



IP Office™ Platform 10.0

IP Office Platform Security Guidelines

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means 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, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. 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, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo), UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

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

License type(s)

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

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

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

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

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

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: <https://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>. Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Downloading Documentation

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

Contact Avaya Support

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

Contents

1. Overview

1.1 Disclaimer	9
1.2 Purpose	9
1.3 Intended Audience.....	9
1.4 Information classifications and NDA requirements.....	9
1.5 Applicability.....	10
1.6 Responsibility for IP Office Security.....	10
1.7 Responsibility for Security Updates.....	10
1.8 Document Changes since Last Issue.....	10

2. IP Office Security Fundamentals

2.1 Encryption.....	13
2.1.1 Message Authentication.....	14
2.1.2 Security Database.....	14
2.2 Authentication and Authorization Framework.....	15
2.3 Linux Platform Security.....	16
2.4 IP Office Services.....	17
2.5 Default Security Settings.....	18

3. User Accounts and Rights of Access

3.1 Service Users.....	21
3.1.1 Changing Administrative Users, Rights Groups and Authentication.....	21
3.1.2 Default Administrative Users and Rights Groups.....	22
3.2 Security Settings on Upgrade.....	25

4. Password and PIN Management

4.1 Password and PIN Policy.....	29
4.1.1 Administrative User Passwords.....	30
4.1.2 IP Office Users' Passwords and Login Codes....	32

5. Certificates and Trust

5.1 Certificate Terminology.....	35
5.1.1 Components of a Certificate	36
5.1.2 Certificate Security.....	36
5.1.3 Certificate Checks.....	36
5.1.4 Certificates and the Transport Layer Security (TLS) Protocol.....	37
5.1.5 Certificate File Naming and Format.....	37
5.2 IP Office Certificate Support.....	38
5.2.1 Interface Certificate Support.....	38
5.2.2 Initial Certificate Settings.....	39
5.2.3 Certificate Name Content.....	43
5.2.4 Certificate Check Controls.....	45
5.2.5 Certificate Distribution.....	46
5.2.6 Determining Trust Policy.....	49
5.2.7 IP Office PKI Trust Approaches.....	50
5.2.8 Selecting IP Office PKI.....	52
5.2.9 Implementing IP Office PKI.....	52
5.2.10 Certificates from External Certificate Authorities.....	54
5.2.11 Certificate Maintenance	56

6. VoIP Security

6.1 IP Office Platform Media Security.....	58
6.2 VoIP Signalling Security.....	60

6.3 Endpoint Provisioning Security.....	60
6.4 SRTP Performance & Capacity.....	61
6.5 Secure Call Indications.....	61
6.6 VoIP Security Planning Considerations.....	62

7. Securing the IP Office Platform Solution

7.1 General Guidelines.....	64
7.2 Assessing IP Office Security Requirements.....	65
7.3 Security Administration.....	65
7.4 Change security defaults.....	65
7.5 Remove unnecessary accounts.....	65
7.6 Disable Unused Services/Interfaces.....	66
7.7 Ensure Minimum Rights of Access.....	67
7.8 Enforce a Password Policy.....	68
7.9 Update Certificates.....	68
7.10 Securing Telephony Users & Extensions.....	69
7.11 Hardening for Remote Worker Operation.....	70
7.12 Securing Trunks/Lines.....	71
7.13 Secure Voice Media.....	71
7.14 Preventing Unwanted Calls.....	72
7.15 Securing CTI Interfaces.....	75
7.16 Securing IP Office Manager.....	75
7.17 Securing Web Manager/Web Control.....	75
7.18 Securing Web Licence Manager.....	75
7.19 Securing System Status Application.....	76
7.20 Securing Sys Monitor.....	76
7.21 Configuration and Other Sensitive Data	77
7.22 Securing Voicemail Pro.....	77
7.23 Securing Embedded Voicemail.....	78
7.24 Securing Contact Recorder.....	78
7.25 Securing one-X Portal.....	78
7.26 Securing Web License Manager (WebLM).....	79
7.27 Securing Avaya Contact Center Applications.....	79
7.28 Limiting IP Network Exposure.....	80
7.29 Secure Maintenