackers cannot compromise RPMs that are not present.
- **Least privilege:** All IP Office applications run as non-root. The root SSH access on is disabled.
- **Ports:** Unnecessary IP ports closed.
- **Linux OS:** Security-Enhanced Linux (SELinux) is enabled, which provides increase security using kernel-level mechanisms that reduce the threat of compromise and limits potential damage from malicious or flawed applications.
- **Firewall protection:** The Linux-based products of Avaya use the IPTables firewall that protects the system against various network-based attacks.
- **Access Security Gateway (ASG) support:** ASG is a challenge-response authentication system that replaces passwords for technical support accounts. When users attempt to log in to a server, the system displays a randomly-generated number instead of prompting for a password. With this randomly-generated number, users perform a calculation to determine the correct response and gain access to the server only after entering the correct response.
- **Drive partition protection:** Processes that can write significant quantities of data to the hard drive such as the backup/restore HTTPS server and Voicemail Pro have quotas assigned to ensure disk space is not exhausted by malicious or unintentional actions.

Third party security and management packages/tools

Several antivirus and other security packages for Linux are available, however Avaya does not support the use of such software on IP Office as it has a level of natural immunity and the packages can severely impact performance.

For more information, see the document *Anti-Virus Policy Statement for Avaya Products Running on the Linux OS* located on the Avaya support site at https://downloads.avaya.com/css/appmanager/css/P8Secure/documents/100156571.

Security Settings Default Values

Defaults values for IP Office security settings are loaded on first startup and on reset. They have a level of security and include enforced password changes for accounts.

Note:

IP Office release 9.0 and earlier require additional changes from default to make them more secure.

It is possible to reset the IP Office security settings using a management interface, the IP500 V2 serial port, or power-on reset buttons. For this reason, it is important to make the IP Office installation physically secure.

For information about IP Office Administrative user defaults see Default Service Users and Rights Groups on page 26. For information about certificate defaults see Initial Certificate Settings on page 43.

The following default security settings are applied to the various IP Office service interfaces.

Interface	Default Setting	Default Security?	Notes
Configuration	Secure, Medium	Yes	IP Office Manager configuration access
Security Administration	Secure, Medium	Yes	IP Office Manager security settings access
System Status Interface	Secure, Medium	Yes	SSA access
Enhanced TSPI	Unsecure Only	No	One-X Portal CTI access
HTTP	Unsecure + Secure	No	Phone and IP Office Manager file access, Voicemail Pro, IP Office Line, SysMonitor (secure)
Web Services	Secure, Medium	Yes	Web Manager and SMGR
TFTP Server	Active	No	Allows access for Manager upgrade and UDP whois discovery
TFTP Directory Read	Inactive	n/a	DECT R4 system directory
TFTP Voicemail	Inactive	n/a	Used for Voicemail Pro R9.0 and prior
Program Code	Active	No	Manager upgrade access
Devlink	Active	No	DevLink and SysMonitor UDP/TCP access
TAPI	Inactive	n/a	1st and 3rd party TAPI interfaces only.

Table continues…

Interface	Default Setting	Default Security?	Notes
HTTP Directory Read	Active	No	One-X Portal directory access, external directory feature
HTTP Directory Write	Active	No	One-X Portal directory access

The local security settings for one-X Portal, Voicemail Pro, IP Office Contact Center, and Contact Recorder may be reset using the Linux console CLI and root access.

Chapter 4: User Accounts and Rights of Access

There are two main types of users in the IP Office solution.

- A telephony user is called an **IP Office User**.
- An administrative user is called a **Service User**.

IP Office users are defined in the main configuration settings. Service users are defined in the security settings.

A special type of Service User is the **Security Administrator**, with permanent access to all security settings. An IP Office system can have no Service or IP Office users configured, but the Security Administrator cannot be removed or disabled.

In order to provide a central authentication database for the Authentication and Authorization (AA) framework, a secure web service is provided by IP Office to other applications. Linux one-X Portal, Voicemail Pro and Web Management use this service to 'Refer' administrative logins to the database.

Service Users

Access to system settings is controlled by **Service Users** and **Rights Groups** stored in the control unit's security settings. These are stored separately from the system's configuration settings. All actions involving communications between Manager and the system require a service user name and password. That service user must be a member of a Rights Group with permissions to perform the required action.

Security Administrator: The security administrator can access the system's security settings and the account cannot be removed or disabled.

In addition a further security setting can force this account to have exclusive security rights, preventing another Service Users from security settings access.

Service Users: Each service user has a name, a password and is a member of one or more Rights Groups. The accounts may be in one of a number of states, including enabled, disabled, locked out and enforced password change.

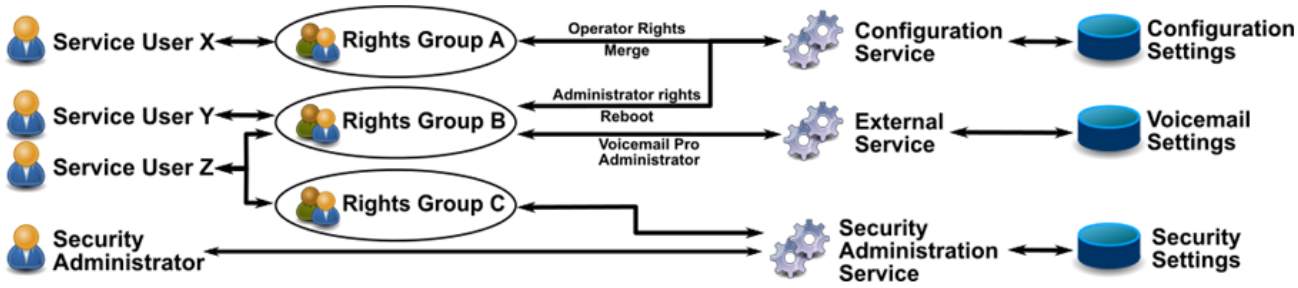
IP Office supports a maximum of 64 Service Users.

Rights Groups: The Rights Groups to which a service user belongs determine what actions they can perform. It can be thought of as a role, but has much more flexibility. Actions available to Rights Groups include configuration, security actions and maintenance actions. Where a service user has been configured as a member of more than one Rights Group, they combine the functions available in the separate Rights Groups.

IP Office supports a maximum of 32 Rights Groups.

Application Roles: In addition to rights of IP Office service access, Rights Groups can also contain 'Roles' for IP Office Manager and Web Manager; the settings of these roles determine what rights of access the Service User has within that application. It allows more granularity of access control within that application than the basic service access rights. For example the IP Office configuration service has two basic rights of access: Read All and Write All. However the Manager Operator roles can further constrain what can be written, viewed or edited.

Example Rights Assignment



In the above illustration:

- Service user X can read and write the configuration. However they can only edit Operator settings and can only make changes that can be merged.
- Service user Y can read and write the configuration, edit all settings and make changes that require reboots or merges. They can also access the Voicemail Pro settings.
- Service user Z can read and write the configuration, edit all settings and make changes that require reboots. They can also access the security and the Voicemail Pro settings.
- The Security Administrator can only access the security settings.

Changing Administrative Users and Rights Groups

IP Office Manager and Web Manager allow modification of Service Users and Rights Groups. Prior to any change, the following should be considered:

- A Server Edition or multi-site IP500 V2 deployment must have consistent Service Users and Rights Groups. IP Office Manager and Web Manager have synchronization tools to assist.
- All changes must follow security best practices such as password policy and minimal rights of access.

Security Settings on Upgrade

When the IP Office system is upgraded and new rights groups or services added, existing users will only be granted the new rights if the Service Users' accounts are at default. This prevents unexpected changes of rights on upgrade. If access to these new rights or services are required, they must be added manually after the upgrade process has been completed.

Default Service Users and Rights Groups

Security Administrator Account

The following Security Administrator account is present on first startup and security settings reset.

Name	Default Account Status	Usage	Rights Group Membership	Notes
Security	Enabled, Force password change	This is the default security administration account. Has all rights to all security management and maintenance services	Implied all security rights	Cannot be removed or disabled

Service User Accounts

The following Service User accounts are present on first start-up and security settings reset.

Name	Default Account Status	Usage	Rights Group Membership	Notes
Administrator	Enabled, Force password change	This is the default account used for system configuration using the IP Office and Web Manager applications, including one-X Portal/Voicemail Pro administration. Has all rights to all management and maintenance services including security settings.	Administrator, System Status, Business Partner	Should not be removed or disabled Should not be renamed
EnhTcpaService	Enabled	This account is used for one-X Portal for IP Office connections to the system.	TCPA Group	Although not enforced, the password should be change as soon as possible in both IP Office and one-X Portal Enable only when one-X Portal deployed
IPDECTService	Disabled	This account is used for DECT R4 system provisioning	IPDECT Group	Enable only when DECT R4 deployed and provisioning mode active
BranchAdmin	Disabled	This account is used for System Manager (SMGR)	SMGR Admin	Enable only when SMGR deployed; will be enabled when the Initial

Table continues…

Name	Default Account Status	Usage	Rights Group Membership	Notes
		access in a branch deployment		Configuration Utility (ICU) run and SMGR administration selected. Must not be renamed
BusinessPartner	Disabled	Similar access rights to Administrator and can be used as a separate account for Business Partners	Business Partner	Should be removed/ disabled unless required
Maintainer	Disabled	Maintenance account without edit configuration or security access. Can be used for Manager (read-only), Web Manager (read-only), System Status Application (SSA), Backup/ Restore, System Monitor, Upgrade	Maintainer	Should be removed/ disabled unless required

Rights Groups

The following Rights Groups are present on first start-up and security settings reset.

Name	Usage	Rights Group User	Notes
Administrator Group	Allows full access to the IP Office Manager application to configure the system. No security or maintenance access	Administrator	All IP Office Manager operations are permitted
Manager Group	Allows limited access to the IP Office Manager application to configure the system.	–	All IP Office Manager operations permitted except: • Delete Short Code • View LAN2 Settings
Operator Group	Allows limited access to the IP Office Manager application to configure the system.	–	All IP Office Manager operations permitted except: • New object creations • View LAN2 Settings • Delete Directory • Delete ICR

Table continues…

Name	Usage	Rights Group User	Notes
System Status Group	Allows limited access to the SSA and Sys Monitor applications.	Administrator	Sys Monitor access right only checked when using service users with Sys Monitor
TCPA Group	This group is used by the one-X Portal for IP Office application.	EnhTcpaService	
IPDECT Group	This group is used by the DECT R4 master base station to extract DECT settings from IP Office.	IPDECTService	
SMGR Admin	This group is used by SMGR to configure IP Office.	BranchAdmin	Do not change the access rights
Security Admin	Allows access to security settings only	–	
Backup Admin	Allows access to all backup and restore services only, including one-X Portal	–	
Upgrade Admin	Allows access to the upgrade service	–	Allows upgrade of both IP Office applications and operating system
System Admin	Allows configuration of IP Office, one-X Portal and Voicemail Pro	–	
Maint Admin	Allows configuration of IP Office, one-X Portal and Voicemail Pro along with backup, restore and upgrade	–	Typically used for maintenance personnel
Business Partner	Full access to all configuration, security and maintenance services.	Administrator, BusinessPartner	
Customer Admin	Web Management , one-X Portal and Voicemail Pro administration	–	No IP Office manager access
Maintainer	Allows configuration view only, along with SSA, Sys Monitor backup, restore and upgrade		Typically used for maintenance personnel with no need for configuration changes

Rights Group Assignment

Service	Access Right	Rights Group						
		• 1 = Administrator Group • 2 = Manager Group • 3 = Operator Group • 4 = System Status Group			• 5 = TCPA Group • 6 = IPDECT Group • 7 = SMGR Admin			
		1	2	3	4	5	6	7
Configuration	Read all configuration	✓	✓	✓				
	Write all configuration	✓	✓	✓				
	Merge configuration	✓	✓	✓				
	Default configuration	✓	✓	✓				
	Reboot/Shutdown immediately	✓	✓	✓				
	Reboot when free	✓	✓	✓				
	Reboot at time of day	✓	✓	✓				
Security Admin	Read all security settings							
	Write all security settings							
	Reset all security settings							
	Write own service user password							
System Status	System Status Access				✓			
	Read all configuration				✓			
	System Control				✓			
	Sys Monitor				✓			
Enhanced TSPI	Enhanced TSPI Access					✓		
HTTP	DECT R4 Provisioning						✓	
Web Services	Security Read All							✓
	Security Write All							✓
	Security Write Own Password							✓
	Config Read All							✓
	Config Write All							✓

Table continues…

Service	Access Right	Rights Group						
		• 1 = Administrator Group • 2 = Manager Group • 3 = Operator Group • 4 = System Status Group			• 5 = TCPA Group • 6 = IPDECT Group • 7 = SMGR Admin			
		1	2	3	4	5	6	7
	Backup							✓
	Restore							✓
	Upgrade							✓
External	Voicemail Pro Basic							
	Voicemail Pro Standard							
	Voicemail Pro Administrator							✓
	One-X Portal Administrator							
	one-X Portal Super User							
	Web Control Administrator							
	Web Control Security							
	WebRTC Administrator							

Chapter 5: Password Management

In general, password resistance to *Guessing* (attacks using default passwords, dictionary words, or brute force) and *Cracking* (attacks that attempt to match the login calculation without needing to know the actual password) can be greatly improved by 'strong' passwords and a password change policy.

A strong password is typically one that:

- Is long (e.g. more than 8 characters)
- Complex (e.g. contains upper, lower and numeric characters)
- Does not contain sequences or repeated characters
- Is not easily guessable. Guessable passwords include:
  - Password same as account name or extension number (or reversed)
  - Dictionary words
  - Dictionary words with number substitution
  - Backwards words
  - Personal or corporate information
  - Date of birth
  - Default passwords

There are many additional sources for information on password strength and management. For example:

- NIST Special Publication (SP) 800-118, *Guide to Enterprise Password Management (Draft)*

  http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf
- Centre for the Protection of National Infrastructure (CPNI), *PROTECTING SYSTEMS AND DATA, PASSWORD ADVICE*

  http://www.cpni.gov.uk/documents/publications/2012/2012029-password_advice.pdf

Password Policy

On a new installation of IP Office, when you first login to Manager or Web Manager, you must change the three system account passwords: Administrator, Security Administrator and system password.

Both Service and IP Office User password policy is configured in the **Security Settings | General** tab of IP Office Manager. The policy settings include:

- Service user minimum name and password length

- Service user minimum password complexity
- Number of consecutive failure attempts and the subsequent action
- Ensure no previous passwords are reused
- Enforced password change – both immediate and periodic
- Idle account time out
- Separate set of IP Office User policy settings to allow differentiation

Administrative User Passwords

There are various accounts used for administrative, maintenance and machine/service access, whose account settings are located in a number of places. The following table lists those interfaces and where the account settings are located.

Login Interface	Account Settings	Notes
• Manager • Server Edition Manager • Web Manager • System Status (SSA) • Web Control • Voicemail Pro client • SysMonitor	Service User name and password. Various rights of access Password: 1-31 Unicode characters	Change using Manager in security settings mode or Web Security Manager. Security settings for Service User password policy apply. SysMonitor will use this account when the **Security | System | Unsecured Interfaces | Use Service User Credentials** is active.
• Manager upgrade	System password Password: 1-31 ASCII printable characters	Change using Manager in security settings mode.
• SysMonitor • DevLink	Sysmon password Password: 1-31 ASCII0-9, a-z, A-Z characters	Change using Manager in security settings mode SysMonitor will use this password when the **Security | System | Unsecured Interfaces | Use Service User Credentials** is inactive
• Voicemail Pro client	Three admin roles: • Administrator • Standard • Basic Password:	Change using VMPro client, Voicemail Pro Administrators tab. Used for Windows Voicemail Pro at all times.

Table continues…

Login Interface	Account Settings	Notes
	5-31 ASCII printable characters except \ / : * ? < > | , ;.	Used for Linux Voicemail Pro as a fallback when IP Office Referred Authentication is not available.
• Contact Recorder	Two admin roles: • System Admin • Restricted Admin Password: 1-99 Unicode characters except space	Change using Contact Recorder web admin page, system tab.
• One-X Portal admin	Two admin roles: • Administrator • Backup/restore Password: 1-31 Unicode characters	Change using one-X Portal admin web page, **Configuration | Users** panel. Used for Windows one-X Portal at all times. Used for Linux one-X Portal as a fallback when IP Office Referred Authentication is not available.
• Linux Secure Shell (SSH)	One admin role: Administrator Password: 1-31 ASCII printable characters	Change using Web Control login screen. Can only change password.
• Linux Console interface (CLI)	Two admin roles: • Administrator • root Password: 1-31 ASCII printable characters	Change using Web Control login screen. Change using Web Control, **Setting | System** tab. Can only change passwords.
• Voicemail Pro, IP Office service interface	VMPro password Password: 1-31 ASCII printable characters	Change using Manager in security settings mode. Change using VMPro client, **System Preferences | General** tab. When zero length (default), IP Office will use the system password.
• One-X Portal, IP Office service interface	Service User name and password Password: 1-31 Unicode characters	Change using Manager in security settings mode or Web Security Manager. Change using one-X Portal admin web page, **Configuration | Providers | Default-CSTA-Provider | Edit** panel.
• TAPI Link Pro (3rd party TAPI)	System password Password: 1-31 ASCII printable characters	Change using Manager in security settings mode.

Table continues…

Login Interface	Account Settings	Notes
		TAPI Link Lite is covered in IP Office User Passwords and Login Codes on page 34.
• DECT R4 Provisioning	Service User name and password Password: 1-31 Unicode characters	Change using Manager in security settings mode. Change using base station web admin interface.

IP Office User Passwords and Login Codes

The following table indicates which IP Office components use what password, voicemail PIN or login code when logging in to the various interfaces.

- **Password** is defined by the configuration field **User | User | Password** and is typically used during application login.
- **Voicemail Code** is defined by the configuration field **User | Voicemail | Voicemail Code** and used for mailbox login.
- **Login Code** is defined by the configuration field **User | Telephony | Supervisor Settings | Login Code** and used for phone login.

  The **Extension | Extn | Phone Password** field (release 9.0+) allows VoIP phone login against the extension, not the user record.

Login Interface	Account Settings	Notes
• SoftConsole • One-X Portal browser • One-X Mobile Preferred • Windows/iPad Flare • IP Office Video Softphone • Outlook plugin, Call Assistant • Salesforce & Lync plugin • TAPI Link Lite (1st party TAPI) • Phone Manager • RAS (dial in) Users	• Name: User | User | Name • Password: User | User | Password • Attributes: 0-31 ASCII 0-9, a-z, A-Z characters	Security settings for IP Office user password policy apply. TAPI Link Pro and DevLink are covered in Administrative Users on page 32. Avaya Communicator (Windows and iPad) can also use the extension number.
• Voicemail Pro mailbox • Embedded Voicemail mailbox	• User extension: User | User | Extension • Voicemail Code:	Voicemail settings for password/PIN policy apply.

Table continues…

Login Interface	Account Settings	Notes
	User | Voicemail | Voicemail Code • Attributes: 0-15 ASCII digits	User's voicemail code input not required if accessing voicemail from a trusted extension.
• IP Office user phone login	• User extension: User | User | Extension • Login Code: User | Telephony | Supervisor Settings | Login Code • Attributes: 0-31 ASCII digits	No password policy settings apply. Temporary lock out upon number of consecutive failed attempts.
• H323 Phone registration • SIP Phone registration	• Phone extension: Extension | Extn | Base Extension • Login Code: User | Telephony | Supervisor Settings | Login Code • Attributes: 0-31 ASCII digits	No password policy settings apply. Temporary lock out upon number of consecutive failed attempts. For R9.0, **H323 Extension | Extn | Phone Password** field is used if set.

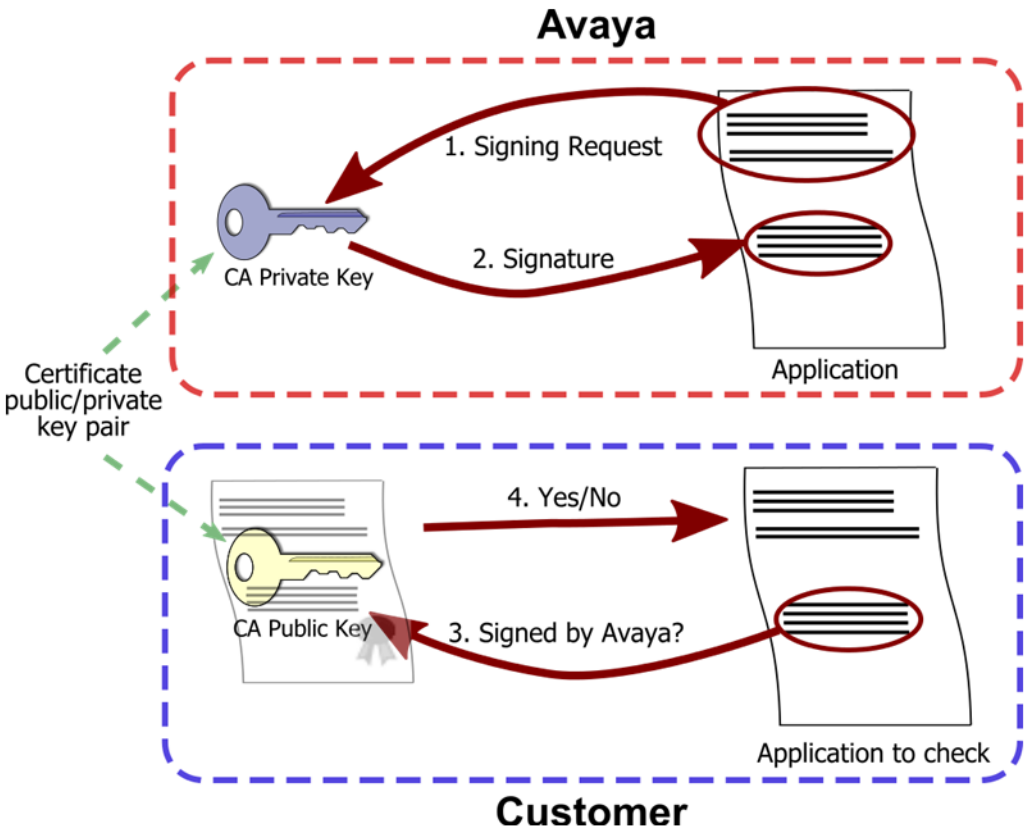
Chapter 6: Certificates and Trust

Digital certificates are used within the IP Office solution for a number of purposes.

- Signing firmware, applications and Java applets to assure their origin.
- Identifying IP Office to other systems, applications and users.
- Verifying the identity of other systems, applications and users.
- Setting up Transport Layer Security (TLS) links, including HTTPS and SIP.
- Incorporating IP Office into a wider trust domain.

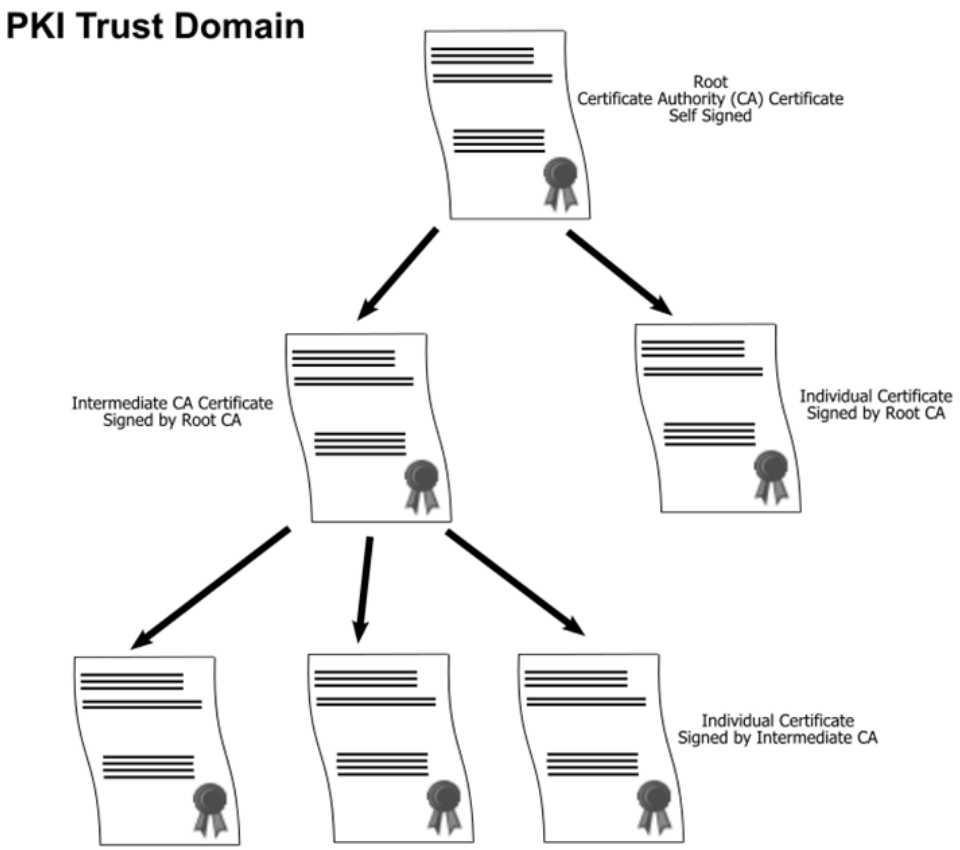
Digital certificates are defined by the X509v3 format and have become the de facto standard for most security operations that involve identity verification. The identity of individuals, systems, and applications can be asserted by a certificate with a ‘public’ key and its corresponding ‘private’ key. The public key is part of the certificate, along with other identity information and other digital security data.

For example, Avaya signs its applications with its private key and makes the corresponding certificate public. To check the application, take the certificate and use the public key to unlock the signature and verify. The private key must remain private, since anyone with access to the private key can masquerade as Avaya.



One point from the above example is that the private key must remain private; anyone with access to the key can masquerade as Avaya.

To ensure greater trust, a trusted party can sign the public key and the information about its owner. A trusted party that issues digital certificates is called a certification authority (CA), similar to a governmental agency that issues drivers' licenses. A CA can be an external certification service provider or a government, or the CA can belong to the same organization as the entities it serves. CAs can also issue certificates to other subordinate CAs, which creates a tree-like certificate trust called a Public-Key Infrastructure (PKI).



Certificate terminology

The following terms and definitions are used in the context of certificates.

- **Certificate**: A digital certificate containing identity information, a public key and other digital security data conforming to the X.509 v3 standard.
- **Certificate Authority (CA)**: An entity that can issue identity certificates signed by another certificate.
- **Root CA Certificate**: A 'self-signed' certificate (i.e., a certificate that has been signed by itself) representing the certificate authority's root of the certificate hierarchy whose private key can be used for signing other certificates. Most operating systems and browsers ship with many root CA Certificates from public authorities that are trusted by default.
- **Intermediate CA Certificate**: A certificate which has been created by signed by CA for the purpose of signing other certificates.
- **Identity Certificate**: A certificate used to represent an entity's identity. To be used as an identity certificate the associated private key must also be present.
- **Trusted Certificate**: A certificate that is trusted by an entity.
- **Trusted Certificate Store (TCS)**: A store of trusted certificates.
- **Trusted Root/Trust Anchor**: The top level certificate that is trusted by an entity.

- **Certificate Chain**: A list of certificates, starting with the Identity Certificate followed by one or more CA certificates (usually the last one being Root CA certificate) where each certificate in the chain is signed by the subsequent certificate.
- **Trust domain**: A single PKI trust structure, e.g. an 'island of authority'.
- **Server Authentication**: The checking of a server's certificate by a client.
- **Mutual Authentication**: The checking of a client's certificate by a server.
- **Certificate Identity Verification**: The source of the certificate (IP address, URL, etc.) is checked against the contents of the certificate's Name and Subject Alternative Name fields.

Certificate Components

Certificates are made up of a number of fields, some mandatory and some optional.

- **Version**: usually V3 – indicating X.509 v3 format
- **Serial Number**: A unique number used to uniquely identify the certificate. There is no requirement that the number is actually serialised, just that it's unique.
- **Subject (AKA Issued to)**: The entity (person, system etc.) identified by the certificate. This is divided into a number of sub fields: Common Name (CN), Organisation Unit (OU), email, etc. Typically the CN is referred to as the 'Name' of the certificate.
- **Subject Alternative Name**: Alternative names by which the entity can be identified. These entries are often tested to assure the recipient the source of the certificate. For example the IP Address of the remote server should match one of the names in this field.
- **Issuer (AKA Issued by)**: The CA entity that verified the information and issued the certificate. This is also divided into a number of sub fields like Subject.
- **Valid From**: The UTC time/date the certificate is first valid from.
- **Valid To**: The expiration time/date.
- **Key Usage**: Purpose for which the public key can be used (e.g. certificate signing, encryption, etc.).
- **Signature Algorithm:** The cryptographic algorithm used to create the signature.
- **Signature:** The signature data to verify that it came from the issuer. Encrypted with the issuer's private key, can be decrypted with the issuer's public key found in the issuer's certificate.
- **Public Key Algorithm**: The public key type (e.g. RSA, DSA etc.).
- **Public Key**: The public key.

There are other fields that may be present. See RFC 5280 for more information.

Certificate Security

The size of the public key and the thumbprint algorithm used determine in part how resistant the certificate is to being compromised. Many government bodies have determined that certificates with MD5 and SHA-1 signature algorithms, or public keys of less than 2048 bits are not secure.

Certificate Checks

When a certificate is received with a view to verifying identity, a number of tests and checks can be carried out.

- The certificate is assessed for basic validity such as integrity, start/end date, usage information, and strength of public key.
- The subject of the received certificate and any alternative names are verified against the source of the certificate. For example, the IP address or the domain name. This is termed “Certificate Identity Verification”.
- The Issuer is extracted and the Trusted Certificate Store (TCS) searched for a certificate that matches. When found the received certificate’s signature is checked using the public key of the trusted certificate. This is repeated until a trusted Root CA certificate is found.
- If revocation information present in the Root CA certificate, the received certificate is checked with the CA to see if it has been revoked (i.e. certificate has be cancelled or withdrawn by the authority).

Due to the variety of implementations, certificate content, configurable setting and heritage, many systems and applications differ greatly in their application of such tests.

Certificates and the Transport Layer Security (TLS) Protocol

Certificates are used by TLS in a number of ways:

- Exchanging the keys used for the symmetric encryption at the beginning of the session
- Verifying the identity of the TLS server
- Verifying the identity of the TLS client

Due to the way TLS works, the server must always have a certificate or else the TLS session cannot start and that certificate is always presented to the client. In order to obtain the client’s certificate, the server must explicitly request it.

Typically the identity verification of both client and server is configurable, along with the exact set of checks carried out on the received certificates. Without such checks TLS can be susceptible to man-in-the-middle attacks.

Certificate File Names and Format

Like many aspects of certificates, there are various options and standards (both formal and informal) associated with certificate files. There are four main encodings/internal formats for certificate files. Note that these are encodings, not file naming conventions.

DER: Distinguished Encoding Rules (DER) format, which is a binary format used to represent a certificate. Typically used to describe just one certificate, and cannot include a private key.

PEM: Privacy Enhanced Mail (PEM) is a Base 64 (i.e. ASCII text) encoding of DER, one certificate is enclosed between '-----BEGIN CERTIFICATE-----' and '-----END CERTIFICATE-----' statements. Can contain a private key enclosed between '-----BEGIN PRIVATE KEY -----' and '-----END BEGIN PRIVATE KEY -----' statements. More than one certificate can be included. PEM can be identified by viewing the file in a text editor. This is an unsecure format and not recommended for private key use unless it is protected with a password.

PKCS#12: Public Key Cryptography Standard (PKCS) #12. A secure, binary format, encrypted with a password. Typically used to describe just one certificate, and its associated private key, but can also include other certificates such as the signing certificates. This is the recommended format for private key use.

PKCS#7: A Base 64 (i.e. ASCII text) encoding defined by RFC 2315, one or more certificates are enclosed between '—BEGIN PKCS—' & '—END PKCS7—' statements. It can contain only Certificates & Chain certificates but not the private key. It can be identified by viewing the file in a text editor.

File Extensions

There are many common filename extensions in use.

- .CRT: Can be DER or PEM. Typical extension used by Unix/Android systems' public certificates files in DER format.
- .CER: Can be DER or PEM. Typical extension used by Microsoft/Java systems' public certificates files in PEM format.
- .PEM: Should only be PEM encoded.
- .DER: Should only be DER encoded.
- .p12: Should only be in PKCS#12 format. Typical extension used by Unix/Android systems' identity certificates/private key pair files. Same format as .pfx hence can be simply renamed.
- .pfx: Should only be in PKCS#12 format. Typical extension used by Microsoft systems' identity certificates/private key pair files. Same format as .p12 hence can be simply renamed.
- .pb7: Should only be in RFC 2315 format. Typical extension used by Microsoft and Java systems for certificate chains.

3rd party tools such as OpenSSL and the Windows Management Console Certificate snap-in can be used to convert between the various formats, but care should be taken not to expose any private key. See Converting Certificate Files on page 135.

IP Office Certificate Support

The IP Office platform supports certificates in a number of ways, most of which are configurable using the security settings.

- An identity certificate for each system and their local applications, including an optional separate identity certificate for management and telephony interfaces.
- Unique identity certificate self-generation by all systems when required.
- Identity certificate can be administered using IP Office Manager or Web Manager, or obtained automatically using the Simple Certificate Enrolment Protocol (SCEP).
- DER and PEM for certificate file import/export, and PKCS#12 for certificate/private key pair import/export.
- A Certificate Authority on the Server Edition Primary Server and the Application Server, including Subject Alternative Name support.
- The certificate processing can support up to 4096 bit public RSA keys, and SHA-2 hashing, as well as the legacy 1024/SHA-1.

  Note:

  one-X mobile for Android does not accept server identity certificate of sha1_1024bit.
- A Trusted Certificate Store (TCS) of 64 entries minimum.
- Configurable default TCS content, restored on security settings reset.
- Individual per-service controls to enforce mutual certificate authentication where the client's certificate is requested and tested.
- Separate management and telephony received certificate check levels that provide increasingly rigorous tests. This includes a 'high' setting that tests not only the trust chain but also the presence of the received certificate in the TCS.
- Intermediate CA certificate support, both for the CAs and the identity certificate chain offered by IP Office and its applications.
- Errors, alarms and warnings to help identify certificate issues.

Currently IP Office certificate support does not include the following.

- Linux Applications (including one-X Portal, Voicemail Pro and Contact Recorder) cannot be configured for mutual authentication. They cannot check any received certificate against the TCS.
- SIP clients' certificates are not requested; the IP Office telephony certificate check settings only apply to SIP Lines and SM Lines.
- The received certificate tests of IP Office do not include revocation checks such as OCSP or CRLs.
- The received certificate tests of IP Office do not include assuring the source of the certificate using Subject Alternative Name entries. That is, certificate identity verification.
- No support for DSA or EC-DSA public key certificates, or RSA public keys above 4096 bits.

  It is recommended to use RSA public keys of 2048 bits.
- IP Office Linux and IP500 V2 servers do not support the manual generation of a Certificate Signing Request (CSR) where the private key is retained within the server. Either a web form

based request or a third party tool to create a CSR can be used. See Appendix H - Text-based Certificate Signing Requests on page 127 for more information on how to generate a CSR for IP Office.

Interface Certificate Support

Certificates are supported on all IP Office TLS and SSH interfaces including HTTPS, whether client or server.

Note:

SSLv2 and SSLv3 are not supported by IP Office.

For information about basic TLS functionality see Certificates and teh Transport Layer Security (TLS) Protocol on page 40.

There are a number of IP Office settings that affect certificate operation

The table in Appendix E Interface Certificate Support on page 115 lists all TLS links in the IP Office platform solution and their security capabilities including certificate support.

The table in Appendix F IP Office VoIP Endpoint Security on page 119 lists VoIP clients in the IP Office platform solution and their security capabilities.

Initial Certificate Settings

IP500 V2

IP500 V2 will always create a unique self-signed CA certificate upon initial start-up and on security settings reset. It will contain the certificate fields listed below.

This certificate can be used for PKI operations in a limited manner. It has some security value, but is not part of a wider PKI and therefore, not trusted by anything else unless this certificate is installed in the relevant TCS.

Certificate Field	Contents	Notes
Version	V3	Always X.509 V3 format
Serial Number	Large random number	Ensures serial number unique Not more than 20 bytes
Subject (Issued To)	CN = ipoffice-*nnnnnnnnnn*.avaya.com O = Avaya Inc OU = GCS	Where: *nnnnnnnnnn* is the LAN 1 mac address, e.g. ipoffice-00e00705918e.avaya.com

Table continues…

Certificate Field	Contents	Notes
	L = Basking Ridge S = New Jersey C = US E = support@avaya.com	
Subject Alternative Name(s)	1: DNS Name=ipoffice-*nnnnnnnnnn*.avaya.com 2: IP Address=a.b.c.d 3: IP Address=e.f.g.h	Where: • *nnnnnnnnnn* is the LAN 1 mac address • a.b.c.d is the LAN 1 IP address at the time of certificate creation • e.f.g.h is the LAN 2 IP address at the time of certificate creation
Issuer (Issued by)	CN = ipoffice-*nnnnnnnnnn*.avaya.com O = Avaya Inc OU = GCS L = Basking Ridge S = New Jersey C = US E = support@avaya.com	Same content as Subject: Self-signed certificate
Valid From	DD/MM/YY HH:MM:SS	Reflects the UTC time/date minus 24 hours when the certificate was created. If the real time clock was corrupt/not set, the time will be fixed to 00:00:00 1st January of the year the software was released.
Valid To	Valid From plus 7 years	
Key Usage	keyAgreement keyEncipherment digitalSignature, nonRepudiation, dataEncipherment keyCertSign	Marked non-critical The certificate can be used for the set of IP Office certificate operations
Extended Key Usage	id-kp-serverAuth id-kp-clientAuth	Marked non-critical The certificate can be used for the set of IP Office certificate operations

Table continues…

Certificate Field	Contents	Notes
Basic Constraints	cA: true pathLenConstraint: 0	Marked critical The certificate can be used in isolation as a CA, no other certificates may be signed by this one
Signature Algorithm	sha256RSA	
Signature	Signature data	
Public Key Algorithm	RSA	
Public Key	Size 2048 bits	

Linux Servers Prior to Ignition

The UCM and default Server Edition distributions before ignition has completed do not have a trusted certificate. In order to connect a browser to ignite, this certificate requires to be temporarily accepted. It should never be stored permanently. It is self-signed and contains a subject and issuer of `ipoffice-default.avaya.com`.

Once ignition has completed, it is replaced by the relevant identity certificate according to the resultant server type.

Server Edition Primary Server and Application Server

The Primary and Application Server have an inbuilt certificate authority. During the ignition process the installer can chose to keep the default CA root certificate used for signing, or import another as a public/private key pair. This imported certificate can either be a root CA or an intermediate CA.

If the internal CA is retained, it has the contents listed below.

Certificate Field	Contents	Notes
Version	V3	Always X.509 V3 format
Serial Number	Large random number	Ensures serial number unique Not more than 20 bytes
Subject (Issued To)	CN = ipoffice-root-*SubjectName*.avaya.com O = Avaya Inc OU = GCS L = Basking Ridge S = New Jersey C = US E = support@avaya.com	Where: - *SubjectName* is the hostname configured during ignition. See **Note 1**.
Subject Alternative Name(s)	1: DNS Name= ipoffice-root-*hostname*.avaya.com	A copy of the Subject CN

Table continues…

Certificate Field	Contents	Notes
Issuer (Issued by)	CN = ipoffice-root-*hostname*.avaya.com O = Avaya Inc OU = GCS L = Basking Ridge S = New Jersey C = US E = support@avaya.com	Same content as Subject: Self-signed certificate
Valid From	DD/MM/YY HH:MM:SS	Will reflect the UTC time/date minus 24 hours when the certificate was created. If the real time clock was corrupt/not set, the time will be fixed to 00:00:00 1st January of the year the software was released.
Valid To	Valid From plus 10 years	
Key Usage	digitalSignature keyCertSign cRLSign off-line cRLSign	Marked non-critical The certificate can be used for the set of IP Office certificate operations
Extended Key Usage		Not present
Basic Constraints	cA: true pathLenConstraint: 1	Marked critical The CA certificate may sign further identity or intermediate CA certificates
Subject Key Identifier	Key Identifier	This value is placed in the Authority Key Identifier of any signed certificates
Signature Algorithm	sha256RSA	
Signature	Signature data	
Public Key Algorithm	RSA	
Public Key	Size 2048 bits	

Notes:

1. The field **SubjectName** is set according to the following process:
   - In Web Manager, if **Platform | Settings | System | Network | Host Name** set to something other than:
     - localhost
     - localhost.localdomain
     - the installer default (mac address)

then use the **Hostname** field.

- If **Hostname** not used, use a DNS resolution of LAN1 if not then LAN2.
- If **Hostname** not used and no successful DNS resolution, use the default name of 'Eth0 mac' e.g. 'ipoffice-root-00e007057307.avaya.com'
- The correct host name should be set during ignition, if not the root CA certificate will need to be regenerated.

Also, as part of ignition, an identity certificate is created signed by the internal CA with the properties listed below.

Certificate Field	Contents	Notes
Version	V3	Always X.509 V3 format
Serial Number	Large random number	Ensures serial number unique Not more than 20 bytes
Subject (Issued To)	CN = *SubjectName* O = Avaya Inc OU = GCS L = Basking Ridge S = New Jersey C = US E = support@avaya.com	Where: - *SubjectName* is the hostname configured or detected. See **Note 1.**
Subject Alternative Name(s)	1: DNS Name= ipoffice-root-DN.avaya.com 2: IP Address=a.b.c.d 3: IP Address=e.f.g.h	Where: • DN is the hostname configured during ignition • a.b.c.d is the LAN 1 IP address at the time of certificate creation • e.f.g.h is the LAN 2 IP address at the time of certificate creation (if present) See **Note 2**.
Issuer (Issued by)	CA certificate subject fields	Certificate signed by the internal CA
Valid From	DD/MM/YY HH:MM:SS	Will reflect the UTC time/date minus 24 hours when the certificate was created. If the real time clock was corrupt/not set, the time will be fixed to 00:00:00 1st January of the year the software was released.
Valid To	Valid From plus 7 years	
Key Usage	keyAgreement keyEncipherment digitalSignature,	Marked non-critical The certificate can be used for the set of IP Office certificate operations

Table continues…

Certificate Field	Contents	Notes
	nonRepudiation, dataEncipherment	
Extended Key Usage	id-kp-serverAuth id-kp-clientAuth	Marked non-critical The certificate can be used for the set of IP Office certificate operations
Basic Constraints	subjectType: endEntity pathLenConstraint: 0	Marked critical Indicates Identity certificate
Authority Key Identifier	Key Identifier	Matches the Subject Key Identifier field of the CA certificate
Signature Algorithm	sha256RSA	
Signature	Signature data	
Public Key Algorithm	RSA	
Public Key	Size 2048 bits	

Notes:

1. The field **SubjectName** is set according to the following process:
   - In Web Manager, if **Platform | Settings | System | Network | Host Name** set to something other than:
     - localhost
     - localhost.localdomain
     - the installer default (mac address)

     then use the **Hostname** field.
   - If **Hostname** not used, use a DNS resolution of LAN1 if not then LAN2.
   - If **Hostname** not used and no successful DNS resolution, use the default name of ‘Eth0 mac’ e.g. ‘ipoffice-root-00e007057307.avaya.com’
   - The correct host name should be set during ignition, if not the root CA certificate will need to be regenerated. Identity certificate regeneration is done automatically if the Web Manager setting **Platform | Settings | General | Certificates | Renew automatically** setting is left at default.
2. The correct LAN 1 and LAN 2 address should be set during ignition, if not the identity certificate will need to be regenerated. This is done automatically if the Web Manager setting **Platform | Settings | General | Certificates | Renew automatically** setting is left at default.

Server Edition Secondary Server and Linux Expansion

The Secondary Server and Linux Expansion do not have an inbuilt certificate authority. The ignition process creates a unique self-signed identity certificate with the properties listed below.

This identity certificate has limited value and should be replaced by one generated by the Primary Server or other external CA.

Certificate Field	Contents	Notes
Version	V3	Always X.509 V3 format
Serial Number	Large random number	Ensures serial number unique Not more than 20 bytes
Subject (Issued To)	CN = *SubjectName* O = Avaya Inc OU = GCS L = Basking Ridge S = New Jersey C = US E = support@avaya.com	Where: - *SubjectName* is the hostname configured or detected. See **Note 1.**
Subject Alternative Name(s)		None
Issuer (Issued by)	CN = *SubjectName* O = Avaya Inc OU = GCS L = Basking Ridge S = New Jersey C = US E = support@avaya.com	Same content as Subject: Self-signed certificate
Valid From	DD/MM/YY HH:MM:SS	Will reflect the UTC time/date minus 24 hours when the certificate was created. If the real time clock was corrupt/not set, the time will be fixed to 00:00:00 1st January of the year the software was released.
Valid To	Valid From plus 7 years	
Key Usage		None
Extended Key Usage		None
Basic Constraints		None
Signature Algorithm	sha256RSA	
Signature	Signature data	
Public Key Algorithm	RSA	
Public Key	Size 2048 bits	

Notes:

1. The field **SubjectName** is set according to the following process:
   - In Web Manager, if **Platform | Settings | System | Network | Host Name** set to something other than:
     - localhost
     - localhost.localdomain
     - the installer default (mac address)

     then use the **Hostname** field.
   - If **Hostname** not set, use a DNS resolution of LAN1 if not then LAN2.
   - If **Hostname** not set and no successful DNS resolution, use the default name of 'Eth0 mac' e.g. 'ipoffice-root-00e007057307.avaya.com'
   - The correct host name should be set during ignition, if not the root CA certificate will need to be regenerated.

Certificate Name Content

The certificate fields **Subject Name** (Common Name field) and **Subject Alternative Name** have particular significance to IP Office and its various clients.

Although IP Office does not process the Subject Alternative Name (SAN) field itself, specific content is required for SIP endpoints and other clients, typically as verification of the certificate's source. See Appendix F IP Office VoIP Endpoint Security on page 119 for more Avaya client information.

When requesting or creating identity certificates for IP Office systems, all connected systems that process the received IP office certificate should be reviewed for their Name and SAN requirements. This should also include any future systems connected within the lifetime of the certificate.

Typical considerations include:

- The system's Fully Qualified Domain Name (FQDN) for the Subject Name. If there is no relevant domain name, a meaningful and unique text name for the system should be considered as this field can be displayed to users. The Name field should not be empty
- The system's Fully Qualified Domain Name (FQDN) as one SAN entry in DNS format. This should always be present if any other SAN entries are required.

  Example: DNS:ipoffice.avaya.com
- Any other domain name or FQDN of the system as one SAN entry in DNS format.

  Example: DNS:avaya.com
- The IP Address of LAN 1 as one SAN entry in IP format.

  Example: IP:192.168.42.1
- The IP Address of LAN 2 as one SAN entry in IP format.

  Example: IP:192.168.43.1

- Any NAT IP Address as one SAN entry in IP format.

  Example: IP: 135.11.53.53

- Any SIP domains in use as one SAN entry for each SIP domain, in DNS format. This is typically the value configured in **Manager | LANx | VoIP | SIP Registrar | Domain Name**.

  Example: DNS:sip.avaya.com

- Any SIP domains in use as one SAN entry for each SIP domain, in URI format. This is typically the value configured in **Manager | LANx | VoIP | SIP Registrar | Domain Name**.

  Example: URI:sip:sip.avaya.com

IP500 V2 and Server Edition Primary/Application server support the creation of certificates with up to 8 SAN fields with the following options:

- DNS: used for hostname or FQDN
- URL: used for URLs and URIs
- IP: IP Address in v4 format
- Email: email address

These SAN fields can also be used for Certificate Signing Requests via SCEP. See Initial Certificate Settings on page 43 for the default Name SAN fields added on initial certificate creation.

For many straightforward deployments only a single FQDN as the subject name is required, such as one-X Portal and Voicemail Pro on Windows, UCM or Application Server where DNS always resolves itself to the same FQDN.

Other deployments where the identity of the system differs depending upon access (e.g. LAN or WAN) or the use of SIP endpoints with secure signalling, SANs will typically be required.

Certificate Check Controls

There are three levels of received certificate checks performed by IP Office on supported interfaces; these apply to any certificate received from any remote TLS client or server.

- **Low**: Only the received certificate is checked for validity and strength. This has no value in determining trust.
- **Medium**: The Low checks are carried out then the TCS is searched for a complete trust chain to a root CA. This is typical of the way browsers check certificates. Note that these tests do not include Certificate Identity Checks using the Name and Subject Alternative Name fields.
- **High**: This will not only perform Low and Medium checks, it will also check that a copy of the received certificate is in the store. This allows a far smaller trust domain to be implemented where only individual certificates are accepted. This is a form of “certificate pinning” and overcomes one of the limitations of the standard tree structure of PKI; every certificate issued by the root CA is always trusted.

See *Administering Avaya IP Office™ Platform with Manager* for a detailed list of checks performed.

The extended 'High' trust checks are activated with the settings:

- Manager **Security | System | Certificates | Received Certificate Checks (Telephony)** = High.

  Applies to all certificates received on the SIP-TLS interfaces.
- Manager **Security | System | Certificates | Received Certificate Checks (Management)** = High.

  Applies to all certificates received on the Management TLS and HTTPS interfaces.
- Manager **Configuration | Line | Line | Security** = High.

  Applies to certificates received on that IP Office WebSocket Line, regardless of the management received certificate checks (WebSocket Lines use the IP Office HTTP/S server).

Mutual Authentication

Where IP Office acts as a TLS/HTTPS server, certain security settings activate a certificate request from the client. If no certificate is received, the IP Office will reject the connection. If a certificate is received, certificate checks will be applied. This is the main mechanism used to enforce trust checks by IP Office.

Mutual authentication is activated with the settings listed below.

- Manager **Security | Services | Configuration | Service Security Level** = High.

  Applies to IP Office Manager configuration settings and Configuration Web Service DevConnect interfaces.
- Manager **Security | Services | Security Administration | Service Security Level** = High.

  Applies to IP Office Manager security settings.
- Manager **Security | Services | HTTP | Service Security Level** = High.

  Applies to HTTPS clients connecting to port 443 and 411, typically H323 phones, DECT R4, IP Office lines, Voicemail Pro, and SysMonitor.
- Manager **Security | Services | Web Services | Service Security Level** = High.

  Applies to Web Manager interface.
- Manager **Security | System | Certificates | Received Certificate Checks (Telephony)** = Low, Medium or High.

  Applies to SIP and SM Lines.
- Manager **Configuration | Line | Line | Security** = High.

  Applies to IP Office Lines.

There are three levels of received certificate checks performed by IP Office on supported interfaces. These apply to any certificate received.

- **Low**: Only the received certificate is checked for validity and strength. This has no value in determining trust.
- **Medium**: The Low checks are carried out then the TCS is searched for a complete trust chain to a root CA. This is typical of the way browsers check certificates. Note that these tests do not include Certificate Identity Checks using the Name and Subject Alternative Name fields.
- **High**: This will not only perform Low and Medium checks, it will also check that a copy of the received certificate is in the store. This allows a far small trust domain to be implemented

where only individual certificates are accepted. This overcomes one of the limitations of the standard tree structure of PKI; every certificate issued by the root CA is always trusted.

See *Administering Avaya IP Office™ Platform with Manager* for a detailed list of checks performed.

The extended **High** trust checks are activated with these settings:

- Manager **Security | System | Certificates | Received Certificate Checks (Telephony)** = High.

  Applies to all certificates received on the SIP-TLS interfaces.

- Manager **Security | System | Certificates | Received Certificate Checks (Management)** = High.

  Applies to all certificates received on the Management TLS and HTTPS interfaces.

- Manager **Configuration | Line | Line | Security** = High.

  Applies to certificates received on that IP Office WebSocket Line, regardless of the management received certificate checks (WebSocket Lines use the IP Office HTTP/S server).

For additional information, see Appendix E Interface Certificate Support on page 115.

Certificate Distribution

Identity Certificate Distribution

IP Office supports three main mechanisms to distribute identity certificates, the selection of which will depend upon the trust policy chosen. One unique identity certificate is required for each IP Office – two if a separate telephony trust domain is required.

In all cases (External CA, Internal CA, SCEP), when a new identity certificate is received by IP Office, all relevant interfaces/applications are updated. This will cause service loss on one-X Portal and Voicemail Pro, but not IP Office itself.

Manual from an External CA

A manual signing request (CSR) is created and sent to an external CA who verified the contents and creates an identity certificate signed by the CA. Once the identity certificate/private key is obtained, Manager or Web Manager can be used to administer it on IP Office.

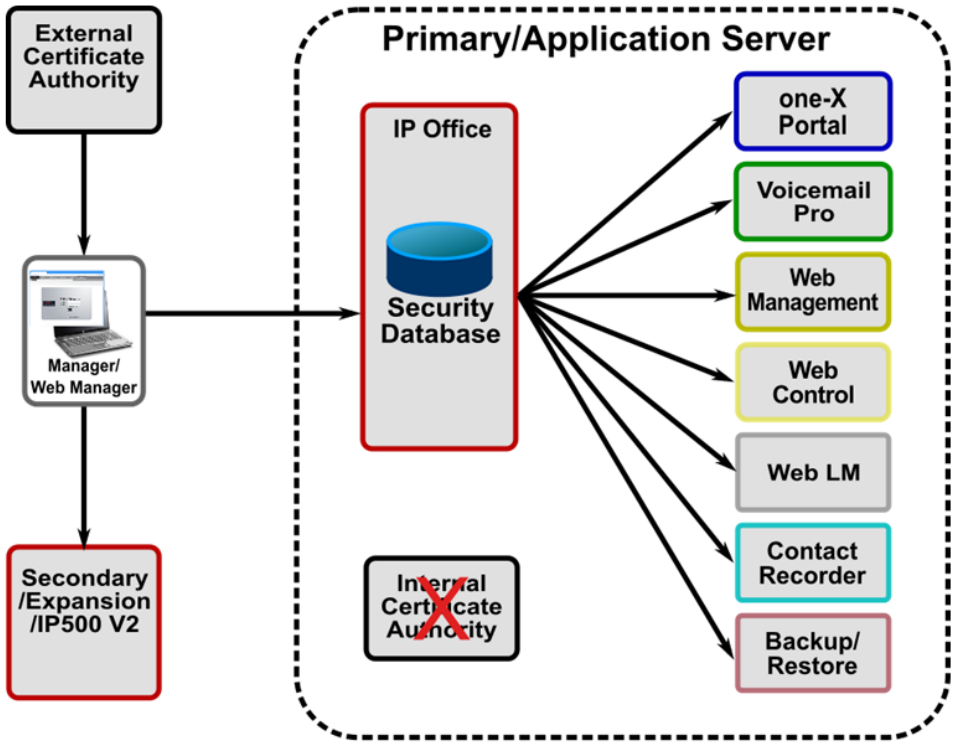


Figure 2: External Certificate Authority

For more information on creation of a PKI based on an External CA, see Implementing IP Office PKI on page 60.

For more information on external Certificate Authorities, see Certificates from External Certificate Authorities on page 62.

Manual from the Primary Server or Application Server

The internal certificate authority can be used to create a set of unique identity certificates in a secure PKCS#12 file format. The PKCS#12 file also includes the CA certificate. These identity certificates can be utilized for any entity including IP Office, phones, Manager PCs, etc. Once the identity certificate/private key file is saved to the local PC, Manager or Web Manager can be used to administer it on IP Office.

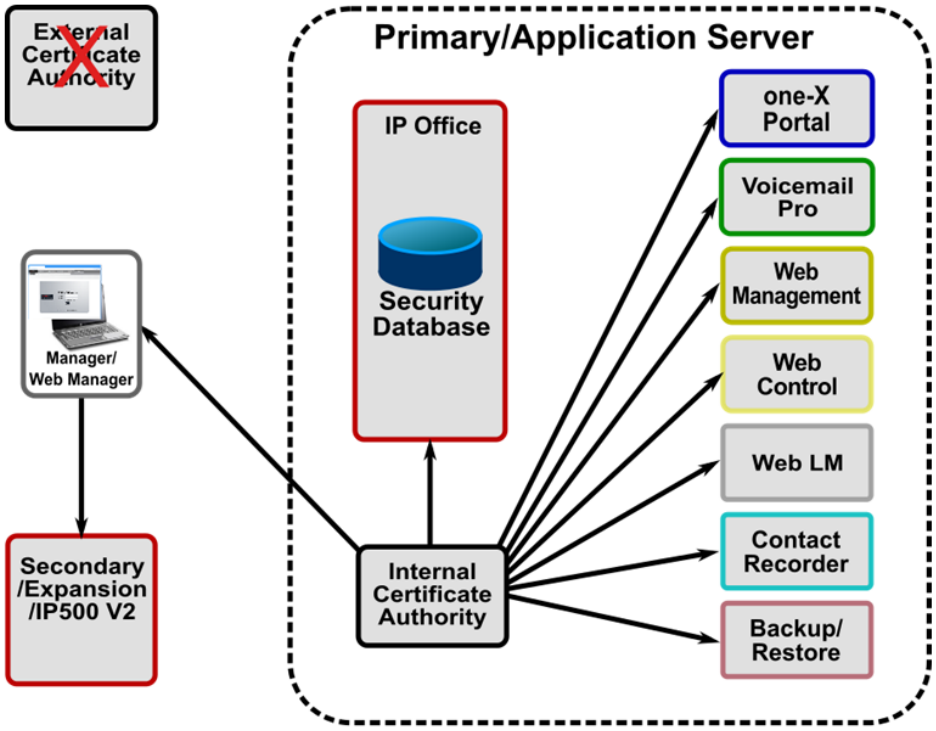


Figure 3: Internal Certificate Authority

For more information on creation of a PKI based on an internal CA, see Implementing IP Office PKI on page 60.

Automatic using Simple Certificate Enrolment Protocol (SCEP)

Each IP Office is configured with the location of the SCEP server along with a password. The IP Office will periodically perform a CSR until it obtains its identity certificate. The private key is kept internally. The SCEP server must be administered to accept the signing request and issue the correct certificate. As part of the enrolment process the CA certificate used to sign the SCEP request is placed into the TCS after which the IP Office will trust any other certificate signed by that CA. This is the mechanism used in IP Office branch deployments with System Manager (SMGR).

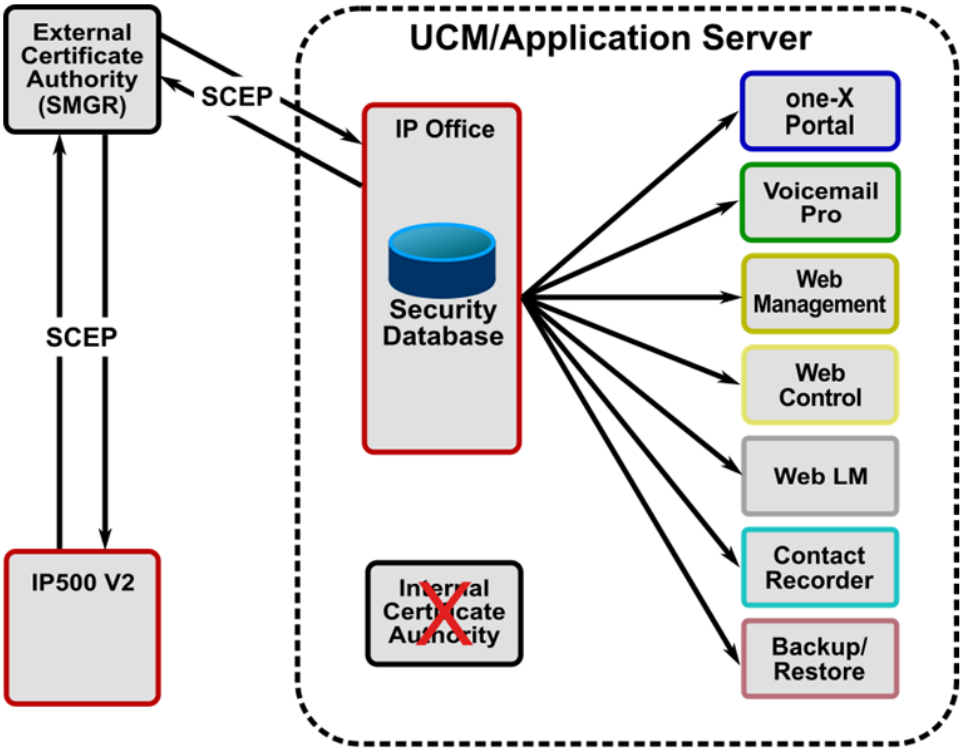


Figure 4: Simple Certificate Enrollment Protocol

In all cases (External CA, Internal CA, SCEP), when a new identity certificate is received by IP Office, all relevant interfaces/applications are updated.

For more information on creation of a PKI based on SCEP, see Implementing IP Office PKI on page 60.

Root CA Certificate Distribution

If the trust policy selected uses a well-known public CA (such as Verisign™), their root certificates are typically already installed in the relevant operation systems and browsers. However, IP Office does not have well-known public CA certificates in its TCS – these can be downloaded from the CA's web site and manually administered via Manager or Web Manager for each IP Office.

For more information on Root CA Certificate distribution, see Implementing IP Office PKI on page 60.

Intermediate CA Certificate Distribution

If the trust implementation additionally uses Intermediate CA certificates, the IP Office certificate chaining feature can be activated and the Intermediate CA(s) needs to be added to the TCS. This ID certificate chain is propagated to all local TLS interfaces. This will remove the need to administer Intermediate CA certificates in the various clients' trusted certificate stores.

For more information on Intermediate CA Certificate distribution, see Implementing IP Office PKI on page 60.

Determining Trust Policy

With today's secure communication requirements, it is not possible to ignore the use of certificates to implement trust relationships, even if the identified needs are minimal. A trust policy must be selected and implemented before exposing IP Office services. This section provides some information to assist in the determination of such a policy; however it cannot provide definitive guidance or include outside factors.

Note:

IP Office branch deployments have a specialized environment and requirements. See the documents

- *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*
- *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*
- *Avaya IP Office™ Platform in a Branch Environment Reference Configuration*

The following questions are applicable when considering a trust policy for IP Office.

- What international, national, corporate or other trust requirements exist?
- Is there an existing trust/PKI infrastructure that IP Office should be part of?
- Are IP Office services being exposed on public interfaces?
- Are IP Office platform components deployed on unsecure platforms or environments?
- Are IP Office clients/endpoints deployed on unsecure platforms or environments?
- What are the trust requirements for 3rd party systems that connect to IP Office?
- Is the ability to trust IP Office without administering certificates on clients/endpoints significant?
- Is there a need for a separate management and telephony trust domain?
- Which interfaces and services need to use trust checks and which do not?
- Does trust need to be one-way (e.g. client checks sever), or both-way (e.g. client and server check each other)?
- Is there a need to provide the extended trust checks of IP Office where all clients' certificates must be present in the TCS? This is useful when the PKI tree trust structure is insufficient.
- How many ID certificates are required? At least one unique certificate per IP Office server, two if a separate telephony trust domain is needed?
- How are certificates to be obtained and distributed and recovered?
- What certificate renewal and distribution methods should be supported?
- Is the CA able to provide the correct certificate content? For example Subject Alternative Name content?

This list is not exhaustive. For further information, see Assessing IP Office Platform Security Requirements on page 74.

There are five main approaches that can be used with the IP Office Platform.

- PKI Trust domain based on the Primary or Application Server internal root CA.

- PKI Trust domain based on the Primary or Application Server internal Intermediate CA.
- PKI Trust domain based on an external Certificate Authority.
- PKI Trust domain based on an external Certificate Authority via SCEP.
- No PKI trust domain.

Approach 1: PKI Trust Domain Based on Primary Server or Application Server Internal Root CA

This option allows identity certificates to be generated using the root CA certificate of the server. Relative advantages include:

- Cost over a commercial CA.
- Control of the CA is internal.
- Certificate content format compatible with other Avaya components.
- The certificate policy is flexible and not subject to commercial considerations.
- The trust relationships do not extend outside of the deployment – i.e. it remains a private domain.

Relative disadvantages include:

- The root CA certificate is untrusted by 3rd parties and other IP Office components and therefore needs to be distributed.
- The certificate creation and distribution process is manual.

Approach 2: PKI Trust Domain Based on the Primary or Application Server Internal Intermediate CA

This option allows identity certificates to be generated on the Primary or Application Server using an intermediate CA certificate obtained from an external Certificate Authority.

Potential advantages for intermediate CA certificate on the Primary/Application Server:

- Generated ID certificates are part of a wider trust.
- Control of the CA is internal.
- ID certificate content format compatible with other Avaya components.
- ID certificates with private domains and address ranges IP addresses can be created.
- The root CA certificate is (typically) trusted by 3rd parties and therefore does not need to be distributed.

Potential disadvantages include:

- Cost, if using a commercial provider. Signing certificates are typically more expensive.
- The certificate policy is subject to commercial considerations.
- The root CA certificate is untrusted by IP Office components and therefore needs to be distributed.
- The certificate creation and distribution process is manual.
- All clients need to support certificate chains in the TLS exchange. If not, the intermediate CA certificate needs to be distributed.

Approach 3: PKI Trust Domain Based on an External Certificate Authority

This option allows identity certificates to be obtained direct from an external Certificate Authority using a manual process.

Potential advantages for identity certificates from an external CA:

- Useful for small deployments when no Primary or Application Server exists – for example a Windows server running one-X Portal or Voicemail Pro.
- Generated ID certificates are part of wider trust domain.
- The root CA certificate is (typically) trusted by third parties and therefore does not need to be distributed.

Potential disadvantages include:

- Public certificate authorities will not issue certificates for private domains or address ranges.
- Cost, if using a commercial provider.
- Control of the CA is external.
- The certificate policy is subject to commercial considerations. ID certificate content format may not be compatible with Avaya components.
- The root CA certificate is untrusted by IP Office components and therefore needs to be distributed.
- The certificate creation and distribution process is manual.

Approach 4: PKI Trust Domain Based on an External Certificate Authority via SCEP

This option allows identity certificates to be obtained direct from an external Certificate Authority using an automated process.

Potential advantages for identity certificates obtained using SCEP:

- Generated ID certificates are part of a wider trust domain.
- ID certificate content format compatible with Avaya components.
- The root CA certificate is (typically) trusted by 3rd parties and therefore does not need to be distributed.
- The root CA certificate is always trusted by IP Office components and therefore does not need to be distributed.
- The certificate creation and distribution process is automated, supporting many systems efficiently.

Potential disadvantages include:

- Compatibility with SECP servers is currently limited to EJBCA – the CA present on SMGR.
- Public certificate authorities will not issue certificates for private domains or address ranges.
- Cost, if using a commercial provider.
- Control of the CA is external.
- The certificate policy is subject to commercial considerations.

Approach 5: No Trust Domain

This can only be considered when a single IP500 V2 or Primary Server has no external public interfaces and is completely within a secure closed environment. Installation is achieved by retaining the default identity certificate. No trust relationships are active and no certificates are checked.

PKI Maintenance will consist of renewing the identity certificate by deleting the existing using IP Office Manager or Web Manager; this will create a new certificate for the next 7 years. Any existing browser exceptions will need to be re-asserted.

Implementing IP Office PKI

Once the trust policy has been determined, the implementation process will depend on the option selected.

PKI Trust Domain based on Primary or Application Server root CA

- The Primary Server CA should be used for Server Edition deployments. The Application Server for non-Server Edition deployments. The same CA must be used for all systems in a deployment.
- For every device (server, IP 500V2 etc.) use the CA to create a unique ID certificate for each with the correct name content and save to a local directory.

  The name fields of the certificate are important for correct interoperation with clients; see Certificate Name Content on page 37 for more information. See Appendix G - Using the IP Office Certificate Authority on page 122.
- Save the root CA certificate in both PEM and DER formats to a local directory using the Web Manager setting **Platform | Settings | General | Certificates | CA Certificate | Download (PEM-Encoded)** and **Download (DER-Encoded)**
- Use Web Manager or IP Office Manager to save the CA certificate in each TCS.
- Use Web Manager or IP Office Manager to save the ID certificate on the relevant IP Office server. See Updating Certificates on page 79.
- If H.323 phones are using HTTPS for provisioning, the root CA certificate must be present on each phone.
- Distribute the root CA certificate to all clients and browsers. The mechanisms vary and some require PEM format, some require DER. See the relevant client and browser documentation.
- Verify that the correct ID certificate has been applied on each device using a browser or other diagnostic tool.
- Enable certificate checking in the IP Office security settings and IP Office lines.
- Verify using SE Manager that all IP Office systems are online.
- Enable secure connections for clients.
- Verify each client can connect successfully.
- Ensure all ID certificate files are stored securely.
- Once all checks have been carried out, a configuration backup should be taken.

PKI Trust Domain based on Primary or Application Server Intermediate CA

- The Primary Server CA should be used for Server Edition deployments. The Application Server for non-Server Edition deployments. The same CA must be used for all systems in a deployment.
- Select an appropriate Certificate Authority that can fulfil the trust and certificate requirement of the deployment. For more information on external public authorities, see Certificates from External Certificate Authorities on page 47.
- Request an Intermediate CA certificate/private key pair from a trusted Certificate Authority in PCKS#12 format. An intermediate CA certificate differs in content to a root CA or a device identity certificate.For more information on external public authorities, see Certificates from External Certificate Authorities on page 62.
- Download the root CA certificate (and any further intermediate CA certificates) from the Certificate Authority in PEM and DER format to a local directory.
- Install Intermediate CA certificate the on the Primary or Application Server. This can either be done during ignition, or post ignition via the Web Manager setting **Platform | Settings | General | Certificates | CA Certificate | Import**.
- For every device (server, IP 500V2 etc.) use the CA to create a unique ID certificate for each with the correct name content and save to a local directoryThe name fields of the certificate are important for correct interoperation with clients; see Certificate Name Content on page 50. See Appendix G - Using the IP Office Certificate Authority on page 122.
- Save the intermediate CA certificate in both PEM and DER formats to a local directory using the Web Manager setting **Platform | Settings | General | Certificates | CA Certificate | Download (PEM-Encoded)** and **Download (DER-Encoded).**
- Use Web Manager or IP Office Manager to:
  - Save both the root and intermediate CA certificate in the TCS, and then
  - Activate the certificate chaining feature **Offer ID Certificate Chain**.
- Use Web Manager or IP Office Manager to save the ID certificate on the relevant IP Office server. See Updating Certificates on page 79.
- Distribution of the root CA certificate to phones, clients and browsers is as per PKI Trust Domain based on Primary or Application Server root CA section above.
- Verification and enabling steps are as per PKI Trust Domain based on Primary or Application Server root CA section above, with the note that many external CAs provide online verification tools.
- Once all checks have been carried out, a configuration backup should be taken.

PKI Trust Domain based on an External Certificate Authority

- The CA on the Primary or Application Server is not used; disable the setting **Platform | Settings | General | Certificates | Identity Certificates | Renew automatically.**
- Select an appropriate Certificate Authority that can fulfil the trust and certificate requirement of the deployment. For more information on external public authorities, see Certificates from External Certificate Authorities on page 62.
- For every device (server, IP 500V2 etc.) request the CA to create a unique ID certificate for each with the correct name content and save to a local directory.

The name fields of the certificate are important for correct interoperation with clients. See Certificate Name Content on page 50 for more information. For more information on external public authorities, see Certificates from External Certificate Authorities on page 62.

- Download the root and any intermediate CA certificate from the Certificate Authority in PEM and DER format to a local directory.
- Use Web Manager or IP Office Manager to:
  - Save both the root and intermediate CA certificate in the TCS, then
  - Activate the certificate chaining feature **Offer ID Certificate Chain**
- Use Web Manager or IP Office Manager to save the ID certificate on the relevant IP Office server. See Updating Certificates on page 79.
- Distribution of the root CA certificate to phones, clients and browsers is as per PKI Trust Domain based on Primary or Application Server root CA section above.
- Verification and enabling steps are as per PKI Trust Domain based on Primary or Application Server root CA section above, with the note that many external CAs provide online verification tools.
- Once all checks have been carried out, a configuration backup should be taken.

PKI Trust Domain based on an External Certificate Authority via SCEP

- The CA on the Primary or Application Server is not used; disable the setting **Platform | Settings | General | Certificates | Identity Certificates | Renew automatically.**
- Select an appropriate Certificate Authority that can fulfil the trust and certificate requirement of the deployment, including a SCEP service based on EJBCA.
- The steps required to enable SCEP operation are covered in the IP Office Branch documentation.

Certificates from External Certificate Authorities

An external Certificate Authority (CA) provides a way of obtaining identity certificates that are trusted by third parties. These CA providers typically perform the following functions:

- Validates the certificate requestor's identity and ownership of the domain
- Issues certificates
- Maintains certificate status information
- Updates Certificate Revocation Lists

Most commercial CAs are part of one or more industry organisations such as:

- The Certificate Authority Security Council. https://casecurity.org/
- The CA/Browser Forum. https://cabforum.org/

Both have online resources that can assist in selecting and using a CA. In addition there are other web resources from the CA providers themselves.

Selecting a Certificate Authority

Note:

An external Certificate Authority cannot issue certificates with name content that cannot be externally verified. This includes any local domain names and private IP addresses. If local domain names or private IP addresses are required, the CA of the Primary or Application server should be used.

Select a Certificate Authority that can fulfil the trust and certificate requirement of the deployment. Selection criteria are outside of this document but should include for IP Office deployments:

- Is the Certificate Authority trusted?
- Can the Certificate Authority provide RSA 2048 bit + SHA-2 identity certificates for web servers? Code signing and other certificate type are not used by IP Office.
- Does the Certificate Authority support a web form based Certificate Signing Request (CSR)? If not, external tools are required to provide the CA with a text-based CSR. See Appendix H - Text-based Certificate Signing Requests on page 127 for more information about creating such text-based CSRs.
- Can the Certificate Authority provide identity certificates in PKCS#12 format? If not, external tools are required to convert the identity certificate to the correct format for import into IP Office. See Certificate File Naming and Format on page 41 for more information on certificate file formats. See Appendix H - Text-based Certificate Signing Requests on page 127 for more information about converting file formats.
- If required, can the Certificate Authority provide multi-domain (AKA ‘Multi-SAN’ or ‘Unified Communications’) certificates?
- If required, can the Certificate Authority provide a signing CA certificate? The option would be required for *Approach 2: PKI Trust domain based on Primary or Application Server Intermediate CA* above.
- Will the root CA already be in the client browsers and operating systems? Are all client browsers and operating systems covered?
- Are intermediate signing certificates used? This can increase deployment complexity if intermediates are used.
- Are the signing certificates provided in both PEM and DER format? See Certificate File Naming and Format on page 41 for more information on certificate file formats.
- What notification/assurance level is required? Providers typically offer a number of levels under various names:
  - Basic, AKA ‘Domain Validation’ – only the domain name is validated, not the company itself. Browsers should not raise an error/warning, but no company information is shown. This level is not recommended for IP Office interfaces where verification of company identity is important.
  - Intermediate, AKA ‘Organization Validation’ – the domain and company are validated. Browsers should not raise an error/warning, company information is shown.
  - Enhanced, AKA ‘Extended Validation’ – the domain and company are validated in detail. Browsers should display a green verified background and company information is displayed.
- How long are the identity and signing certificates valid for? Shorter periods increase the maintenance overhead.

- Can a free trial certificate be obtained to verify correct operation? IP Office has been tested successfully with a number of providers' identity certificates but due to quantity of providers, assurance cannot be given that all providers' certificates can be supported successfully.
- Are test and other support utilities provided?

Obtaining Identity Certificates

Once a provider has been selected, the certificate requirements need to be identified:

- The name fields of the certificate are vital for correct interoperation with clients. See Certificate Name Content on page 50 for more information.
- The certificate should be RSA2048 bit, with SHA-2 signature algorithm
- The quantity and duration
- The assurance level
- Whether single domain or multi-domain
- The certificate should be for a web server and not a signing certificate

Once requirements identified, a Certificate Signing Request (CSR) is made to the CA. This can use a number of methods:

- Form based, using the CA's web site or downloaded utilities: The private key and the certificate are created by the CA and sent/downloaded by the customer.
- Text based, using the OpenSSL package: The private key is created by OpenSSL and kept on the PC. The certificate is created by the CA and OpenSSL used to join the two parts together in a PKCS#12 file.
- Text based, using Microsoft windows tools: The private key is created by Microsoft OS tools and kept on the PC. The certificate is created by the CA and Microsoft OS tools used to join the two parts together in a PKCS#12 file.
- Automated via SECP: The private key is created by IP Office, kept on the system. The certificate is created by the CA and IP Office joins the two parts together.
- Web form based, using a third party site. This is not recommended.

Currently IP Office Linux and IP500 V2 servers do not support the generation of a CSR where the private key is retained within the IP Office server. This means if the CA does not support form-based CSR, the OpenSSL or Microsoft windows tools methods of Appendix H - Text-based Certificate Signing Requests on page 127 must be used.

Once a CSR is submitted to the CA, they will review the application and if successful issue the identity certificate along with the signing certificate(s). The required format of IP Office identity certificates is PKCS#12. The required formats for the signing certificates are PEM and DER. See Certificate File Naming and Format on page 41.

If the file formats are not as required by IP Office utilities can be used to convert; these can be provided by the CA or 3rd party tools can be used. Examples of conversion using 3rd party tools are contained in Appendix H - Text-based Certificate Signing Requests on page 127.

Certificate Maintenance

Regardless of the certificate/trust structure used, all certificates expire and may under exceptional circumstances be compromised. It addition due to identity certificate naming requirements, update may be necessary due to hostname or IP address change. The certificate policy should include provision for replacement/update of CA and individual certificates, both trusted and identity.

If left at default, IP Office's identity certificates will expire seven years after installation and the root CA certificate in ten. For certificates obtained from an external authority it can be a little as 12 months.

For identity certificates derived from a CA, replacement is relatively straight forward as the CA (and hence the basic trust relationship) is unchanged: Obtain the relevant replacement before expiry with the same content and replace. If the root or intermediate CA requires changing, the process can be more extensive depending on whether the associated public/private key pair also changes. The IP Office internal CA on the Primary will optionally retain the public/private key pair if the CA certificate is recreated via Web Management.

If the root CA public/private key pair is changed, all identity certificates need to be renewed and should be done well before CA expiry. The new CA should be installed in the relevant trust stores alongside the old; this allows a transition period during which all identity certificates can be replaced.

Administrative logins to Manager and Web Manager will display an identity certificate expiry warning, along with the number of days remaining. IP Office will not warn about pending expiry of certificates in the TCS.

Renewing an IP500 V2/Secondary/Expansion Server ID Certificate

If the default self-signed certificate or SCEP is being used, deleting the current will force another to be generated/obtained. When creating the new certificate, the Common Name and Subject Alternative Name files can be specified in the Manager security settings. If not specified, the default values are used. For Server Edition, all processes will restart. For IP500 V2, the transition will be smooth.

If the ID certificate has been obtained from an external CA, a replacement can be administered using IP Office Manager or Web Manager.

Renewing a Primary/Application Server Edition ID Certificate

If the ID certificate has been created by the internal CA, the Web Management setting **Platform | Settings | General | Certificates | Renew automatically** determines whether the creation and application is automatic due to expiry, host name change, or IP Address. If not automatic, **Generate** and **Apply** can be used.

If the ID certificate has been obtained from an external CA, a replacement can be administered using IP Office Manager or Web Manager.

Renewing a Primary/Application Server CA Certificate

A new certificate can be created using Web Management **Platform | Settings | General | CA Certificate | Create new**. This will create a completely new root CA certificate and will also require new ID certificates for all entities. To keep all existing ID certificates, select **Renew existing**. This will create a new certificate with the same content and public/private keys, but a different serial number and start/end date. Only this new root CA requires distribution, in-date existing ID certificates signed by the previous CA will still be valid. Care must be taken not to abuse the

convenience of this feature as the longer the public/private keys are unchanged, the greater the risk of compromise.

See Appendix G - Using the IP Office Certificate Authority on page 122.

Recovering an ID, CA or TCS Certificate

All certificates are part of the security settings backup and restore process. To recover an ID certificate, the latest backup set must be restored. For Server Edition, all processes will restart.

Troubleshooting

The certificates exchanged by any IP Office interface can be displayed using 3rd party tools like Wireshark. The IP Office identity certificate can also be displayed in Manager, Web Manager, and browsers.

Failure of received certificate checks by IP Office result in an alarm event which contains the cause. These alarms also include certificate check failures as reported by the far end via TLS Alert messages. IP Office Manager and browsers also report certificate checks failures.

If an HTTP/TLS interface appears to have certificate issues it may be possible to temporarily disable certificate checking or enable an unsecure version of that interface.

The IP Office Manager security settings interface to IP Office should always be accessible; IP Office will always ensure it has an identity certificate (creating a self-signed one if the previous is deleted or corrupted), and Manager can be configured to accept any certificate. See Securing Manager on page 87.

It has been found on rare occasions that low-end routers when performing Network Address Translation (NAT) will modify IP addresses within the certificate name fields, rendering them corrupt. Changing the firewall/router is the best solution, but a temporary work around may be to remove any IP address entries subject to NAT.

Chapter 7: VoIP Security

VoIP (Voice Over IP) media security provides a means by which two endpoints capable of communication can engage in more secure media exchanges. There are a number of approaches that can be used.

- Secure Real-time Transport Protocol (SRTP).
- Datagram Transport Layer Security (DTLS).
- A Virtual Private Network (VPN) implemented using IPsec or another VPN technology such as SSL VPN.
- Other IP transports with security support such as Multiprotocol Label Switching (MPLS).

VPN and other IP transport security is briefly discussed in Limiting IP Network Exposure on page 94. However, the relative merits for each media security approach is outside the scope of this document.

SRTP supports RTP media protection on a point to point basis providing confidentiality, message authentication and replay protection. SRTP also supports authentication and replay protection for the RTP Control Protocol (RTCP). Note that RTCP is not used as the signalling channel for VoIP calls, but contains Quality of Service (QoS) information.

The confidentiality (implemented by symmetric key encryption) and authentication (implemented by Hashed Message Authentication Code, HMAC) are optional and independent of each other.

SRTP encryption relies upon dynamically generated secure keys to be sent to the far endpoint. This cannot be achieved via the SRTP protocol so an alternative secure mechanism is required, typically via the associated signalling channel, for example SIP-TLS for SIP and ‘Annex H’ for H.323.

As SRTP is point to point, all individual links involved in the VoIP call, including key exchange/ signalling, must be secure for the call to be secure from end to end.

IP Office Platform Media Security

IP Office support both SRTP and IPsec for VoIP media security. IP Office’s IPsec feature can be utilized, but it is not recommended as it limited to the IP500 V2 platform and uses a legacy key exchange mechanism (IKEv1).

VoIP media security using SRTP is supported on IP Office in Standard Edition, Server Edition, Select and hosted, without the need for extra licensing, for the connections:

- IP Office Line
- SIP Line

- SM Line
- Avaya H.323 extensions: 96x1 (9608, 9611, 9621, 9641)
- Avaya SIP extensions: 96x1 (Centralized in branch deployments), 11xx, 12xx, B179, E129, Radvision XT series
- Avaya Communicator for iPad and Windows
- one-X Mobile Preferred for iOS and Android
- 3rd Party SIP extensions that support SRTP

Some IP Office connections do not support SRTP media security:

- Analogue and digital extensions
- Analogue and digital lines/trunks
- Voicemail Pro link
- H.323 trunks
- Avaya H.323 extensions: 96x0, 16xx, 36xx, 46xx, 56xx, 36xx
- Avaya SIP extensions: D100, E159, E169
- Avaya IP DECT and DECT R4
- Avaya IP Office Softphone (Mac)
- 3rd Party SIP extensions that do not support SRTP

The following configurable SRTP options are supported by IP Office.

SRTP feature	Options	Support	Default	Notes
SRTP Operation	Disabled	Yes	Yes	All SRTP settings are per system with a per line and per extension override.
	On: Best Effort	Yes		
	On: Enforce	Yes		
RTP Encryption	Off	Yes		
	On: AES128-CTR	Yes	Yes	
	On: AES128-F8	No		
RTP Authentication	Off	Yes		RTP Authentication should not be disabled.
	On: SHA-1/32	Yes		
	On: SHA-1/80	Yes	Yes	SHA-1/80 provides stronger authentication for a small bandwidth increase.
RTCP Encryption	Off	Yes	Yes	
	On: AES128-CTR	Yes		Some Avaya and 3rd party endpoints do not support encrypted RTCP.
	On: AES128-F8	No		
RTCP Authentication	On: SHA-1/32	Yes		RTCP Authentication always active.
	On: SHA-1/80	Yes	Yes	SHA-1/80 provides stronger authentication for a small bandwidth increase.

IP Office supports a per-system SRTP set of controls, with a per-line and extension override, including encryption and authentication settings. By default, SRTP operation is disabled. However, upgrades of IP Office branch systems from previous releases using the SM line and SRTP will maintain their settings.

The SRTP operation control is the setting **Media Security** and has the following values:

- **Disabled**: SRTP is not available
- **Enforce**: RTP is not available on that call leg. **Note:**This doesn't enforce end to end SRTP, only SRTP on the call leg configured as Enforce
- **Best Effort**: always offer both SRTP and RTP and given choice, choose SRTP.

Where SIP soft clients connect to IP Office in simultaneous-registration mode (i.e. another device is registered for the same user), they not have a per-extension override of media security settings. IP Office will handle calls of these devices according to its system-level Media Security settings

In order to provide complete call security, the SRTP key exchange also requires to be secured. See VoIP Signalling Security on page 69.

VoIP Signalling Security

Securing the signalling of VoIP links is necessary when SRTP is enabled and can also be a security measure in itself. The security mechanism is dependent upon the type of link

Link Type	Key Security Mechanizm	Notes
IP Office Line	WebSocket HTTPS	Only the IP Office Line with WebSocket transport and Security setting of **Medium** or **High** should be used.
SIP Line	SIP-TLS	Additional line configuration is required to enable SIP-TLS. Also supports the SIPS URI scheme
SM Line	SIP-TLS	Additional line configuration is required to enable SIP-TLS Also supports the SIPS URI scheme
Avaya H.323 extensions	H.323	No additional configuration required This does not secure the complete H.323 signalling channel, just the registration key exchange and dialed digits.
Avaya SIP extensions	SIP-TLS	Additional SIP registrar configuration is required to enable SIP-TLS

For SIP extensions, the relevant LAN's SIP registrar layer 4 protocol setting should be configured to enable the TLS protocol. SIP-TLS requires the administration of certificates; see Certificates and Trust on page 36.

For SIP or SM lines, the line's transport setting should be configured to use the TLS protocol and certificate checks enabled. A further consideration is the use of the SIPS URI scheme as defined by RFC 3261 and RFC 5630. Enabling the SIPS URI Type setting will cause all sessions originated from the trunk to use SIPS, indicating the requirement for secure SIP links for the call. The system setting **System | VoIP Security | Strict SIPS** when active, causes IP Office to reject an call to a SIP

or SM Line that is not configured for SIP-TLS and the SIPS URI Scheme. When not set, IP Office permits the downgrading of a SIP-TLS call to an unsecure SIP call. Care should be taken when using SIPS URI scheme and Strict SIPS, as support by both Avaya clients and ITSPs is varied which could result in failed calls. This is of high importance for emergency call planning.

Current SIPS support of Avaya clients is covered in Appendix F IP Office VoIP Endpoint Security on page 119. For further detail, see the relevant client documentation.

Endpoint Provisioning Security

When either media or signalling security is used, settings are required on the endpoints themselves. Some remote endpoint provisioning is supported directly by IP Office and can be more securely conveyed via HTTPS rather than the default HTTP.

Endpoint support of secure remote provisioning is covered in Appendix F IP Office VoIP Endpoint Security on page 119.

Where remote endpoint provisioning is not supported by an endpoint, settings local to the device are used.

For further details, see the relevant client documentation.

SRTP Performance and Capacity

SRTP is more processing intensive than RTP to the extent that the concurrent call capacity of an IP500 V2 is reduced by 66% and Linux servers by 50%. See the “Capacity Planning” section in *Deploying IP Office™ Platform Server Edition Solution*. These reductions only occur when the media stream terminates or originates on IP Office. For this reason it is important to use direct media wherever possible.

SRTP direct media will occur when both external endpoints SRTP capabilities match, if they do not, IP Office will terminate both streams and convert. This will reduce the concurrent SRTP call capacity by two. This in turn places great importance on the various SRTP configuration settings within both IP Office and the various endpoints.

The following IP Office recommendations should be followed as a starting point, and only varied if necessary.

- RTP encryption and authentication should be kept on; some endpoints will not negotiate at all if either is off.
- RTP encryption/authentications setting should be AES-128/CTR plus SHA-1/80.
- RTCP encryption should be kept off; some systems (including Avaya Communication Manager) do not support RTCP encryption.
- All SIP extensions where possible should be configured for best effort (capability negotiation or ‘cap-neg’); this allows the IP Office settings to dictate SRTP behaviour.**Note:**When Auto generated configuration files that IP Office provides to 11xx/12xx and B179 device types

always indicates to the phones to do best effort, when the IP Office SRTP configuration is Best Effort or Enforce.

- Ensure consistency between the system and per-extension SRTP settings for SIP soft clients that connect to IP Office in simultaneous-registration mode (Avaya Communicator and one-X Mobile).
- All direct media settings on.
- Default codec selections which should ensure the mandatory G711 codec is always available.

Another performance consideration is the extra bandwidth incurred when SRTP is active; authentication adds 4 or 10 bytes to each packet for both RTP and RTCP. Given a 20ms sample period, active SRTP uses the following approximate IP bandwidth for a single call.

Codec	No SRTP	+RTCP auth	+RTP/RTCP auth	Notes
G.711	84 kbps	SHA1/80: 85 kbps	SHA1/80: 86 kbps	2.4% increase
		SHA1/32: 84.5 kbps	SHA1/32: 85 kbps	1.2% increase
G.729	25 kbps	SHA1/80: 26 kbps	SHA1/80: 27 kbps	8% increase
		SHA1/32: 25.5 kbps	SHA1/32: 26 kbps	4% increase
G.722	84 kbps	SHA1/80: 85 kbps	SHA1/80: 86 kbps	2.4% increase
		SHA1/32: 84.5 kbps	SHA1/32: 85 kbps	1.2% increase

Secure Call Indications

There are no direct indications on phone displays that signal the call is secure. If assurance is required, Media Security should be set to Enforce and Strict SIPS activated.

The call leg SRTP status can be displayed by System Status Application and SysMonitor, see Appendix D – SRTP Troubleshooting.

VoIP Security Planning Considerations

Prior to deploying secure media or signalling using IP Office, the following must be considered.

- The IP Office SRTP feature supports media security natively without license or IP infrastructure requirements, but can add extra interoperation complexity with various endpoints.
- Signalling security must be considered whenever SRTP is contemplated. Signalling security can be considered on its own as a security improvement mechanism.
- Secure phone provisioning must be considered whenever SRTP is contemplated.
- SRTP will reduce the concurrent call capacity of IP Office systems, therefore direct media should be used whenever possible. It may also reduce the capacity and performance of other connected systems.
- The exact SRTP support of each endpoint type should be assessed to determine how best to achieve security, direct media and other performance criteria.
- IP Office default SRTP settings should be retained wherever possible and only varied under exceptional circumstance.

- IP Office branch deployments have a specialized environment and requirements. See the documents
  - *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*
  - *Administering Centralized Users for an IP Office™ Platform Enterprise Branch*
  - *Avaya IP Office™ Platform in a Branch Environment Reference Configuration*

Chapter 8: Securing the IP Office Platform Solution

Introduction

IP Office can be made a very secure product, however only a certain number of features are active by default or on upgrade from previous releases. This is in order to ease the initial installation but will not fully protect the system without following the suggestions listed in this document, other Avaya security publications and the relevant IP Office installation/Administration manuals. It is therefore necessary to check and implement the configuration options listed here.

Additional setting may be necessary to further secure the individual deployment. Avaya is presenting this information for guidance only; the customer is responsible for ensuring their system is secure.

General Guidelines

The recommended process for improving the security of IP Office is to *Assess* the requirements, *Implement* changes as needed, then to *Monitor* the system and *Respond* in a timely manner to any detected threats.

All guidelines and steps should be followed regardless of the actual IP Office deployment.

Assess:

- Review existing installations
- Plan new deployments
- Identify security risks and requirements

Implement:

- Change security defaults
- Remove unnecessary accounts
- Disable unused services/interfaces
- Enforce password policy
- Secure users and extensions
- Secure trunks/lines
- Prevent unwanted Calls

- Secure voicemail and one-X Portal
- Limit IP network exposure
- Secure management applications & configuration data
- Secure servers
- Activate reporting/monitoring
- Checks and tests

Monitor:

- Monitor alarms and logs
- Detect other unusual activity
- Review Avaya Security advisories
- Review Avaya IP Office Software updates and technical bulletins
- Monitor telephony provider communication
- Periodic security reassessment

Respond:

- Investigate and react to any incident
- Report to appropriate organizations
- Ensure the latest software updates/service packs are installed

Assessing IP Office Platform Security Requirements

It is vital that a security risk assessment is carried out on all IP Office installations, both initial (prior to deployment or for existing deployments if one has not yet been carried out), and periodically after initial assessment to review any change.

A primary differentiation of security risk for IP Office is whether the system is potentially accessible from external or unsecured networks or individuals, especially the Internet.

This document does not cover security assessments in any detail. However there are many resources available that cover this process. Examples are listed below.

- US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology System*.

  http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

- UK British Standards Institute (BSI) ISO/IEC 27001, *Self-assessment questionnaire*.

  http://www.bsigroup.co.uk/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISOIEC27001-Assessment-Checklist-UK-EN.pdf

  http://www.bsigroup.co.uk/en-GB/iso-27001-information-security/ISO-27001-for-SMEs/

- The SANS Institute also provides a wide range of security-related information, including risk assessments and audits.

http://www.sans.org/reading-room

Security Administration

The security settings are stored on the system and are separate from the system's configuration settings. To change a system's security settings, Manager must first be switched to security mode by selecting **File | Advanced | Security Settings** from the menu bar.

Security settings can only be loaded directly from a system. These settings cannot be saved as a file on the local PC, nor do they appear as a temporary file at any time. By default Manager and the system will always attempt to use a secured link for configuration and security settings exchanges.

Change Security Default Settings

All default passwords must be changed to a unique and ‘strong’ password. See Password Management on page 31 for more information on password strength.

In the Manager **Security Settings | General** tab, change the following settings.

- For the Security Administrator account, change **Password** to a strong password of 8 or more characters. Set **Minimum Password Complexity** to **High**
- Change service user account **Administrator** password to a strong password of 8 or more characters.
- If required, add a customer administration account (again with strong password) with the minimum rights of access. The account status **Force New Password** should be set. This will enforce a password change at the next login (for example, during customer or engineering installation).
- Change the System, Voicemail Pro and Monitor passwords to a strong password of 8 or more characters.

Removing Unnecessary User Accounts

All unnecessary administration and IP Office user accounts should be removed or disabled to reduce the likelihood of forgotten default accounts being used for unauthorized access. Any remaining accounts must have their passwords changed. See User Accounts and Rights of Access on page 24 for more information on the differing account types and locations.

Perform these steps to manage user accounts.

Procedure

1. Open the Manager security settings.
   a. Select **Security Settings | Service User**.
   b. Remove all unnecessary service user accounts. Delete the unnecessary service account or set the account status to **Disabled**.
2. For all remaining active Service User accounts, change the password to a strong one of 8 or more characters.

   Note:

   If using Server Edition, see Securing Server Edition Servers on page 95 for alternative Service User administration using Web Manager.
3. Open the Manager configuration settings.
   a. Select **Users**.
   b. Delete any RAS telephony user accounts (for example RemoteManager) that are not required.

Disabling Unused Interfaces and Services

Disable all interfaces and services that are not required. Additionally, consider enabling interfaces and services only when required.

Procedure

1. Log in to the Manager security settings and select **System | Unsecured Interfaces**.
2. Uncheck all Application controls and enable only the minimum according to the following table.

Application Control	Affected Application	Notes
TFTP Server	IP Office Manager Upgrade Phone Manager DECT R4* Legacy Voicemail Pro UDP whois** Network Viewer	Disables all TFTP access, including TFTP Directory Read, TFTP Voicemail and Program Code. * When inactive, DECT will continue operating but without the system directory feature. ** TCP whois discovery should be used in Manager.
TFTP Directory Read	Phone Manager DECT R4*	Also used for legacy applications: IP DECT*, Analog DECT, Conferencing Centre, CRM, MMM.

Table continues…

Application Control	Affected Application	Notes
	TAPI Install**	* When inactive, DECT will continue operating but without the system directory feature. ** TAPI installation will generate a warning, but it can be ignored Also controlled by the general TFTP Server setting above.
TFTP Voicemail	Legacy Voicemail Pro	Enable only when Voicemail Pro R9.0 and earlier is used Not applicable to embedded voicemail. Also controlled by the general TFTP Server setting above.
Program Code	IP Office Manager Upgrade	Used for upgrades from IP Office Manager. Must be disabled when not required. Also controlled by the general TFTP Server setting above.
DevLink	DevLink System Monitor*	Must be disabled when not required. * When inactive, SysMonitor can still use the HTTP / HTTPS access method.
TAPI	TAPI Link Lite (1st party TAPI) TAPI Link Pro (3rd party TAPI)	Enable only when TAPI required. Note that TAPI driver installation will fail if the TAPI interface is not active. This setting will not affect other CTI links such as one-X Portal, IPOCC or ACCS.
HTTP Directory Read	one-X Portal* IP Office Centralised Directory	Enable only when one-X Portal or IP Office Centralized Directory used. * When inactive, one-X Portal will continue operating but without the personal directory feature.
HTTP Directory Write	one-X Portal*	Enable only when one-X Portal deployed. * When inactive, one-X Portal will continue operating but without the personal directory update feature.

3. Select **Security Settings | Services**.
4. Enable only the minimum services at the recommended **Service Security Level** according to the following table.

Service Name	Application	Service Security Level	Notes
Configuration	Manager, Configuration Web Service (DevConnect)	Secure, Medium	Should always be enabled.
Security Administration	Manager	Secure, Medium	Should always be enabled.
System Status Interface	SSA	Secure, Medium	Disable if SSA not present.

Table continues…

Service Name	Application	Service Security Level	Notes
Enhanced TSPI	one-X Portal	Unsecure Only	Disable if one-X Portal not present.
HTTP	H323 Phones (HTTP or HTTPS) Embedded File Manager (HTTP), IP Office Softphone (HTTP or HTTPS) SysMonitor (HTTP or HTTPS) VMPro (HTTPS) IP Office Line (HTTP or HTTPS)		Controls the IP Office HTTP server. Disable if not required, else if just HTTPS required, set to **Secure, Medium**. If HTTP must be enabled, set the **System | System | Avaya HTTP Client Only** setting active. This will reject all non-Avaya clients.
Web Services	Web Manager	Secure, Medium	Disable if Web Management or System Manager (SMGR) not used.
External	Voicemail Pro, one-X Portal,Web Control,WebRTC	n/a	Not a true service interface.

5. Open the configuration settings and select **System | System**.

   Check the **File Writer IP Address** setting. This specifies the IP address allowed to write files to the IP Office (IP500 V2 and Linux) using HTTP and TFTP protocols. It should be set to 0.0.0.0 (disabled) and set only when files need to be transferred.

Enforcing a Password Policy

Change the security settings to enforce minimum password complexity

On bad logins, disable service users temporarily and IP Office users permanently. If a Service user fails to login 3 times within 10 minutes, the account will be locked for 60 seconds. If an IP Office user fails to login 5 times within 10 minutes, account will be locked permanently and the administrator will be required to unlock the account using Manager.

Note:

This recommended IP Office User password policy must always be enforced if the system is potentially accessible from unsecured networks, including the Internet. For example, when SIP trunks or VoIP remote worker extensions are supported.

Procedure

1. Log in to the Manager security settings and select the **General** tab.
2. Set the Service User details.
   a. **Minimum Name Length** to 6
   b. **Minimum Password Length** to 8
   c. **Password Reject Action** to **Log and Temporary Disable**
   d. **Minimum Password Complexity** to **Medium**
   e. **Previous Password Limit (Entries)** to 4
3. Set the IP Office User details.
   a. **Password Enforcement** to **On**.
   b. **Minimum Password Length** to 8
   c. **Minimum Password Complexity** to **Medium**
   d. **Password Reject Limit** to 5
   e. **Password Reject Action** to **Log and Disable Account**

   Note:

   The IP Office user password policy only applies to the password field, not the voicemail or user login code. See Password Management on page 31 for more information.

Updating Certificates

It is essential to understand the information and recommendations in Certificates and Trust on page 36 to determine the certificate and trust requirements of the system prior to installation.

- If required, create a new platform identity certificate using Manager **Security | System | Certificates | Identity Certificate**. This identity certificate is automatically propagated to all TLS/HTTPS interfaces of the server.

  If an intermediate CA is used to create the identity certificate, place the root CA in the Trusted Certificate Store and then activate the setting **Security | System | Certificates | Offer ID Certificate Chain**. This root CA must also be added to the `system/primary/certificates/tcs/add` directory.
- If a separate telephony identity certificate is required, it can be administered using the Manager security settings.

- The two default certificates trusted by IP Office must be removed if not required. To achieve this, place a copy of the certificate in the `system/primary/certificates/tcs/delete` directory using the Manager or Web Manager File Manager tool.

  Any default certificates to be trusted by IP Office must be added to the `system/primary/certificates/tcs/add` directory. See Appendix B Default Trusted Certificates on page 107 for more information and how to create the certificate files.
- After ensuring that all other IP Office components' identity certificates are correctly configured, set the received certificate check levels appropriately using the Manager settings **Security | System | Certificates | Received Certificate Checks (Management)** and **Security | System | Certificates | Received Certificate Checks (Telephony)**.

Securing Telephony Users and Extensions

Users and extensions should be configured to restrict access to only necessary features, default login codes changed, and auto-create disabled.

Procedure

1. Open the Manager configuration settings.
2. Select **Users**.

   Delete all unused users.

   Note:

   Do not delete the NoUser account.
3. Disable the following auto-create settings. (In release 9.1, the auto-create settings are disabled by default.) If you use the auto-create settings to assist installation, disable the settings once installation is complete.
   - **LAN1 | VoIP | H323 Gatekeeper | Auto-create Extn**
   - **LAN1 | VoIP | H323 Gatekeeper | Auto-create User**
   - **LAN1 | VoIP | SIP Registrar | Auto-create Extn/User**
   - **LAN2 | VoIP | H323 Gatekeeper | Auto-create Extn**
   - **LAN2 | VoIP | H323 Gatekeeper | Auto-create User**
   - **LAN2 | VoIP | SIP Registrar | Auto-create Extn/User**
   - **Line | IP DECT | Gateway | Auto-Create Extension**
   - **Line | IP DECT | Gateway | Auto-Create User**

   If any auto-create feature is used to assist installation, the settings must be deactivated as soon as possible. Note that in release 9.1 and later, these settings will automatically be deactivated 24 hours after being set to avoid inadvertent exposure.

4. If no H.323 extensions are supported, disable the **LAN1/LAN2 | VoIP | H323 Gatekeeper Enable** setting. If H.323 extensions are supported, enable only the relevant LAN's gatekeeper.
5. If no H.323 remote workers are supported, disable the **LAN1/LAN2 | VoIP | H323 Gatekeeper | H323 Remote Extn Enable** setting. If H.323 remote workers are supported, enable only the relevant LAN's **Remote Extn**.
6. If no SIP extensions are supported, disable the **LAN1/LAN2 | VoIP | SIP Registrar Enable** setting. If SIP extensions are supported, enable only the relevant LAN's registrar.
7. If no SIP remote workers are supported, disable the **LAN1/LAN2 | VoIP | SIP Registrar | SIP Remote Extn Enable** setting. If SIP remote workers are supported, enable only the relevant LAN's SIP **Remote Extn**.
8. For all VoIP (SIP, H323, DECT) users, the **User |Telephony | Supervisor Settings | Login Code** must be set.

   The Login Code must not be a sequence, repeated digits, or same as the extension number. If it is a remote extension, this must not be less than 9 digits.
9. All auto-created VoIP users must have their **User |Telephony | Supervisor Settings | Login Code** changed from the default. If it is a remote extension, this must not be less than 9 digits.
10. Change the default name for all auto-created non-VoIP (Digital, Analog) users.
11. For all user, enable only the necessary **User | User | Profile** features.
12. Only enable the minimum necessary **User | Web Self-Administration** interface features.

    Web Self-Administration is a new feature for release 9.1 and disabled by default. The ability to control viewing of each tab of the Web Self-Administration page can be controlled on a per-user basis.

Self Admin Tab	User Setting
Profile	User
Voicemail	Voicemail
Do Not Disturb	DND
Mobility	Mobility
Forwarding	Forwarding
Personal Directory	Personal Directory
Button Programming	Button Programming
Download	none (always available)

13. For IP Office release 8.1 and earlier, disable all **User | Phone Manager Options** unless required. This can be achieved via the application of User Rights (**User Rights | Phone Manager**)
14. If different from the system-wide setting, change the **Extn | VoIP | Media Security** setting. See VoIP Media Security on page 67.

15. If the VoIP extension is configured for secure media (SRTP) or operates in an unsecure environment, any settings file supplied by IP Office should be conveyed via HTTPS not HTTP. This will additionally require certificate administration. See Certificates and Trust on page 36.

Hardening for Remote Worker Operation

Whenever SIP or H323 remote worker operation is supported, extra considerations are required to ensure that the external access does not compromise IP Office security.

Important:

IP Office must only be connected externally via a properly configured Firewall. It must never be connected directly.

- The maximum value for the following port range settings must be set to no more than 50750.
  - **LAN1/LAN2 | VoIP | Port Number Range | Maximum**
  - **LAN1/LAN2 | VoIP | Port Number Range (NAT) | Maximum**

    Note:

    If more RTP ports are required, the minimum value may be changed.
- For all remote workers, the **User |Telephony | Supervisor Settings | Login Code** must be set.

  The Login Code must not be a sequence, repeated digits, or same as the extension number. It must not be less than 9 digits.

  The setting **Extension | Extn | Phone Password** can be used to separate out the phone registration.
- For each H323 remote worker extension, set the **Extension | VoIP | IP Address** to the public IP Address of the phone.

  Note:

  Not possible if more than one phone is behind the same firewall/NAT.
- Since the IP Office remote worker feature support does not include native signalling or media encryption, a Virtual Private Network (VPN) solution between the remote endpoints and a secure gateway must be considered. For information on VPN operation and options see “Remote Phone Support” in *Avaya IP Office™ Platform Solution Description*.
- A Session Border Controller (SBC) should be considered for enhanced SIP remote worker security. The Avaya SBC for Enterprise is a solution specifically tailored for IP Office SIP remote workers and SIP trunks. For more information see “Configuring the Avaya Session Boarder Controller for IP Office Remote Workers” in *Administering Avaya IP Office™ Platform with Manager*.

Securing Trunks

SIP trunking and off-switch or trunks-to-trunk forwards/transfers should be disabled when not required, and a Session Border Controller (SBC) used for enhanced SIP security. Links between IP Office systems can be optionally secured.

- If using SIP trunks, IP Office must only be connected externally via a properly configured firewall. See Limiting IP Network Exposure on page 94. IP Office must never be connected directly.
- If SIP trunks are not configured for a particular LAN interface, disable the **LAN1/LAN2 | VoIP | SIP Trunk Enable** setting
- Many IP Office customers rely on the Services Providers to provide a secure SIP trunk environment. For a stronger security posture, implementation of the Avaya Session Border Controller for Enterprise (Avaya SBCE) is recommended as a best practice. Avaya SBCE also provides Advanced Services such as Secure Remote Worker and Encryption Service supporting VPN-less access to IP Office for SIP endpoints outside the enterprise firewall.

  The Avaya SBC for Enterprise is a solution specifically tailored for IP Office. For more information see *Deploying Avaya IP Office™ Platform SSL VPN Services*.
- Off-switch forwards/transfers should be disabled on a system or user basis, with the system setting taking precedence over the user.
  - The user setting is **User | Telephony | Supervisor Settings | Inhibit Off-Switch Forward/ Transfer**.

    This can also be set using the **User Rights** settings.
  - The system wide setting is **System | Telephony | Telephony | Inhibit Off-Switch Forward/ Transfer**.
- Analog trunks-to-trunk forwards/transfers should be disabled on a per-line basis unless required. Use the setting **Line | Analog Options| Analog Trunk to Trunk Connection**.
- Other changes to restrict calls are contained in Preventing Unwanted Calls on page 84.
- IP Office Lines (previously know as SCN trunks) may be secured using the **Line | Line | Transport Type** of WebSocket Client/Server, and a **Line | Line | Security** setting of **Medium** or **High**. One IP Office system must be the WebSocket Client, the other the server. For Server Edition deployments, the Primary and Secondary should always be the WebSocket Server. For the **High** setting, certificate configuration is required. See Certificates and Trust on page 36 for more information.

Securing Voice Media

In an unsecure environment with no other VoIP security, IP Office's VoIP media security should be enabled.

Enabling VoIP media security will reduce the platform concurrent call capacity considerably. It will also require SIP call signalling security. For more information, see VoIP Media Security on page 67. This should be reviewed prior to enabling any IP Office VoIP media security.

Preventing Unwanted Calls

The following recommendations cannot be precise due to the wide variation of national, international and customer dial plans, however they can be adapted as required for specific deployments. Toll fraud, dial-through attacks or general unwanted incoming or outgoing calls can be mitigated in IP Office by:

- Call barring
- Authorization Codes
- Call logging
- Phone Lock
- Auto Logout
- Out of hours barring
- Blocking off-switch and trunk-to-trunk transfers
- Removing mobile call control
- Ensuring Emergency Numbers are defined

Call Barring

The normal way of call barring is to have a default outgoing route and then lock down undesired numbers. When locking down un-desired numbers it is important to take in to account IP Office dialling rules and add an N after any dial string you are trying to block.

For example to block calls to Premium rate numbers (1900-xxx-xxxxx US or 09… UK):

	US	UK
Telephone Number	1900N	09N or 909N

It is important to ensure that the Telephone Number is followed by an N so that it matches even when dialled en-bloc (or redial).

Many countries have prefixes that may be dialled before normal PSTN numbers, for example to force CallerID presentation, (*67(US)/141(UK) to Withhold CallerID, *82(US)/1470(UK) to present CallerID) it is important to include versions of all barred short codes including these prefixes or just bar any call attempts using these prefixes.

User Based Barring

There are several potential methods for achieving different routing/barring rules for Users. One effective method that

- minimises the per-user configuration
- can be part of user rights templates

- centralises the routing/barring configuration
- maintains features like secondary dial tone

is to create copies of the 50:Main ARS for the different access levels required.

As 50:Main is the default it makes sense for that to be the one that is used for most users, or on sites with specific concerns about security the most restricted.

For this example we will define two alternate ARS entries for Local & Long Distance, and Unrestricted, by copying the default Main then restrict Main to be local only. All the ARS tables must route Emergency Calls.

The new Short Codes in the Main ARS will be:

Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
0N;	0N	Barred	0
1N;	1N	Barred	0
XN;	N	Dial 3K1	0
XXXXXXXXXN	N	Dial 3K1	0
*67N		Barred	0
*82N		Barred	0

The 0N; and 1N; codes have been changed to barred and barred codes added for *67 and *82. Note the addition of the N to ensure a match for redial, etc. Short codes can be added for areas where 7 digit local dialling is still available if required, also it might be useful to create Short Codes to trap local Area Codes that have been dialled with a leading 1, also Freephone dialling.

The Local & Long Distance Short codes will be:

Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
0N;	0N	Barred	0
1XXXN;	1N	Dial 3K1	0
XN;	N	Dial 3K1	0
XXXXXXXXXN	N	Dial 3K1	0
1900N		Barred	0
*67N		Barred	0
*82N		Barred	0

This will allow all calls starting ‘1’ except Premium Rate (1-900 numbers), the 1N; Short Code is modified to 1XXXN; to avoid people pausing during dialling matching a simple “1N;” short code. The barring for *67 and *82 is repeated.

The Unrestricted ARS short codes will be:

Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
N;	N	Dial 3K1	0

This is totally unrestricted. In an operational system, it is unlikely for there to be totally unrestricted out-dialling. The default system short code for dialling is unchanged.

Add specific User Short Codes for users who are allowed greater dialling privileges, similar to the default system Short code but pointing to the appropriate ARS entry. This can be done via User Rights Templates.

For more information on ARS operation, see the field descriptions for the Manager ARS tab in *Administering Avaya IP Office™ Platform with Manager*.

Protecting Phones

In some environments, one of the risks is not from the normal phone users but from people who have physical access to the phone. There are several mechanisms that can protect the phones when the normal users are away from their desks.

- **Phone Lock**

  Phones can be locked using the Lock feature on the phone Features menu. Locking the phone also locks the Features menu. The 1400, 9500, and 9600 series phones have an option to specify a timer where the phone will automatically lock itself after a specified period of inactivity.

- **Short Codes**

  The “Outgoing Call Bar On” short code prevents the phone being used to make outgoing calls. Internal and Emergency calls are allowed. “Outgoing Call Bar Off” with the users’ Login code unlocks the phone.

- **Logging out/Hot Desking**

  Users can log out of the phone, which leaves the phone with the special ‘NoUser’ account associated with it. This NoUser is Outgoing Call Barred. Users must have a login code to be able to log out of their default phone (the phone with their extension number).

- **Auto Logout**

  The **Extension | Telephony | Supervisor Settings | Login Idle Period** can be used to log out a phone if it is idle for a period of time.

- **Out of Hours Call Routing**

  A time profile can be associated with an ARS so that when the time Profile is inactive, a different ARS is used for routing calls. For example, set the extra ARS tables to point to Main out of hours so that only Local and Emergency Calls can be made.

- **Trusted Voicemail Source**

  When a phone is in an un-controlled area, it is advisable to remove the default Trusted Source Number for Voicemail access, so that all IP Office Voicemail access requires entering the Voicemail access code, even from the user’s home extension.

Making Calls from Protected Phones

Once phones have outbound dialling locked down, it often becomes necessary to provide occasional exceptions. It is possible for a privileged user (Receptionist for example) to transfer secondary dial tone to a restricted user to allow them to make a call that they would not otherwise be able to make.

A more versatile solution is to use Authorization Codes. Authorization Codes permit a user with a Code to go to a restricted phone and make a call with their privileges without the necessity of Hot Desking for the call. This is sometimes called “Roaming Class of Service” on other systems. For information see the field descriptions for the Manager Authorization Codes tab in *Administering Avaya IP Office™ Platform with Manager*

Note that Emergency Calls are always permitted, hence the need to ensure Emergency Dialling has been correctly defined.

Forwarding Protection

When a user has forwarding active, any call routing, including barring for calls to that user, will be applied. If a user cannot make long distance call, and attempts to forward to a long distance number, the call will fail. As call routing/barring can vary by time of day it is not possible to block the attempt to configure long distance as the forwarding target.

Use the setting **System | Telephony | Telephony | Inhibit Off-Switch Forward/Transfer** to inhibit all off-switch forwarding and transfers. When enabled, this takes precedence over all user settings.

This setting can also be set per user using **User | Telephony | Supervisor Settings | Inhibit Off-Switch Forward/Transfer**.

Remote Forwarding Controls

By default IP Office and the IP Office Voicemail applications do not provide any mechanisms for remote modification of User Forwarding settings. However, Mobile Call Control can be enabled to give access. For information, see “Mobile Call Control” in *Administering Avaya IP Office™ Platform with Manager*.

There is also a Voicemail Pro **Configuration Menu** option that can be added to a custom call flow to allow users to remotely change their forwarding and other settings.

Before enabling either of these options the warnings in the manuals must be considered and a judgement made to decide if the benefit is worth the risk of unauthorized access.

Securing Manager

It is important that not only the IP Office and server applications, but the management tools and associated configuration data are secured from attack.

Applying the following configuration settings on the Manager **File | Preferences | Security** tab ensures more secure IP Office communications and helps keep configuration data away from unauthorized users.

Configuration Parameter	Setting
Request Login on Save	Enabled
Close Configuration/Security Settings After Send	Enabled
Save Configuration File After Load	Disabled
Backup Files on Send	Disabled
Enable Application Idle Timer (5 minutes)	Enabled
Secure Communications	Enabled

- The **Manager Certificate Check** on the **File | Preferences | Security** tab should be set according to the security policy. It should be set to **None** only for recovery purposes. For more information see Certificates and Trust on page 36 and Appendix C Windows Certificate Management on page 110.
- If mutual certificate authentication is required (i.e. the IP Office Configuration or Security Administration service will request a certificate from Manager) the **File | Preferences | Security | Certificate offered to IP Office** needs to be set with an identity certificate. See Appendix C Windows Certificate Management on page 110. If **Current User** is selected, it will only apply the current Windows user. If **Local Machine** is selected, it will be used for all Windows users of that PC.
- To prevent other administrators from modifying the **File | Preferences | Security** tab settings, ensure those Service Users do not have the rights to edit security settings, or have the **Administrator** Manager Operator Role.
- On the Manager **File | Preferences | Directories** tab, change the **Working Directory (.cfg Files)** to be different from the **Binary Directory (.bin Files)**. If the two directory settings are the same, it potentially allows remote TFTP/HTTP file access to the folder containing copies of configuration files.

  Ensure all offline configuration files, exported files or other configuration data are controlled.
- Ensure all offline configuration files, exported files or other configuration data are controlled.

Securing Web Manager and Web Control

Web Manger and the Linux Web Control Panel are browser-based online management tools that always use HTTPS communication.

- Any browser used for web-based management should have the CA certificate/ID certificate of the IP Office installed in the relevant trusted certificate store. It is possible in some browsers to provide temporary or permanent exceptions, but this should be avoided. For more information about certificates and browser support, see Certificates and Trust on page 36.
- Ensure all offline configuration files, exported files or other configuration data are controlled

Securing Web Licence Manager

Web Licence Manager (WebLM) administrative account are separate to IP Office and logins to WebLM are not integrated into the IP Office AA framework. WebLM administration is browser-based and always uses HTTPS communication.

- Change the password of the default account as soon as possible.
- All passwords must be ‘strong’ and of 8 or more characters. See Password Management on page 31. Any unused accounts must be deleted.
- Any browser used for web-based management should have the CA certificate/ID certificate of the IP Office installed in the relevant trusted certificate store. It is possible in some browsers to provide temporary or permanent exceptions, but this should be avoided. For more information about certificates and browser support, see Certificates and Trust on page 36.

Securing System Status Application

SSA will always attempt to connect to the IP Office using the secure TLS service first if the login page setting **Secure Connection** is selected. However if the TLS connection attempt fails, it will offer the user the option to connect over the unsecure connection.

- To prevent the use of the unsecure connection, the Manager security setting **Services | System Status Interface | Service Security Level** should be set to **Secure, Low** or **Secure, Medium**

  Note:

  The use of SSA with the TLS connection will limit the status monitoring capacity, particularly on the IP500 V2 platform. If high SSA events or call rates are anticipated, the unsecure connection should be used with alternative security arrangements.
- There is no checking of the IP Office certificate by SSA when the TLS connection is used hence no certificate configuration is possible on SSA.
- If not required by support personnel using SSA, the rights **Rights Groups | System Status | Read all configuration** and **Rights Groups | System Status | System control** should be removed from the Service User account.
- Any snapshot file saved by SSA may be read by any other SSA instance without authorization. This file can include configuration and other sensitive information and therefore access to the file must be controlled.

Securing Sys Monitor

SysMonitor has a number of connection methods: Two legacy (UDP and TCP), and two contemporary (HTTP and HTTPS). Only the HTTPS method is fully secure, but has the highest processing overhead. UDP has the least.

IP Office support of the various SysMonitor connection methods is controlled by the security settings as follows.

HTTP Service Security Level	HTTP	HTTPS	UDP	TCP
Disabled	Disabled	Disabled	n/a	n/a
Unsecure Only	Enabled	Disabled	n/a	n/a
Unsecure + Secure	Enabled	Enabled	n/a	n/a
Secure Low	Disabled	Enabled	n/a	n/a
Secure Medium	Disabled	Enabled	n/a	n/a
Secure High	Disabled	Enabled	n/a	n/a

Unsecured Interfaces | DevLink	HTTP	HTTPS	UDP	TCP
Disabled	Disabled	n/a	Disabled	Disabled
Enabled	Enabled	n/a	Enabled	Enabled

- A Service User account should be used rather than the legacy Monitor Password, the Manager security using the setting **System | Unsecured Interfaces | Use Service User Credentials**. For default accounts that can use SysMonitor in this way refer to Default Service Users and Rights Groups on page 26.
- The legacy UDP and TCP connection methods should be disabled via the Manager security setting **System | Unsecured Interfaces | DevLink**.

  Note:

  If the legacy connection methods are not disabled, the password exchange between SysMonitor and IPOffice is unsecure.
- Select the correct connection methods in the SysMonitor **File | Select Unit** tab. If HTTPS is used, an identity certificate (certificate plus private key) is requested. This is used by SysMonitor to identify itself.For more information about certificates and PKI, see Certificates and Trust on page 36.
- To ensure only HTTPS is used, the Manager security setting **Services | HTTP | Service Security Level** should be set to disable HTTP.

  Note:

  The IP Office HTTP service is used by many components including H323 phones, IP Office lines, SoftConsole, Voicemail Pro and one-X Portal.
- Any log files saved by SysMonitor may be read by any other SysMonitor instance without authorization. This file can include configuration and other sensitive information and therefore access to these files must be controlled.

Securing Configuration and Other Sensitive Data

IP Office security settings are automatically encrypted and locked to the individual IP Office and cannot be exported, but configuration and other data for IP Office, Voicemail Pro and one-X Portal contain some unencrypted information that may pose a security or privacy threat.

- Any backup data store, for example a file server used for backup/restore, copies of SD cards, must be secured from unauthorized access.
- Any backup/restore mechanism itself must be secure. IP Office, Voicemail Pro, and one-X Portal support secure backup and restore options such as HTTPS, SFTP and SCP.
- Access to call recordings which are held as files on the Voicemail Pro or Contact Recorder server must be controlled.
- Offline and exported configuration files, SysMonitor logs, and Linux server logs should be controlled, for example using encryption with password protection. This should include any configuration or other sensitive data sent outside of the organization.

Securing Voicemail Pro

If incorrectly configured, Voicemail Pro can provide opportunity for unauthorized administrative or mailbox access and toll fraud via the outcalling feature.

- Use the Voicemail Pro client to manage the Administrator account password. The password should be strong and 8 or more characters. Delete any unused accounts.

  Note:

  For Voicemail Pro R9.0 and higher on Server Edition, UCM and the Applications Server, all authentication is deferred to the “local” IP Office. The default administration account is only used under failure conditions. For UCM and Application Server, the local IP Office is a management instance running on the server itself.
- Use the Voicemail Pro client to configure the password used to access the IP Office in **Administration | Preferences | General | Voicemail Password**. The password should be strong and 8 or more characters.

  This password must match the password entered in the Manager setting **File | Advanced | Security Settings | System | Unsecured Interfaces | Voicemail Password**.
- In Manager, the default value for **File | Advanced | Preferences | General | Voicemail IP Address** is 255.255.255.255. Enter the IP address of the Voicemail server.
- Only users and groups that are entitled to use voicemail should have their mail box activated. All others should be disabled using the Voicemail Pro client **Disable Mailbox** setting.

  Note:

  Disabling the mailbox will also disable IMAP, MAPI, email and Web Voicemail integrations for the user
- All mailboxes must be protected by password/Voicemail Code access, except when connecting from trusted extensions with the use of the **User | Source Numbers** field). The recommended minimum is 4 digits for internal use, and 9 when the mailbox can be accessed externally.

- The mailbox password/ Voicemail Code policy can be enforced by enabling the **Voicemail Code Complexity** settings on the Manager **System | Voicemail** tab.
- To prevent Toll fraud via the outdialling feature, enable **Outcalling Control** on the Manager **System | Voicemail** tab.

  If outcalling is required, implement call barring. See Preventing Unwanted Calls on page 84.
- When a phone is in an un-controlled area, the default Trusted Source Number for Voicemail access should be removed, so that all IP Office Voicemail access requires entering the Voicemail access code, even from the user's home extension.
- Disable all unused services such as SMTP and MAPI.
- If the SMTP send feature is used, TLS and authentication should be used if possible.
- If the IMAP4 server feature is used, TLS should be used if possible.

Securing Embedded Voicemail

If incorrectly configured, Embedded Voicemail can provide opportunity for unauthorized administrative or mailbox access and toll fraud via the outcalling feature.

- All mailboxes must be protected by password/Voicemail Code access, except when connecting from trusted extensions. The recommended minimum is 4 digits for internal use, and 9 when the mailbox can be accessed externally.
- The mailbox password/ Voicemail Code policy can be enforced by enabling the **Voicemail Code Complexity** settings on the Manager **System | Voicemail** tab.
- To prevent Toll fraud via the outdialling feature, enable **Outcalling Control** on the Manager **System | Voicemail** tab.

  If outcalling is required, implement call barring. See Preventing Unwanted Calls on page 84.
- When a phone is in an un-controlled area, the default Trusted Source Number for Voicemail access should be removed, so that all IP Office Voicemail access requires entering the Voicemail access code, even from the user's home extension.

Securing Contact Recorder

For more information on the Contact Recorder settings described below, see the section **General Setup** > **Recorder** in *Administering Avaya IP Office™ Platform Contact Recorder*.

- Contact Recorder gives full administrator rights to the first user accessing the web administration page. Therefore, it is important to configure the name and password.
- Ensure a password policy is in place and delete any unused accounts.

  All passwords must be strong and of 8 or more characters.
- Disable the insecure administrative interface (HTTP). Log in to the web administration interface and set **System | Manage Users | Allow unencrypted (http) access** to **No**.

- The Advanced Security section of the Contact Store documentation should be reviewed, however the changing of Contact Recorder ports is not recommended.

Securing one-X Portal

- On first log in to the default **Administrator** account, change the password to a strong password of 8 or more characters.

  Note:

  This account is used by one-X Portal if the IP Office authentication service is not available, see User Accounts and Rights of Access on page 24.

- For subsequent password management, go to the **Configuration | Users** page.

  Delete any unused accounts.

- On the one-X Portal administration page, navigate to **Configuration | Providers | CSTA-Provider | Edit** and configure the password used to access IP Office.

  The password must match the password configured for the IP Office Manager user ID **EnhTcpaService**.

- If one-X Portal clients are to be used externally, follow the procedure Hardening for Remote Worker Operation on page 82.

- If external one-X Portal clients are configured to support VoIP calls, follow the procedure Limiting IP Network Exposure on page 94.

- One-X Portal offers both an HTTP (8080 + 8069) and HTTPS (8443/9443 + 8063) interface for web clients. HTTPS must be used for external access. The HTTP ports can be disabled using the setting **Security | Protocol | Secure Connection (HTTPS)**.

- To administer an Identity certificate for the HTTPS interfaces of Linux-based one-X Portal servers, see Updating Certificates on page 79.

- To administer an Identity Certificate for the HTTPS interfaces of Windows-based servers, use the one-X Portal administration web page and import the PKCS#12 format certificate file using the setting **Configuration | Certificate | Import.** Note this certificate is specific to the one-X Portal HTTPS interfaces and not part of the Windows OS certificate store and must include all intermediate certificates

- On first log in to the default **Superuser** backup and restore account, change the password to a strong password of 8 or more characters.

  For subsequent password management, go to the one-X Portal AFA page and select **Configuration | Edit**.

Limiting IP Network Exposure

It is vital to control the IP network access of IP Office to reduce the exposure to attack. Network security integration is outside the scope of this document, However, this section covers some items that must be reviewed as part of network security hardening.

If using any level of external IP access, IP Office must only be connected via a properly configured firewall or other network security mechanism such as VPN. IP Office must never be connected directly. If no external IP access is required, IP Office must be isolated using a firewall or other mechanism.

Using Manager, the IP Office IP Route table must be inspected for any gateway routes that may have been unintentionally acquired via DHCP. Delete routes if not required and the modigy the DCHP settings to prevent reoccurrence.

Firewall

Any Firewall used **must** be selected, deployed, tested and managed by competent personnel to meet the needs of the IP Office deployment.

The NIST Special Publication (SP) 800-41, *Guidelines on Firewalls and Firewall Policy* provides background information, including other helpful resources. It is located at http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf.

Only the absolute minimum of Firewall ports and protocols should be opened for use with IP Office. For example, set only the port direction and protocol needed. The relevant IP Office port matrix for each release must be used. A link to the port matrix document is located on the Avaya Product Security page at https://support.avaya.com/security.

Firewall guidelines:

- If a remote IP address is static, an ITSP SIP trunk for example, the source address should be configured to constrain the access further.
- IP Office unsecure ports/protocols should never be exposed to the Internet.
- If using a stateful Firewall, H.323 inspection should be turned off as this will interfere with IP Office operation.

Session Border Controller

The Avaya Session Border Controller for Enterprise (SBCE) serves as a security and demarcation device between the IP-PBX and the Carrier facility. Avaya supports an implementation of the Avaya SBCE parallel to the firewall. However, it is recommended for best practices security to put it behind the firewall as part of a layered defence strategy. The Avaya SBCE performs NAT traversal, securely anchors signalling and media, and can normalize SIP protocol implementation differences between carrier and Enterprise SIP implementations.

Remote Maintenance Access

Due to the combination of ports and protocols used in typical maintenance activities, Virtual Private Network (VPN) technologies should be used.

IP Office supports secure and high integrity SSL VPN connectivity, and Avaya offers IP Office Support Services (IPOSS) based on this technology. For more information, see *Deploying Avaya IP Office™ Platform SSL VPN Services*.

For Enterprise Branch deployments, Avaya's Secure Access Link (SAL) gateway can be utilized.

Securing Maintenance Interfaces

Events and alarms can be securely sent to syslog servers (including the IP Office Primary Server) using the TLS protocol. This can be enabled using the Manager setting **System | System Events | Alarms | Syslog | Protocol**. Both the System Status Application and SysMonitor access to IP Office can be secured. See Securing Management Applications on page 87.

SNMP should not be used as this is not secure.

Enabling security on these interfaces will increase the software processing of the IP Office and will be unsuitable for instances where high traffic is expected. In a high traffic scenario, local monitoring via unsecured interfaces or external secure solution are required. See Limiting IP Network Exposure on page 94.

Unsecure modems should not be left connected to the serial or analogue ports.

Securing Server Edition Servers

- It is important to understand the information and recommendations of Certificates and Trust on page 36 to determine the certificate and trust requirements of the server as options are offered during the initial ignition process.
- The ignition process will enforce a change to the Administrator and security passwords, it also updates the fall back accounts for one-X Portal, Voicemail Pro and Web Control (the local Linux administration web interface).
- All security administrator account passwords of all other systems in the Server Edition solution need to be the same. This can be done using IP Office Manager **Security | General | General** to change individual settings.
- All Service User account credentials used for central management of all systems need to be the same. This can be done using Web Manager **Security Manager | Service Users | Synchronize Service User and System Password**.
- Apply a password policy to the Web Control application using Web Manager **Platform | Settings | System | Password Rules Settings**.
- Enable the setting Web Manager **Platform | Settings | System | Authentication | Enable referred authentication**. This will refer all Web Control logins to the local IP Office. The local Linux Administrator account credentials are only used under failure conditions.
- Disable the HTTP backup/restore server using Web Manager setting **Platform | Settings | System | HTTP Server**. For release 9.1 and later, an HTTPS backup/restore server is always active for this purpose.
- Enable the internal server firewall to apply DoS and DDos attack filters using Web Manager setting **Platform | Settings | System | Firewall Settings | Activate**.

  Note:

  The firewall support on Server Edition does not replace the need for an external firewall. For further information see Limiting IP Network Exposure on page 94.

- Disable any unused unsecure TCP or UDP ports using Web Manager setting **Platform | Settings | System | Firewall Settings | Enable TCP/UDP Ports**. This will apply filtering to all LAN 1 and LAN 2 traffic, regardless of source or destination.
- If the ingress ports utilized by all IP Office operations conform to the following table, the setting **Platform | Settings | System | Firewall Settings | Enable Filter** can be activated.

Protocol	Ports
TCP	22, 25, 37, 143, 389, 411, 443, 445, 514, 993, 1433, 1434, 1718:1720, 4097, 4560, 5060:5061, 5222, 5269, 5443, 5800:5899, 6514, 7070:7071, 7443, 8005, 8063, 8084, 8087, 8135, 8411, 8444, 8666, 8443, 8805, 9092, 9094, 9095, 9443, 9444, 9888, 32768:65280
UDP	37, 53, 67, 68, 123, 161, 162, 389, 500, 514, 520, 1024:65535

  For more information on IP Office port/protocol usage, see the relevant IP Office port matrix which can be found at https://support.avaya.com/security
- If not required, disable the syslog receiver on the **Primary Settings | General** tab.
- If not required, remove the syslog client on the Secondary and each Expansion System using the Manager setting **System | System Events | Alarms | Destination Syslog**.

  Note:

  Removing the syslog destination will stop audit trail and security events being sent to the Primary Server.
- If not required, disable the Access Security Gateway (ASG) support using the Web Manager setting **Platform | Settings | ASG Settings | Status**.
- If required, administer a new server identity certificate using Web Manager **Security Manager | Certificates | Edit**. This identity certificate will be automatically propagated to all TLS/HTTPS interfaces of the server. Alternatively if the system is a Primary Server, the Web Manager **Platform | Settings | General | Certificates | Identity Certificates** settings can be used. For more information see Certificates and Trust on page 36.
- Do not activate the server's Intelligent Platform Management Interface (IPMI). This effectively grants physical access to the server.

Securing the Application Server and UCM

The Application Server and Unified Communications Module (UCM) run a 'Shell' IP Office instance. An IP Office Shell Server is a single installation of selected IP Office features running on Linux with management and maintenance services enabled. All telephony functions are disabled and no licensing is required

- It is important to understand the information and recommendations of Certificates and Trust on page 36 on page 25 to determine the certificate and trust requirements of the server as options are offered during the initial ignition process.
- The ignition process will enforce a change to the Administrator and security passwords, it also updates the fall back accounts for one-X Portal, Voicemail Pro and Web Control (the local Linux administration web interface).

- Apply a password policy to the Web Control application using **Settings | System | Password Rules Settings**.
- Enable the setting **Settings | System | Authentication | Enable referred authentication**. This will refer all Web Control logins to the IP Office Shell Server. The local Linux Administrator account credentials are only used under failure conditions.
- To add further administrative accounts: Use IP Office Manager to load the security settings of the IP Office Shell Server that co-resides on the Application Server/UCM at the same IP address.

  Note:

  This is not the UCM host IP500 V2 address.
- Disable the HTTP backup/restore server using **Settings | System | HTTP Server**. For release 9.1 and higher, an HTTPS backup/restore server is always active for this purpose.
- Disable any unused unsecure ports/protocols using **Settings | System | Firewall Settings**. This will apply filtering to all LAN 1 and LAN 2 traffic, regardless of source or destination.

  Note:

  The firewall support on the Application Server do not replace the needs for an external firewall. For further information see Limiting IP Network Exposure on page 94.
- If not required, disable the Access Security Gateway (ASG) support using the Web Manager setting **Platform | Settings | ASG Settings | Status**.
- If required, administer a new server identity certificate on the IP Office Shell Server using the IP Office Manager **System | Certificates | Identity Certificate | Set**; this identity certificate will be automatically propagated to all TLS/HTTPS interfaces of the server. Alternatively if the system is an Application Server, the Web Control **Settings | General | Certificates | Identity Certificates** settings can be used. For more information see Certificates and Trust on page 36.
- If required, administer a new server identity certificate on the IP Office Shell Server using the IP Office Manager **System | Certificates | Identity Certificate | Set**; this identity certificate will be automatically propagated to all TLS/HTTPS interfaces of the server. For more information see Certificates and Trust on page 36.
- Do not activate the server's Intelligent Platform Management Interface (IPMI). This effectively grants physical access to the server.

Chapter 9: Monitoring IP Office Platform

Constant and consistent monitoring ensures any threats can be identified early and reacted to. In addition to threat monitoring, existing installations should be reviewed for changes in security requirements that may be caused by customer needs, technology, or regulation.

- Activate all necessary reporting. See Activating Reporting and Monitoring on page 100.
- Monitor all alarms and logs, especially for repeated failed logins or other evidence of attack.
- Detect other unusual activity, for example:
  - New VoIP extensions
  - Forwarding set
  - Phones dialling unexpectedly
  - Unable to make outgoing calls
  - Unusual call destinations
  - Unusual call volumes or time of day/week
  - High phone bill
  - Unable to login to phones or applications
  - Unable to use voicemail
  - The string “Barred” is contained in SMDR reports
  - The syslog tag of “IPTables-Rejected” is contained in Linux server syslog events
- Review Avaya Security advisories.
- Review Avaya IP Office application notes, technical bulletins and tips.
- Ensure the latest IP Office service packs are applied.
- Monitor telephony provider communications.
- Conduct periodic security reassessment.

Checks and Tests

Thorough checks and tests must be carried out to ensure the deployment is secure and no previous attacks have compromised the system. Perform the following tasks.

- Check LAN1/LAN2 do not have public IP addresses
- Check the IP Office for insecure internet or inbound IP access by identifying the public IP address of the Firewall (for example, by using http://whatismyipaddress.com), and then testing the following access points:
  - IP Office Manager using the public IP address

- Voicemail Pro client using the public IP address
- System Monitor using the public IP address
- Browser using http://<Public IP Address>
- Browser using http://<Public IP Address>:8080/onexportal-admin.html
- Browser using https://<Public IP Address>:7071
- Browser using https://<Public IP Address>:7070

If any are successful, it indicates an incorrectly configured firewall or other network protection system.

- Use IP Office Manager to load the configuration and review all errors and warnings with particular reference to passwords. None should be present.
- Check for unexpected Extensions and Users.
- Check all users' settings for unusual forwarding destinations.
- Ensure All SIP Extensions' **Extension |Extn |Force Authorisation** setting has not been disabled.
- Check the special IP Office user 'NoUser' Source Number field. Any unexpected entries should be clarified with support personnel. NoUser source numbers are sometimes used to enable specific features or behaviour.
- Use IP Office Manager to load the security settings, if a warning is displayed regarding default settings, the service user accounts are at default.
- Log on to one-X Portal administration page. If a warning is displayed 'Change Administrator Default Password' the administrator account is at default.
- For release 9.0 and higher, if login to Web Control, one-X Portal, or Voicemail Pro fails unexpectedly, check the IP Office security settings for the account being used. The account must have a rights group assigned which contains the correct "External" rights.
- Check that successful and failed logins produce the expected reports and results.
- Test the call barring, emergency calls and authorization codes. Testing of Emergency Calls must be arranged in advance with the PCSP/Emergency Services to avoid prejudicing genuine emergency response.
- Review Firewall, SBC, and call logger reporting.

Response to Incidents

Containment, eradication and recovery is the recommended process to follow if a security incident has been detected.

- Attacked or compromised systems should be isolated or otherwise protected as soon as possible.
- Avaya customers with information regarding any discovered security problems with Avaya products should create a Service Request using the Self Service link on https://support.avaya.com, or by contacting the Customer Support phone number under the Maintenance Support link (1-800-242-2121 for US domestic customers). Non-Avaya customers wishing to report a security finding with Avaya products should send this information to securityalerts@avaya.com . See Appendix A - Avaya Product Security Support on page 85 for further information.

- Avaya provides a document to assist customers with security requests, see https://downloads.avaya.com/css/P8/documents/100161515
- If the attack is IP based, it may be possible to trace the source IP address to the ISP it's registered to and report it.
- A general guide to incident handling is provided by NIST Special Publication (SP) 800-61, *Computer Security Incident Handling Guide*.

  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Activating Reporting and Monitoring

To ensure timely indication of any untoward activities on any component, various reporting mechanisms should be enabled. It is important to ensure that the reporting mechanisms themselves are reliable and secure.

IP Office

The following events and logging features are available for IP Office.

- System events for failed logins and SSL/TLS failures, potentially indicating attempts to gain unauthorized access to the system. Available as syslog, SMTP (email), SNMP traps and displayable in SSA. For information, see:
  - "Service Alarms" in *Using Avaya IP Office™ Platform System Status Application*.
  - The description of the **System | System Events** tab in *Administering Avaya IP Office™ Platform with Manager*.
- Audit trail of administrative logins, their source and result. Available as syslog events, also displayable in SSA and Manager. Note that user and phone based changes are not currently captured. For information, see:
  - "Control Unit Audit" in *Using Avaya IP Office™ Platform System Status Application*
  - **File | Advanced | Audit Trail** in *Administering Avaya IP Office™ Platform with Manager*

  For Server Edition, all events are active and send via syslog to the Primary Server.
- Detailed audit trail of all administrative changes, including security settings. Available as syslog events only.

  By default for Server Edition, all events are active and send via syslog to the Primary Server.
- Reports of all calls available as Station Message Detail Reporting (SMDR) message that can be sent to 3rd party call loggers. For information, see the SMDR section in *Administering Avaya IP Office™ Platform with Manager*

Voicemail Pro

The following events and logging features are available for Voicemail Pro server.

- Audit trail of administrative logins. Available as syslog events only. For information see "Voicemail Pro Syslogs" in *Administering Avaya IP Office™ Platform Voicemail Pro*.

  By default for Server Edition, all events are active and send via syslog to the Primary Server.

- Voicemail box login failures are reported via the IP Office failed login alarms.

Contact Recorder

Audit trail details of administrative logins are available as syslog events and are displayed on the web administration page. For information, see **System** > **Audit Trail** in *Administering Avaya IP Office™ Platform Contact Recorder*.

one-X Portal

The following events and logging features are available for one-X Portal server.

- Audit trail details of administrative logins are available as syslog events. By default for Server Edition, all events are active and send via syslog to the Primary Server.
- One-X client login failures are reported via the IP Office failed login alarms.

Linux-based Servers

Server Edition, Application Server and UCM servers generate security and audit logs via syslog, either saved internally or sent to a remote server.

- To enable the Linux OS security and audit logging, the following settings must be enabled on the **Web Control | Settings | General Tab**.
  - **Authentication and authorization privileges**
  - **Information stored by the Linux audit daemon (auditd)**
  - **Apache web server access_log and error_log**
- By default for Server Edition, all events are active and send via syslog to the Primary Server where they can be stored, viewed and forwarded to external syslog servers. For more information see **Logs | System Events Viewer** and **Settings | General** in the Web Control application.

Other Components

- Activate firewall intrusion detection and reporting.
- Activate SBC intrusion detection and reporting.
- Activate call logger unusual call activity detection and reporting.

Avaya Security Advisories and IP Office Updates

Register for Avaya Security Advisory notifications by using the E-Notification subscription procedures described at http://support.avaya.com.

See Appendix A - Avaya Product Security Support on page 85

Register for IP Office Knowledgebase news, which includes updates on technical bulletins, application notes and technical tips using the options available at: http://marketingtools.avaya.com/knowledgebase/.

Chapter 10: Appendix A — Avaya Product Security Support

The Avaya Product Security Support Team (PSST) performs the following functions:

- Manages Avaya product vulnerabilities and threats.
- Maintains information posted at http://support.avaya.com/security.
- Performs security testing and auditing of the core products of Avaya.
- Resolves security-related field problems in support of Avaya Global Services.
- Manages the securityalerts@avaya.com mailbox.

As a result, the PSST actively monitors security issues related to the following topics:

- Avaya products
- Products that are incorporated into Avaya products
- General data networking and telecommunications, as identified by government agencies

When a security vulnerability is identified, the PSST determines the susceptibility of Avaya products to those vulnerabilities and assigns one of four risk levels: High, Medium, Low, and None. Depending on the category of risk, the PSST creates an Avaya Security Advisory to notify customers of the vulnerability.

Depending on the vulnerability and its risk level, the advisory might include a recommended mitigation action, a recommendation regarding the use of a third-party-provided patch, a planned Avaya software patch or upgrade, or additional guidance regarding the vulnerability or more.

Accessing Avaya Security Advisories

Avaya Security Advisories are posted on the Security Support web site at http://support.avaya.com/security. Customers can register on the Avaya Support web site to receive email notifications of Avaya security advisories. The time frame of distributing advisories is indicated in the following table.

Vulnerability classification of Avaya	Target intervals between assessment and notification
High	Within 24 hours

Table continues…

Vulnerability classification of Avaya	Target intervals between assessment and notification
Medium	Within 2 weeks
Low	Within 30 days
None	At the discretion of Avaya

About this task

Perform this procedure to receive advisories by email on the Avaya Security Support web site.

Procedure

1. In a web browser, go to http://support.avaya.com.
2. If you do not yet have an account, select **Register Now** from the right side of the page and create an account.
3. Once you have registered, go back to http://support.avaya.com and select **Sign In** from the right side of the page and log in using your credentials.
4. Once logged in, click **Profile** on the right side of the page.
5. On the user profile page, click on the **Hi, <your_name>** tab in the upper part of the page.
6. In the tab that opens, click **E Notifications**.

   All available general notifications are listed on the left side of this page.
7. To receive notification when Security Advisories are posted, check the **Security Advisories** check box and then click **Update**.
8. If you want to receive notifications on an individual product and release basis, click **Add More Products**.
   a. Select the product you wish to receive Security Advisory notifications for.
   b. Select the release of the product.
   c. Click the check box for **Security Advisories**.
   d. Click **Submit**.
   e. Repeat for any additional products and releases.
9. You receive a message that the submission is successful.

   You will now receive notification when new and updated Security Advisories are available.

Interpreting an Avaya Security Advisory

The precise definitions that PSST follows in classifying vulnerabilities relative to their potential threat to Avaya products is available in the Security Vulnerability Classification document available at https://support.avaya.com/css/P8/documents/100066674. The following table summarizes the three main categories.

Vulnerability classification	Criteria for classification
High	A product's risk to a particular vulnerability is categorized as **HIGH** if one or more of the following criteria are met: • An exploit can easily be performed by a remote unauthenticated attacker which provides a high-level administrative control of a system and/or a critical application AND does not require user interaction beyond standard operating procedures. • An exploit can be easily performed by a remote unauthenticated attacker which causes the system and/or a critical application to shutdown, reboot, or become unusable AND does not require user interaction. For example, see the advisory at http://support.avaya.com/css/P8/documents/100062710
Medium	A product's risk to a particular vulnerability is categorized as **MEDIUM** if no higher criteria are met, but the risk does meet one or more of the following criteria: • An exploit can be performed which provides access to a user account AND does not directly provide the privileges of a high-level administrative account. • An exploit can be performed which causes the system and/or critical application to shutdown, reboot, or become unusable AND would require existing administrative or local account access. • An exploit can be performed which allows a local user account to escalate privileges. For example, see the advisory at http://support.avaya.com/css/P8/documents/100064239
Low	A product's risk to a particular vulnerability is categorized as **LOW** if no higher criteria are met, but the risk does meet one or more of the following criteria: • An exploit can be performed which may be difficult or unlikely without non-standard direct user interaction but could still lead to compromise of the confidentiality, integrity, or availability of resources. • An exploit can be performed which causes non-critical applications to shutdown, reboot, or become unusable For example, see the advisory at http://support.avaya.com/css/P8/documents/100064944
None	A product's risk to a particular vulnerability is categorized as **NONE** if the Avaya product is not susceptible or affected by exploitation attempts. Avaya Security Advisories rated as a risk level NONE indicate that the affected software packages, modules, or configurations are not utilized on an Avaya product. For example, see the advisory at http://support.avaya.com/css/P8/documents/100064240

Security Advisory Organization

Overview

The overview provides a description of the vulnerability. For operating system or third-party software, a link is also provided for quick access to a website for more information. The linked information provides:

- A description of the risk
- Instructions on how to correct the problem, which might include:
  - Installing an update
  - Revising the administration of the product
- A description of what additional security fixes, if any, are included in the update.

Avaya software-only products

For Avaya software-only products, the advisory lists specific Avaya products that use, but are not bundled with, operating system software that might be vulnerable. Information includes:

- The product version affected
- Possible actions to take to reduce or eliminate the risk

Avaya System Products

For Avaya system or turnkey products, the advisory lists the specific Avaya products that are vulnerable or are bundled with operating system software that might be vulnerable. Information includes:

- The level of risk
- The product version affected
- Possible actions to take to reduce or eliminate the risk

Recommended Actions

The advisory provides a list and description of steps to take to remove the vulnerability. The steps might include installing a security update, administering a security feature, or performing a software upgrade. For operating system and third-party software, the recommended actions are normally identified in detail through website links in the security advisory.

Target Remediation Intervals

Generally, Avaya makes security updates available on or through the Avaya Security website at http://support.avaya.com/security. In addition, Avaya incorporates security updates, if applicable, in subsequent software release packages.

Based on the classification of vulnerability and the availability of a vendor-supplied update, Avaya makes a best effort attempt to provide remediation actions based on the following target intervals

Vulnerability	Target Remediation Interval
High	If a software patch needs to be developed by Avaya, a timeline for availability of a patch will be provided in the Avaya Security Advisory. Avaya will incorporate the fix into a service pack or update (30 days maximum). If a software patch is available, recommended actions will be described in the Avaya Security Advisory. Any recommended actions which can be pursued by the customer will be included in the Avaya Security Advisory when it is issued.
Medium	If a software patch needs to be developed by Avaya, it will be included in the next minor release where the patch can reasonably be incorporated. If no new minor releases are scheduled for a product, and Avaya is providing maintenance support, Avaya will incorporate the fix into a service pack or update (90 days maximum). If a software patch is available, recommended actions will be described in the Avaya Security Advisory. Any recommended actions which can be pursued by the customer will be included in the Avaya Security Advisory when it is issued.
Low	If a software patch needs to be developed by Avaya, it will be included in the next major release where the patch can reasonably be incorporated. If no new major releases are scheduled for a product, and Avaya is providing maintenance support, Avaya will incorporate the fix into a service pack or update (1 year maximum). If a software patch is available, recommended actions will be described in the Avaya Security Advisory. Any recommended actions which can be pursued by the customer will be included in the Avaya Security Advisory when it is issued
None	No remedial actions will be required.

Chapter 11: Appendix B — Default Trusted Certificates

There are two certificates that are trusted by IP Office. They are present on initial default and when the security settings are reset.

Name	Expiry	Thumbprint	Usage
VeriSign Class 3 International Server CA – G3	07 February 2020 23:59:59	b18d9d195669ba0f7829517566c25f422a277104	A VeriSign intermediate certificate authority owned by Avaya. Trusts the Avaya SSLVPN server and on-boarding files used for the Avaya IP Office Support Services (IPOSS). Required for IP Office registration and connection to IPOSS.
SIP Product Certificate Authority	17 August 2027 05:19:39	4e95552ef2ce93edd255d80f4cd1325c7eb98859	An Avaya legacy SIP certificate authority. Trusts other Avaya servers and phones using default identity certificates. IP Office systems do not use identity certificates signed by this CA.

Related Links

[VeriSign Class 3 International Server CA – G3 in PEM format](#) on page 108
[SIP Product Certificate Authority in PEM format](#) on page 109

VeriSign Class 3 International Server CA – G3 in PEM format

```
-----BEGIN CERTIFICATE-----
MIIGKTCCBRGgAwIBAgIQZBvoIM4CCBPzLU0tldZ+ZzANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJp
U2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxW
ZXJpU2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0
aG9yaXR5IC0gRzUwHhcNMTAwMjA4MDAwMDAwWhcNMjAwMjA3MjM1OTU5WjCBvDEL
MAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQLExZW
ZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2UgYXQg
aHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYykxMDE2MDQGA1UEAxMtVmVy
aVNpZ24gQ2xhc3MgMyBJbnRlcm5hdGlvbmFsIFNlcnZlciBDQSAtIEczMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmdacYvAV9IGaQQhZjxOdF8mfUdza
sVLv/+NB3eDfxCjG4615HycQmLi7IJfBKERBD+qpqFLPTU4bi7u1xHbZzFYG7rNV
ICreFY1xy1TIbxfNiQDk3P/hwB9ocenHKS5+vDv85burJlSLZpDN9pK5MSSAvJ5s
1fx+0uFLjNxC+kRLX/gYtS4w9D0SmNNiBXNUppyiHb5SgzoHRsQ7AlYhv/JRT9Cm
mTnprqU/iZucff5NYAclIPe712mDK4KTQzfZg0EbawurSmaET0qO3n40mY5o1so5
BptMs5pITRNGtFghBMT7oE2sLktiEuP7TfbJUQABH/weaoEqOOC5T9YtRQIDAQAB
o4ICFTCCAhEwEgYDVR0TAQH/BAgwBgEB/wIBADBwBgNVHSAEaTBnMGUGC2CGSAGG
+EUBBxcDMFYwKAYIKwYBBQUHAgEWHGh0dHBzOi8vd3d3LnZlcmlzaWduLmNvbS9j
cHMwKgYIKwYBBQUHAgIwHhocaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYTAO
BgNVHQ8BAf8EBAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2Uv
Z2lmMCEwHzAHBgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDov
L2xvZ28udmVyaXNpZ24uY29tL3ZzbG9nby5naWYwNAYDVR0lBC0wKwYIKwYBBQUH
AwEGCCsGAQUFBwMCBglghkgBhvhCBAEGCmCGSAGG+EUBCAEwNAYIKwYBBQUHAQEE
KDAmMCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC52ZXJpc2lnbi5jb20wNAYDVR0f
BC0wKzApoCegJYYjaHR0cDovL2NybC52ZXJpc2lnbi5jb20vcGNhMy1nNS5jcmww
KAYDVR0RBCEwH6QdMBsxGTAXBgNVBAMTEFZlcmlTaWduTVBLSS0yLTcwHQYDVR0O
BBYEFNebfNgioBX33a1fzimbWMO8RgC1MB8GA1UdIwQYMBaAFH/TZafC3ey78DAJ
80M5+gKvMzEzMA0GCSqGSIb3DQEBBQUAA4IBAQBxtX1zUkrd1000Ky6vlEalSVAC
T/gvF3DyE9wfIYaqwk98NzzURniuXXhv0bpavBCrWDbFjGIVRWAXIeLVQqh3oVXY
QwRR9m66SOZdTLdE0z6k1dYzmp8N5tdOlkSVWmzWoxZTDphDzqS4w2Z6BVxiEOgb
Ett9LnZQ/9/XaxvMisxx+rNAVnwzeneUW/ULU/sOX7xo+68q7jA3eRaTJX9NEP9X
+79uOzMh3nnchhdZLUNkt6Zmh+q8lkYZGoaLb9e3SQBb26O/KZru99MzrqP0nkzK
XmnUG623kHdq2FlveasB+lXwiiFm5WVu/XzT3x7rfj8GkPsZC9MGAht4Q5mo
-----END CERTIFICATE-----
```

Related Links

Appendix B — Default Trusted Certificates on page 107

SIP Product Certificate Authority in PEM format

```
-----BEGIN CERTIFICATE-----
MIIEnTCCA4WgAwIBAgIBADANBgkqhkiG9w0BAQUFADB6MQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEqMCgGA1UECxMhU0lQIFByb2R1Y3QgQ2VydGlm
aWNhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVjdCBDZXJ0aWZpY2F0
ZSBBdXRob3JpdHkwHhcNMDMwNzI1MDAzMzE3WhcNMjcwODE3MDUxOTM5WjB6MQsw
CQYDVQQGEwJVUzETMBEGA1UEChMKQXZheWEgSW5jLjEqMCgGA1UECxMhU0lQIFBy
b2R1Y3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVj
dCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDcOytyx7YRzT7VYJov8FGe6g1GJ0h+4Y7YZzzmgHPqpgn+2jluQi1N
NHliMLbYLnrvf6s3+X/zh7ZND2tyrKZMCYaI8FX6X3tYTONZ9ErTYngSJCpLeCuj
c+qgt1SmRsya1+1F9i5jvrFxoOuRb5N05Yv3cI85SFLw7kEr41cQDvshRBWZfo6r
f3bBJjlqRTHc5yGbXXeEs+JrtIveECFB2Q/w3Eg/GbcWGhP1uqHqOPH76aNMYyQP
GMzDBtpCfGh7HkD7jkT2El+AiBKJy0cOcj22+AKbLvh5bffJMTcCPX2Bax2CD2I1
usQ+osTG+FdvuhRBx+WPqBOWsQ0wRKGNAgMBAAGjggEsMIIBKDA/BgNVHSAEODA2
MDQGC2CGSAGG/AsHAgEBMCUwIwYIKwYBBQUHAgEWF21haWx0bzpzaXBjYUBhdmF5
YS5jb207MB0GA1UdDgQWBBSgggcpXDqgxCm4PcMduQZVE75WKjASBgNVHRMBAf8E
CDAGAQH/AgEBMAsGA1UdDwQEAwIBBjCBpAYDVR0jBIGcMIGZgBSgggcpXDqgxCm4
PcMduQZVE75WKqF+pHwwejELMAkGA1UEBhMCVVMxEzARBgNVBAoTCkF2YXlhIElu
Yy4xKjAoBgNVBAsTIVNJUCBQcm9kdWN0IENlcnRpZmljYXRlIEF1dGhvcml0eTEq
MCgGA1UEAxMhU0lQIFByb2R1Y3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5ggEAMA0G
CSqGSIb3DQEBBQUAA4IBAQBgPraSto+++KAFMtUSGVm4jsbknWwazR5yFxltWrgo
osMN+1t351AEJed1DCvUWibbfSylh13PNzYLhSIlmKPR98LVQ4P5l26C2suJPaye
EUX87wDCHe8eNNG93vl54U4aQDum98FSTRlYjdSiL9R3trKLOiiYlLBE1oJHBGPi
FzRXgc0XVGWXMfAquNQ01pzKqu7ET09AWsYbUS4c+J5tdYk9nYk35Y1WtKwOz8MS
gwkB2ncy1rI6IuWvLAUdd9BKcBYGLSMVulVGjl3Oi0V35xxNoyIKQ98RPIb9RcME
zhiIkhUOktmeYHe9BYn8En76q5oOXH0CaIQOld9Vood/
-----END CERTIFICATE-----
```

Removing the Default Trusted Certificate

To remove that default trusted certificate, a file can be used with the IP Office Trusted Certificate Store delete feature.

1. Create a text file with an extension .pem,
2. Copy the above PEM data including the 'BEGIN CERTIFICATE' and 'END CERTIFICATE' lines into the text file. The line termination can be Windows or Linux.

   One .pem, file per certificate.
3. Using the IP Office or Web Manager File Manager tool, copy the file to the `system/primary/certificates/tcs/delete` directory.
4. Restart IP Office.

To add a default trusted certificate, follow the above steps, but copy the file to the `system/primary/certificates/tcs/add` directory.

The default certificate feature also supports the binary DER format. See Certificates and Trust on page 36 for more information on certificate file formats.

Related Links

Appendix B — Default Trusted Certificates on page 107

Chapter 12: Appendix C — Windows Certificate Management

The certificate store used by a number of Avaya applications to save and retrieve X509 certificates is the default one provided by the Windows operating system. The Windows certificate store is relevant to the many applications running on Windows that uses certificates for security, either TLS or HTTPS, including:

- IP Office Manager
- Avaya Communicator
- Google Chrome Browser
- Safari Browser
- Microsoft Internet Explorer
- Microsoft IIS (used by Windows Voicemail Pro)

There are some applications that currently do not use the Windows certificate store:

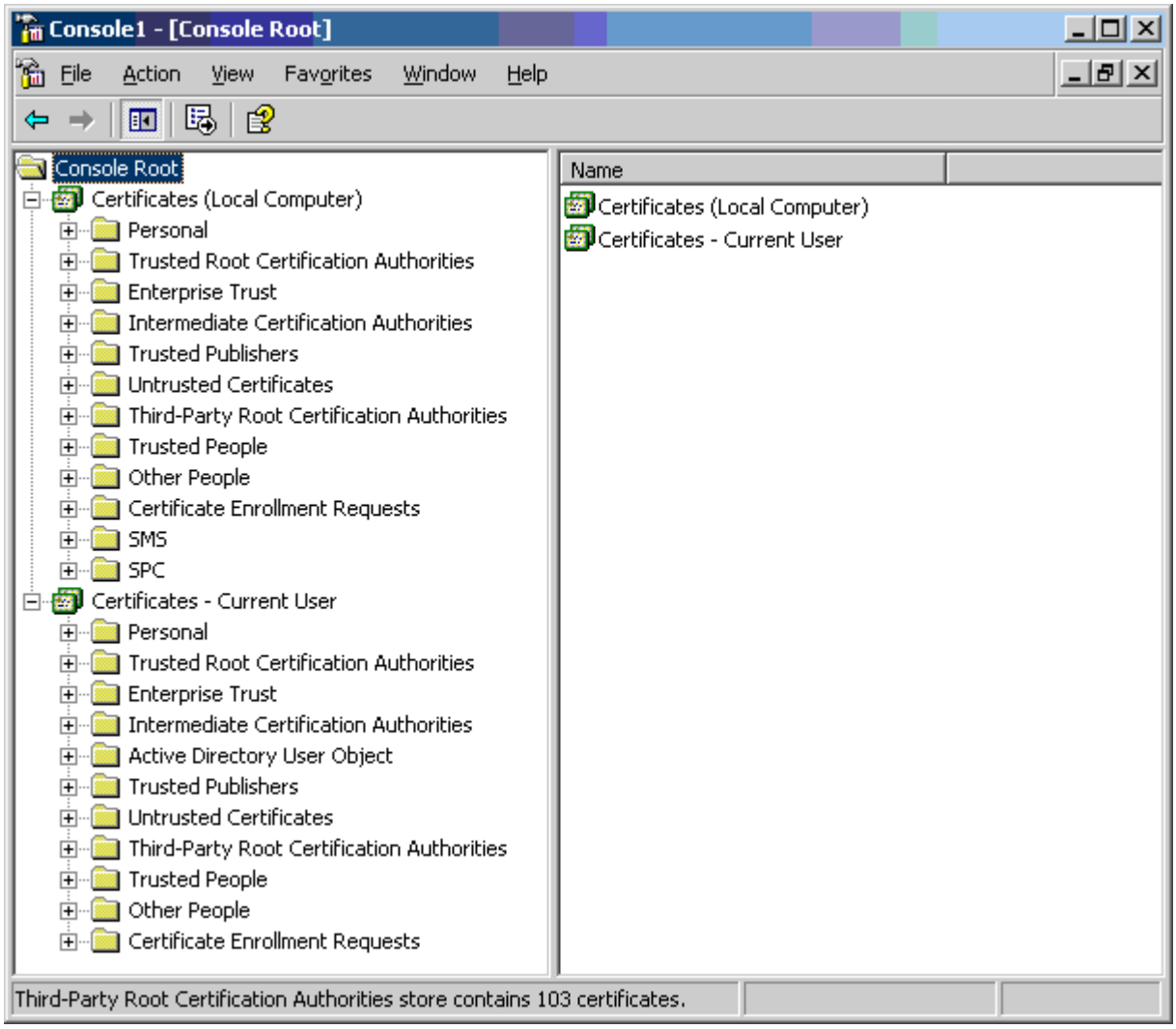
- SoftConsole: uses a local certificate file.
- Firefox Browser: uses an internal certificate store.
- Java Runtime environment 1.6, 1.7 and 1.8: uses an internal certificate store.
- One-X Portal for Windows server.

Warning:

Avaya accepts no responsibility for changes made by users to the Windows operating system. Users are responsible for ensuring that they have read all relevant documentation and are sufficiently trained for the task being performed.

Windows Certificate Store Organization

By default, certificates are stored in the structure shown below.



Each of the sub folders has differing usage. The Certificates - Current User area changes with the currently logged-in windows user. The Certificate (Local Computer) area does not change with the currently logged-in windows user. IP Office Manager only accesses some of the certificate sub folders.

Certificates (Local Computer) Folder	**Manager Use**
Personal | Certificates	Folder searched by Manager 1st for matching certificate to send to the system when requested. Certificate matched by the subject name contained in **File | Preferences | Security | Certificate** offered to the system. Folder accessed whenever 'Local Machine certificate store' used for Security Settings.

Table continues…

Certificates (Local Computer) Folder	Manager Use
	Folder searched by Manager for matching certificate when certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.
Trusted Root Certification Authorities | Certificates	Folder searched by Manager for matching parent certificates when non-self-signed certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.

Certificates - Current User Folder	Manager Use
Personal | Certificates	Folder searched by Manager 2nd for matching certificate (subject name) to send to the system when requested. Certificate matched by the subject name contained in **File | Preferences | Security | Certificate** offered to the system. Folder accessed whenever 'Current User certificate store' used for Security Settings. Folder searched by Manager for matching certificate when certificate received from IP Office, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.
Trusted Root Certification Authorities | Certificates	Folder searched by Manager for matching parent certificates when non-self-signed certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.
Other People | Certificates	Folder searched by Manager for matching parent certificates when non-self-signed certificate received from the system, and **File | Preferences | Security | Manager Certificate Checks** = Medium or High.

Certificate Store Import

In order to use certificates – either for security settings or Manager operation – they must be present in the windows certificate store. Certificates may be placed in the store by the Certificate Import Wizard. The Certificate Import Wizard can be used whenever a certificate is viewed. In order for Manager to subsequently access this certificate the Place all certificate in the following store option must be selected:

- If the certificate is to subsequently identify the system, the Other People folder should be used.
- If the certificate is to subsequently identify the Manager, the Personal folder should be used, and the associated private key saved as well.

Certificate Store Export

Any certificate required outside of the Windows PC must be first saved in the Certificate store then exported. If the certificate is to be used for identity checking (i.e. to check the far entity of a link) the certificate alone is sufficient, and should be saved in PEM or DER format.

If the certificate is to be used for identification (i.e. to identify the near end of a link) the certificate and private key is required, and should be saved in PKCS#12 format, along with a strong password to access the resultant .pfx file.

Chapter 13: Appendix D — SRTP Troubleshooting

Troubleshooting Tools

System Status Application:

Active Calls displays whether call is secure, direct media or relayed, whether SRTP is done by VCM or CPU on IP500 V2. Linux servers always use CPU.

SysMonitor:

- For capturing SRTP traces, set filters to default trace options plus:
  - SIP | Sip + Verbose
  - Media | Media Events | Media handlers
  - Media | VoIP Events | VoIP + Verbose
  - Media | VoIP Events | Primitive + Verbose
- During calls, in the **Status | [S]RTP Sessions** window, column secure describes whether SRTP is used in that call and whether it is done by VCM or CPU on IP500 V2. Use **Show SRTP** button to display further details on SRTP sessions.

Troubleshooting Tips

First step in troubleshooting is to check whether the system and all participating devices are correctly configured. Some endpoints need to be registered using TLS to have SRTP available.

- Ensure that the system is using the default settings for advanced options. If that is not the case, check that it is intentional.
- If SIP devices are used and **Best Effort** is configured, check with SSA/SysMonitor how SRTP is negotiated and whether the device supports cap neg (can be checked by placing a call to device with both SRTP and RTP and then checking whether it responds with SRTP or RTP – if it is SRTP, cap neg is supported). If not, override device media security settings and configure **Enforce** or **Disabled**, as appropriate.
- IP Office lines with **Best Effort** configured and both crypto suites are enabled can result in large call initiation messages on IPO lines, ~ 5000 bytes. If the link is slow and/or the call rate is high it can have a negative impact. Consider using only one crypto suite or the lines' VoIP Settings | Media Security setting to **Enforce** or **Disabled**.

Chapter 14: Appendix E — IP Office Interface Certificate Support

The following table provides an overview of certificate support for the IP Office Platform IP interfaces.

Note:

The relevant endpoint or server documentation should be consulted as supported features may vary with release.

For a full list of ports, see the relevant IP Office port matrix at https://support.avaya.com/security.

Link	Protocol	Cert Support	ID Cert Offered [1]	Cert Trust Checks [2]	Cert check Control [3]	Notes
IP Office						
SIP Line	SIP-TLS	Yes	Tel	Bi	Yes [3] Group 1	
SM Line	SIP-TLS	Yes	Tel	Bi	Yes [3] Group 1	
SIP Extension	SIP-TLS	Yes	Tel	Bi	No	[4]
H323 Extension – signalling	H323	No	n/a	n/a	n/a	[4]
H323 Extension – provisioning	HTTPS	Yes	Man	Bi	Yes [3] Group 2	[4]
DECT R4 Provisioning	HTTPS	Yes	Man	Bi	Yes [3] Group 2	[4]
D100 Provisioning						
IP Office Line	HTTPS	Yes	Man	Bi	Yes [3] Group 3	WebSocket
IP Office Manager - Security	TLS	Yes	Man	Bi	Yes [3] Group 4	Manager and SE Manager

Table continues…

Link	Protocol	Cert Support	ID Cert Offered [1]	Cert Trust Checks [2]	Cert check Control [3]	Notes
IP Office Manager - Configuration	TLS	Yes	Man	Bi	Yes [3] Group 5	Manager and SE Manager
SoftConsole	HTTPS	Yes	Man	Uni	Yes [3] Group 2	WebSocket
SSA	TLS	Yes	Man	Uni	No	
Web Manager (single)	HTTPS	Yes	Man	Bi	Yes [3] Group 6	Web Manager single instance management over port 8443
Web Manager (solution)	HTTPS	Yes	Man	Uni	No	Web Manager Server Edition management over port 7070
System Directory	HTTPS	Yes	Man	Bi	Yes [3] Group 2	Central external directory feature
One-X Portal CTI	TLS	Yes	Man	Uni	No	Supported on Primary/ Secondary Server only.
IPOCC CTI	TLS	Yes	Man	Uni	No	
ACCS CTI	TLS	Yes	Man	Uni	No	
One-X Portal Directory	HTTPS	Yes	Man	Uni	Yes [3] Group 2	Supported on Primary/ Secondary Server only.
Voicemail Pro	HTTPS	Yes	Man	Uni	Yes [3] Group 2	WebSocket
Backup/ Restore client	HTTPS	Yes	Man	Uni	Yes [3] Group 7	
SysMonitor	HTTPS	Yes	Man	Uni	Yes [3] Group 2	
Voicemail Pro						
one-X Portal status	TCP	No	n/a	n/a	n/a	Message Status

Table continues…

Link	Protocol	Cert Support	ID Cert Offered [1]	Cert Trust Checks [2]	Cert check Control [3]	Notes
one-X Portal VM play	HTTPS	Yes	Man	No	No	
Exchange WS client	HTTPS	Yes	Man	Srv	n/a	
SFTP Client	SSHv2	Yes				Exporting voicemail and recording data
One-X Portal						
one-XP Browser/ Call Assistant	HTTPS	Yes	Man [5]	Cli	No	
Outlook, SalesForce, Lync Plugin	HTTPS	Yes	Man [5]	Cli	No	
One-X Mobile Android	HTTPS	Yes	Man [5]	Cli	No	[4]
One-X Mobile iOS	XMPP-TLS	Yes	Man [5]	Cli	No	[4]
Communicator Windows	HTTPS	Yes	Man [5]	Cli	No	[4]
Communicator iOS	XMPP-TLS	Yes	Man [5]	Cli	No	[4]
Backup/ Restore server	HTTPS	Yes	Man	Cli	No	
Linux Server						
Web Control	HTTPS	Yes	Man	Cli	No	
SSH Server	SSHv2	Yes				
SFTP Server	SSHv2	Yes				
WebLM Server						
Web Admin	HTTPS	Yes	Man	Cli	No	
Contact Recorder						
Web Admin	HTTPS	Yes	Man	Cli	No	

Notes:

1. Type of ID certificate presented:
   - Tel = Telephony or management (configurable).
   - Man = Management ID certificate.

2. Support and direction of certificate trust checks:
   - Bi = Mutual certificate checks can be enabled.
   - IPO = Only the IP Office can be enabled to check certificates.
   - Svr = Only the remote server can check certificates.
   - Cli = Only the remote client can check certificates.
3. The grouping for the certificate check controls on the IP Office server component.

Grouping	Control	Notes
Group 1	Manager **Security | System | Certificates | Received Certificate Checks (Telephony)**	Any setting other than **None** will request a client certificate. For more information, see Certificate Checks on page 40.
Group 2	Manager **Security | System | Services | HTTP | Service Security Level** Manager **Security | System | Certificates | Received Certificate Checks (Management)**	For more information, see Certificate Checks on page 40.
Group 3	Manager **Configuration | Line | Line | Security settings**	The HTTP service security level setting is applied first. This allows the general HTTPS server to have cert checks disabled, but still retain check for IP Office lines
Group 4	Manager **Security | System | Services | Security Administration | Service Security Level** Manager **Security | System | Certificates | Received Certificate Checks (Management)**	For more information, see Certificate Checks on page 40.
Group 5	Manager **Security | System | Services | Configuration | Service Security Level** Manager **Security | System | Certificates | Received Certificate Checks (Management)**	For more information, see Certificate Checks on page 40.
Group 6	Manager **Security | System | Services | Web Services | Service Security Level** Manager **Security | System | Certificates | Received Certificate Checks (Management)**	For more information, see Certificate Checks on page 40.
Group 7	Manager **Security | System | Certificates | Received Certificate Checks (Management)**	IP Office HTTP clients will check the server certificate against the TCS for a setting of **Medium** or **High**. For more information, see Certificate Checks on page 40.

4. See Appendix F IP Office VoIP Endpoint Security on page 119 for more details.
5. One-X Portal for Windows uses as separately administered ID certificate.

Chapter 15: Appendix E — IP Office VoIP Endpoint Security

The following table provides an overview of various security aspects of Avaya endpoints with respect to IP Office.

Note:

The relevant endpoint or server documentation should be consulted as supported features may vary with release.

IP Office VoIP Endpoint	Secure Media	Secure Signalling	Secure Remote Settings [1]	IP Office Auto-gen Settings	SIPS Support	Validate Server Cert?	Offer ID Cert? [7]	IP Office Subject Alt Name Required? [8]
96x1	Yes	Yes [2]	Yes	Yes	n/a	Yes	Yes	No
96x0	No	No	Yes	Yes	n/z	Yes	Yes	No
Avaya H.323 Endpoint								
16xx	No	No	Yes	Yes	n/a	Yes	Yes	No
DECT R4	No	No	Yes	Yes	n/a	Yes	Yes	No
IP Office [3]	Yes	Yes	Yes	n/a	n/a	Yes	Yes	No
Voicemail Pro [4]	No	No	Yes	n/a	n/a	No	No	No
Avaya SIP Endpoint								
96x1 [5]	Yes	Yes	Yes	No	Yes	Yes	Yes	No
11xx/12xx	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes [9]
B179	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
E129	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table continues…

IP Office VoIP Endpoint	Secure Media	Secure Signalling	Secure Remote Settings [1]	IP Office Auto-gen Settings	SIPS Support	Validate Server Cert?	Offer ID Cert? [7]	IP Office Subject Alt Name Required? [8]
								[10]
E159	No	No	No	Yes	No	No	No	No
E169	No	No	No	Yes	No	No	No	No
Radvision XT series	Yes	Yes	No	No	Yes [6]	Yes	Yes	Yes [11]
Communicator iPad	Yes	Yes	No	No	Yes [6]	Yes	No	No
Communicator Windows	Yes	Yes	No	No	Yes [6]	Yes	No	No
one-X Mobile iOS	Yes	Yes	No	No	Yes [6]	Yes	No	No
one-X Mobile Android	Yes	Yes	No	No	No	Yes	No	Yes [12]
D100 SIP DECT	No	No	No	Yes	No	No	No	No
IP Office Softphone (Mac)	No	No	Yes	Yes	No	Yes	No	No

Notes:

1. Ability for the phone to remotely download settings and configuration in a secure manner, typically via HTTPS.
2. Partial. Signalling is not fully secure, but regestration, SRTP Key exchange, and dialled digits are.
3. IP Office line with WebSocket and security active.
4. Link between Voicemail Pro and its host IP Office. For Server Edition and UCM this is an internal link.
5. 96x1 SIP phones only supported as centralized users in a branch deployment.
6. Always active when TLS selected.
7. IP Office does not request certificates from SIP clients for the SIP-TLS session at present. It will request a certificate for any HTTPS transfer. according to the **Mutual Authentication** setting; see Certificate Check Controls on page 51 for further information
8. This column indicates whether the client requires Subject Alternative Name support within the received identity certificate from IP Office.
9. • IP.1: IP address of IP Office LAN1

- IP.2: IP address of IP Office LAN2
- IP.3: Public IP Address if remote

10. • DNS.1: FQDN of IP Office
    - DNS.2: IP address of IP Office if the phone is configured to connect to SIP server using IP address instead of FQDN
    - SIP URI: IP address of IP Office
11. • DNS.1: FQDN of IP Office
    - IP.1: IP address of IP Office LAN1
    - IP.2: IP address of IP Office LAN2
12. • DNS.1: FQDN of IP Office
    - IP.1: IP address of IPOffice LAN1
    - IP.2: IP address of IPOffice LAN2
    - IP.3: Public IP address of IPOffice if remote

Chapter 16: Appendix G — Using the IP Office Certificate Authority

The Certificate Authority (CA) feature of the Application Server and Server Edition Primary can be used to:

- Generate an identity certificate for the server itself.
- Generate identity certificates for other devices including IP Office systems, phones and servers.
- Import a new signing certificate
- Refresh the existing signing certificate

Related Links

Generating the CA Server's Own Identity Certificate on page 122
Generating Identity Certificates for Other Devices on page 123
Exporting the Signing Certificate on page 124
Renewing or Replacing the Signing Certificate on page 125

Generating the CA Server's Own Identity Certificate

Use this procedure to manually create an identity certificate for the CA server.

By default, the Primary or Applications servers' own identity certificate is automatically created and signed by the internal CA. It is also automatically re-generated if the LAN1 IP Address, LAN2 IP Address or host name is changed. To prevent automatic regeneration, the Web Management setting **Platform View** > **Certificates** > **Identity Certificates** > **Renew automatically** must be unchecked.

Procedure

1. Log in to Web Manager.
2. On the Solution page, click on the three bar menu icon to the right of the server and select **Platform View**.
3. On the Platform View page, click the **Settings** tab.

   the **General** settings are displayed. Scroll down to view the **Certificate** settings.
4. Under **Identity Certificates**, ensure the check box **Create certificate for a different machine** is unchecked.

5. In the **Default Subject Name**, you can accept the default value or enter a new, unique subject name.

   For more information, see Certificate Name Content on page 50.

6. Enter the **Subject Alternative Name(s)**.

   It is recommended that a full set of subject alternative names are supplied to ensure compatibility with various Avaya clients and endpoints:DNS:<FQDN of server>, IP:<LAN1 IP address>, IP:<LAN2 IP address>, IP:<Public IP address>, DNS:<SIP domain>, URI:sip:<SIP domain>, URI: <LAN1 IP address>, URI: <LAN2 IP address>

   For example:

   DNS:www. tjrlabsystem.com, IP:192.168.0.45, IP:192.168.1.45, IP:135.64.113.102, DNS: tjrlabsystem.sip.com, URI:sip: tjrlabsystem.sip.com, URI: 192.168.0.45, URI:192.168.1.45

7. In the **Duration (days)** field, enter the number of days the certificate will be valid for.

   The start date/time will be the current UTC time of the server. The end date/time will be start time + number of days. Identity certificates should not be valid for more than three years (1095 days). The longer the period, the greater the risk of certificate compromise.

8. Enter the **Public Key Algorithm**. This must be RSA-2048.
9. Enter the **Secure Hash Algorithm**. This must be SHA-256
10. Check the settings and then click **Generate and Apply** .

    The server generates and applies the new certificate during which service loss will occur.

Related Links

Appendix G — Using the IP Office Certificate Authority on page 122

Generating Identity Certificates for Other Devices

Procedure

1. Log in to Web Manager.
2. On the Solution page, click on the three bar menu icon to the right of the server and select **Platform View**.
3. On the Platform View page, click the **Settings** tab.

   the **General** settings are displayed. Scroll down to view the **Certificate** settings.

4. Under **Identity Certificates**, check the check box **Create certificate for a different machine**.
5. In the **Machine IP** field, enter an IPv4 address for the device.

   This is used to create the file name, but not the certificate itself

6. In the **Password** and **Confirm Password** fields, enter a password for the identity certificate.

this is used to secure the identity certificate file and must conform to the complexity requirements.

7. In the **Subject Name** field, enter a unique name for the device.

   For more information, see Certificate Name Content on page 50.

8. In the **Subject Alternative Name(s)** field, enter any subject alternative names.
9. In the **Duration (days)** field, enter the number of days the certificate will be valid for.

   The start date/time will be the current UTC time of the server. The end date/time will be start time + number of days. Identity certificates should not be valid for more than three years (1095 days). The longer the period, the greater the risk of certificate compromise.

10. Enter the **Public Key Algorithm**.

    This should be RSA-2048 for all IP Office devices. Only use RSA-1024 for legacy systems that cannot support RSA-2048.

11. Enter the **Secure Hash Algorithm**

    This should be SHA-256 for all IP Office devices. SHA-1 should only be used for legacy systems that cannot support SHA-256

12. Check the settings and then click **Generate and Apply** .

    The server generatse a PKCS#12 file containing the identity certificate, private key, signing certificate. The file is secured by the password entered and will be requested every time the file is opened.

13. You are prompted to save the file. Save the file to the local machine. The file is deleted on the CA server.

    The PKCS#12 file can now be imported into the IP Office deployment. For one-X Portal Windows this is achieved using the one-X Portal admin web page. For Voicemail Pro Windows, the file is imported into IIS. For IP Office and Linux servers use Web Manager. See the relevant documentation and in this document, see Implementing IP Office PKI on page 60 for more information.

Related Links

Appendix G — Using the IP Office Certificate Authority on page 122

Exporting the Signing Certificate

If the signing certificate is a root CA certificate, it will need to be exported in both PEM and DER formats for later import into various clients and servers in order to trust any identity certificate created by this CA. This does not export the private key, just the certificate

Procedure

1. Log in to Web Manager.

2. On the Solution page, click on the three bar menu icon to the right of the server and select **Platform View**.
3. On the Platform View page, click the **Settings** tab.

   the **General** settings are displayed. Scroll down to view the **Certificate** settings.
4. To export the CA certificate in PEM format:
   a. Under **CA Certificate**, click **Download (PEM–encoded)**.
   b. You are prompted to save the file as `root-ca.pem`. Save the file to the local machine for later distribution.
5. To export the CA certificate in DER format.
   a. Under **CA Certificate**, click **Download (DER–encoded)**.
   b. You are prompted to save the file as `root-ca.crt`. Save the file to the local machine for later distribution.

Related Links

Appendix G — Using the IP Office Certificate Authority on page 122

Renewing or Replacing the Signing Certificate

This procedure presents the options for renewing or replacing the signing certificate.

Procedure

1. Log in to Web Manager.
2. On the Solution page, click on the three bar menu icon to the right of the server and select **Platform View**.
3. On the Platform View page, click the **Settings** tab.

   the **General** settings are displayed. Scroll down to view the **Certificate** settings.

Create a new signing certificate:

4. Under **CA Certificate**, select the **Create New** radio button.

   This creates a completely new root CA certificate and also requires a new ID certificates for all entities. The previous signing certificate is deleted.

Keep all existing ID certificates but refresh the signing certificate:

5. Under **CA Certificate**, select the **Renew existing** radio button.

   This creates a new certificate with the same content and public/private keys, but a different serial number and start/end date. Only this new root CA requires distribution, in-date existing ID certificates signed by the previous CA will still be valid.

Caution:

Care must be taken not to abuse the convenience of this feature as the longer the public/private keys are unchanged, the greater the risk of compromise.

Replace the existing signing certificate:

6. Under **CA Certificate**, select the **Import** radio button.

   The format must be PKCS#12. This replaces the signing certificate and may require new ID certificates for all entities.

Back-up the signing certificate:

7. Under **CA Certificate**, select the **Export** radio button.
   a. A password is requested to secure the PKCS#12 file.
   b. You are prompted to save the file named `root-ca-p12`. Save the file to the local machine and add a `.p12` extension.

Restore the signing certificate:

8. Under **CA Certificate**, select the **Import** radio button.

Related Links

Appendix G — Using the IP Office Certificate Authority on page 122

Chapter 17: Appendix H — Text-based Certificate Signing Requests

One of the following methods can be used to obtain identity certificates based on a text-based Certificate Signing Request (CSR) to an external Certificate Authority (CA). In both cases the PC used will retain the private key and therefore must be secured.

- Microsoft Management Console (MMC) Certificates Snap-in
- OpenSSL Package

For Microsoft Windows-based IP Office application servers for one-X Portal or Voicemail Pro, the Microsoft method is recommended and the server itself can be used to create the CSR and process the received certificate.

For the Linux Application server or Server Edition either method can be used, but the OpenSSL package of the IP Office server itself must not; another PC should create the CSR and process the received certificate.

This section contains procedures for using each method. There is also a procedure for converting certificate files.

Related Links

Creating a CSR using Microsoft Management Console Certificates Snap-in on page 127
Creating a CSR using the OpenSSL Package on page 132

Creating a CSR using Microsoft Management Console Certificates Snap-in

Creating the CSR (MMC)

The following step cover use of the Microsoft Management Console Certificates Snap-in to generate a CSR and process the signed identity certificate. The identity certificate will reside in the Local Machine Personal certificate store and will not be active on any machine interface by default.

All steps must be carefully followed to avoid errors. Further information on the snap-in and certificate operations can be found at https://technet.microsoft.com/en-us/library/cc771157.aspx. Ensure all

naming information has been identified (Common name, Alternate subject names, organization details etc.)

If the selected CA provides instructions or utilities to generate CSRs using Microsoft tools, those can be used in preference to the following steps providing the correct format and content result. Any question on format or content should be clarified with the CA.

Important:

You must be logged in and run the console session as administrator.

Procedure

1. Open Microsoft Management Console (MMC). Click the Windows **Start** menu and in the Search field, enter `mmc`.

   The Console window opens.
2. Select **File** > **Add/Remove Snap-in**.
3. In the Add or Remove Snap-ins window, select **Certificates** from the **Available snap-ins** list and then click **Add**.
4. In the Certificates snap-in window, select **Computer account** and click **Next**.
5. In the Select Computer window, select **Local computer** and click **Finish**.
6. In the Add or Remove Snap-ins window, click **OK**.
7. In the Console window, in the navigation tree on the left, expand **Certificates (Local Computer)**.
8. Right click **Personal** and select '**All Tasks** > **Advanced Operations** > **Create Custom Request**.
9. In the Certificate Enrollment window, click **Next**.
10. Select **Proceed without enrolment policy** and click **Next**.
11. Select **(No Template) Legacy Key**
12. Select **PKCS #10** and click **Next**
13. Under **Certificate Information**, click the down arrow next to **Details** and then click **Properties**.
14. On the **General** tab, type the domain name of the certificate in the **Friendly Name** field.
15. On the **Subject** tab, in the **Subject Name** field, enter the information below, clicking **Add** after entering each type. Do not add any entries not required (for example Organizational Unit Name) or not requested by the CA.

Type	Value	Notes
Country	Country Name (2 letter code)	The Country Name is a 2 letter code defined by https://www.iso.org/obp/ui/#home.

Table continues…

Type	Value	Notes
		Select Country codes, and click search e.g. US
State	State or Province name	Should not be abbreviated.
Locality	Locality name	e.g. City
Organization	Organization name	e.g. Company Name
Organization Unit	Section/Department name	e.g. IT
Common Name	FQDN of server	e.g. www.example.com
Email	Contact email address	e.g. contact@example.com

16. If the CSR is for a multi-domain/SAN certificate, in the **Alternative Name** field, enter the information below, clicking **Add** after entering each type.

Type	Value	Notes
DNS	DNS SAN entry	The first Alternative Name field should be DNS with the same value as the Common Name. e.g. www.example.com e.g. example.com
IP address (v4)	IP SAN entry	e.g. 135.11.53.53 e.g. 135.11.53.63
URL	URI SAN entry	e.g. sip:example.com e.g. 135.11.53.53

17. On the **Extension** tab, expand **Key usage**.
18. From the **Available options** list, select each of the following options and click **Add**: **Digital signature**, **Key encipherment**, and **Data encipherment**.
19. Clear the check box **Make these key usages critical**.
20. Expand **Extended Key Usage**.
21. From the **Available options** list, select each of the following options and click **Add**: **Server Authentication** and **Client Authentication**.
22. Clear the check box **Make the Extended Key Usage critical**.
23. On the **Private Key** tab, expand **Key type**.
24. Select **Exchange**.
25. Expand **Key options**.
26. In the **Key size** field, select **2048**.
27. Select **Make privet key exportable**.
28. If presented, select **Select Hash Algorithm**, and set the value to **sha256**.

29. Review all entries. Check that the **Key options** > **Key size** is still set to the value to **2048**.
30. Click **OK**.
31. In the Certificate Enrollment window, click **Next**.
32. Enter the **File Name** and specify a location to save the CSR to.
33. Under **File format**, select **Base 64**.
34. Click **Finish**.
35. Open the CSR file in a text editor and copy all of the text, including the start and end lines
36. Go to the CA and follow instruction to paste the full CSR into the SSL enrolment form of the CA. If requested, the server software used to generate the CSR can be specified as Microsoft, or Microsoft IIS 7. If requested, SHA-2 should be selected for the hash algorithm. SHA-1 should not be used

Downloading and Importing the Signed Identity Certificate (MMC)

Procedure

1. After approval and generation, receive/download the certificate files from the CA.

   There should be two or more files:

   - The signed identity certificate which needs to be in PKCS#7/P7B or PEM format
   - Zero, one or more intermediate certificates in PEM format

   Download the root certificate in PEM and DER format and put aside for later distribution to IP Office systems.
2. Copy all to the original CSR directory.

   For more information on certificate file formats, see Certificate File Naming and Format on page 41.
3. On the same server the certificate request was created on, open the Microsoft Management Console (MMC). Click the Windows **Start** menu and in the Search field, enter `mmc`.

   The Console window opens.
4. Select **File** > **Add/Remove Snap-in**.
5. In the Add or Remove Snap-ins window, select **Certificates** from the **Available snap-ins** list and then click **Add**.
6. In the Certificates snap-in window, select **Computer account** and click **Next**.
7. In the Select Computer window, select **Local computer** and click **Finish**.
8. In the Add or Remove Snap-ins window, click **OK**.
9. In the Console window, in the navigation tree on the left, expand **Certificates (Local Computer)**.

10. Right click **Personal** and select '**All Tasks** > **Import**.
11. In the Certificate Import Wizard window, click **Next**.
12. Click **Browse** and select the signed identity certificate received from the CA, then click **Open**.
13. Ensure that these options are selected:
    - **Mark the Private Key Exportable**
    - **Import all Extended Properties**
    - **Import all Certificates in the Chain**
14. Click **Next**.
15. Select **Place all certificates in the following store**.
16. Under **Certificate Store**, select **Personal**.
17. Click **Next** and then **Finish**.
18. Check there is a key icon on the new certificate. If not, the private key is not present.
19. Repeat the import process to import the intermediate certificate file(s). There will be no key icon with these new certificates. Again, these must go into the Personal certificate store.
20. Select the identity certificate and click **Open**.
21. select **Details** and verify the content are as expected.
22. Select **Certification Path** and verify all the certificates are present to the root certificate.

Exporting the Signed Identity Certificate (MMC)

The identity certificate and its private key, root and intermediate certificate(s) are now stored in the Local Machine Personal certificate store. These can now be exported in an appropriate format for IP Office.

Procedure

1. On the same server the certificate request was created on, open the Microsoft Management Console (MMC). Click the Windows **Start** menu and in the Search field, enter `mmc`.

   The Console window opens.
2. Select **File** > **Add/Remove Snap-in**.
3. In the Add or Remove Snap-ins window, select **Certificates** from the **Available snap-ins** list and then click **Add**.
4. In the Certificates snap-in window, select **Computer account** and click **Next**.
5. In the Select Computer window, select **Local computer** and click **Finish**.
6. In the Add or Remove Snap-ins window, click **OK**.

7. In the Console window, in the navigation tree on the left, expand **Certificates (Local Computer)**.
8. Right click the identity certificate (the one with the key icon) and select **All Tasks** > **Export**.
9. Click **Next**.
10. Select **Yes, export the private key**.
11. Click **Next**.
12. Select the following:
    - **Personal Information Exchange - PKCS #12 (.PFX)**
    - **Export all Extended Properties**
    - **Include all Certificates in the certification path if possible**
13. When prompted, enter a strong password to secure the file. This password will be requested when later importing into IP Office.
14. Click **Next**.
15. Enter a file name. Rename the ID certificate file `<file_name>.pfx` to `<file_name>.p12`.
16. Click **Next** and then **Finish**.

    The PKCS#12 file `<file_name>.p12` now has the identity certificate, private key and all intermediate certificates.

    `<file_name>.p12` can now be imported into the IP Office deployment. For one-X Portal Windows, this is achieved using the one-X Portal admin web page. For Voicemail Pro Windows, the file is imported into IIS. For IP Office and Linux servers use Manager or Web Manager. See the relevant documentation and Implementing IP Office PKI for more information.

    Retain the `<file_name>.p12`, root and intermediate certificate files for recovery purposes. Note that a password will always be required to open the PKCS#12 file.

Creating a CSR using the OpenSSL Package

Related Links

Appendix H — Text-based Certificate Signing Requests on page 127
Creating the CSR (OpenSSL) on page 133
Downloading and Combining the Signed Identity Certificate (OpenSSL) on page 134
Converting Certificate Files on page 135

Creating the CSR (OpenSSL)

OpenSSL package is a third-party product and Avaya cannot provide assurance or warranty of purpose in any form. OpenSSL is available for both Microsoft windows and Linux machines. See https://www.openssl.org/.

The following has been tested on Windows 64-bit OpenSSL version 1.0.2d. All steps must be carefully followed to avoid errors. Ensure all naming information has been identified (Common name, Alternate subject names, organization details, etc.). If the selected CA provides instructions or utilities for the use of OpenSSL, those should be used in preference to the following steps. Any question on format or content should be clarified with the CA.

Important:

You must be logged in and run the console session as administrator.

Procedure

1. Create a directory for the CSR and key and change to it.
2. In the directory, create a text file named `openssl.cfg`.
3. Add the following content. Ensure no additional line breaks are included.

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
[req_distinguished_name]
countryName = <Country Name (2 letter code)>
stateOrProvinceName = <State or Province Name (not abbreviated)>
localityName = <Locality Name (e.g. City)>
organizationName = <Organization Name (e.g. Company)>
organizationalUnitName = <Organizational Unit Name (e.g. Section/Department)>
commonName = <Common Name (e.g. www.example.com)>
emailAddress = <Email Address  (e.g. contact@example.com)>
[v3_req]
keyUsage = nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = <www.example.com>
DNS.2 = <example.com>
IP.1 = <135.11.53.53>
IP.2 = <135.11.53.63>
URI.1 = <sip:example.com>
URI.2 = <135.11.53.53>
```

- The values inside angle brackets <> must be replaced with the information specific to the CSR. Ensure that the information requested by the CA is supplied accurately.
- The Country Name is a 2 letter code defined by https://www.iso.org/obp/ui/#home. Select **Country codes** and click **Search**.
- Any entries not required (for example Organizational Unit Name) or not requested by the CA can be removed by removing the whole line.

- If the certificate is for a single domain, remove all lines from `subjectAltName = @alt_names` onwards.
- If the certificate is for multiple domains, the first `alt_name` entry should be `DNS.1` and the same as the `Common Name` (e.g. www.example.com).
-

4. Create the CSR and private key using the command line and ensuring no line breaks. Enter

   ```
   openssl req -new -out <example>.csr -newkey rsa:2048 -sha256 -keyout <example>.key
   -config openssl.cfg
   ```

   The `<example>` items must be replaced with the domain name of the device.
5. When you receive the prompt `Enter PEM pass phrase`, enter a strong password for the private key file. This will be requested later when combining the signed certificate.
6. Verify the CSR. From the command line, enter

   ```
   openssl req -text -noout -verify -in example.csr
   ```
7. Check that the output is as expected.
8. Open the CSR file `<example>.csr` in a text editor and copy all of the text.
9. Go to the CA and follow the instructions to paste the full CSR into the SSL enrolment form of the CA. If requested, the server software used to generate the CSR is OpenSSL, or “Other”. If requested, select SHA-2 for the hash algorithm. SHA-1 must not be selected.
10. Keep the `<example>.csr` file for later use. Note that a password is always be required to open the key file.

Related Links

Creating a CSR using the OpenSSL Package on page 132

Downloading and Combining the Signed Identity Certificate (OpenSSL)

After approval and generation, receive/download the certificate files from the CA. There should be two or more files:

- The signed identity certificate which needs to be in PEM format
- Zero, one or more intermediate certificates which need to be in PEM format

If there are download options, selecting “Other” or “Apache” should provide the correct format.

Procedure

1. Copy all files to the original CSR directory. Rename the identity certificate to the domain name with a `.crt` extension.
2. Download the root certificate in PEM and DER format and put aside for later distribution to IP Office systems.

3. If there is more than one intermediate certificate file, you must combine them. From the command line, go to the CSR directory and then enter

   ```
   cat intermediate1.crt intermediate2.crt intermediate3.crt > intermediates.crt
   ```

4. Join the files into a single PKCS#12 file along with the intermediate certificate file. From the command line and ensuring no line breaks, go to the CSR directory and then enter

   ```
   openssl pkcs12 -export -in example.crt -certfile intermediates.crt -inkey
   example.key -out example.p12
   ```

5. When you receive the prompt `Enter pass phrase for example.key`, enter the password used to secure the private key file when creating the CSR.
6. When you receive the prompt `Enter Export Password`, enter a strong password to secure the output PKCS#12 file. This password is requested when importing into IP Office.
7. Review the PKCS#12 file. From the command line, enter

   ```
   openssl pkcs12 -info -in example.p12
   ```

   The identity certificate, private key and all intermediates must be present.
8. The ID certificate file `example.p12` and `intermediates.crt` can now be imported into the IP Office deployment. For one-X Portal Windows, this is achieved using the one-X Portal admin web page. For Voicemail Pro Windows, the file is imported into IIS. For IP Office and Linux servers use Manager or Web Manager. See the relevant documentation and Implementing IP Office PKI for more information.
9. Retain the `example.key` and `example.p12` root and intermediate certificate files for recovery purposes. Note that a password is always required to open the PKCS#12 and key file.

Related Links

Creating a CSR using the OpenSSL Package on page 132

Converting Certificate Files

The `intermediate.crt` file can be in PEM or DER format. It is PEM format if viewable using a text editor. For more information, see Certificate File Naming and Format on page 41.

If an alternate format is required, you can use OpenSSL to convert files.

To convert PEM to DER:

```
openssl x509 -outform der -in intermediate.crt -out intermediate.der
```

To convert DER to PEM:

```
openssl x509 -inform der -in intermediate.crt -out intermediate.pem
```

Related Links

Creating a CSR using the OpenSSL Package on page 132

Chapter 18: Appendix I — Application and Client Security Dependencies

The following table provides an overview of IP Office components and their dependencies on various IP Office security settings.

IP Office Component	Interface Controls	Login Account	IP Office Certificate Use	Other Controls	Notes
Applications					
IP Office Manager	IP Office Service: - Configuration (secure)- Security Administration (secure) Legacy Interface:- Program Code	Service User	Yes: Management		Program Code used for Manager upgrade of IP500 V2 only
Web Management	IP Office Service: - Web Services	Service User	Yes: Management		
Web Control	IP Office Service: - External	Service User	Yes: Management		
Voicemail Pro	IP Office Service: - HTTP (secure)	Voicemail password	Yes: Management		
One-X Portal	IP Office Service: - EnhTSPI Legacy Interface:- HTTP directory	Service User	No		

Table continues…

IP Office Component	Interface Controls	Login Account	IP Office Certificate Use	Other Controls	Notes
	read- HTTP directory write				
SSA	IP Office Service: - System Status	Service User	Yes: Management		
SoftConsole	IP Office Service: - HTTP	IP Office User	Yes: Management		
SysMonitor	IP Office Service: - HTTP Legacy Interface:- DevLink	Service User or Monitor password	Yes: Management	SysMonitor will use a service user when the **Security | System | Unsecured Interfaces | Use Service User Credentials** is active	
TAPI	Legacy Interface:- TAPI	System password	No		TAPI installer requires IP Office TAPI service enabled
DevLink	Legacy Interface:- DevLink	Monitor password	No		DevLink installer requires IP Office DevLink service enabled (?)
Contact Recorder	None	Internal to Contact Recorder		Disable service in Web Control	
WebRTC	IP Office Service: - External	Service User			See WebRTC client below
DECT R4 Master base station	IP Office Service: - HTTP (secure) Legacy Interface:- TFTP directory read	Service User	Yes: Management		See DECT R4 extension below

Table continues…

IP Office Component	Interface Controls	Login Account	IP Office Certificate Use	Other Controls	Notes
ACCS		Internal to ACCS			See ACCS documentation
IPOCC		Internal to IPOCC			See IPOCC documentation
WebLM	Disable service	Internal to WebLM			See WebLM documentation
Lines					
IP Office Line	IP Office Service: - HTTP	IP Office Line password	Yes: Management		
SIP Line	Remove SIP line	SIP Line	Yes: Management-Telephony		
Analogue/Digital	Remove line	No	No		Analogue/ Digital lines cannot be removed
UC Clients					
Avaya Communicator	One-X Portal Service	IP Office User	Yes: Management	HTTPS only can be enabled by the setting **Protocol | Secure Connection (HTTPS)**	
One-X Mobile	One-X Portal Service	IP Office User	Yes: Management		HTTPS only can be enabled
one-XP Browser/ Call Assistant	One-X Portal Service	IP Office User	Yes: Management		HTTPS only can be enabled
Outlook, SalesForce, Lync Plugin	One-X Portal Service	IP Office User	Yes: Management		HTTPS only can be enabled
Web Collaboration	One-X Portal Service	IP Office User	Yes: Management		HTTPS only can be enabled
WebRTC	WebRTC service SIP Registrar	IP Office User	Yes: Management		
Extensions					

Table continues…

IP Office Component	Interface Controls	Login Account	IP Office Certificate Use	Other Controls	Notes
DECT R4	IP DECT Line	IP Office User, SARI/ PARK	No	Auto-create DECT extension	
H.323	H323 Registrar	IP Office User Or Extension password	No	Auto-create H323 extension	
SIP	SIP Registrar	IP Office User	Yes: Management	Auto-create SIP extension	
Analogue/Digital	No	IP Office User	No		Analogue/ Digital extensions cannot be removed

Index

T

U

V

W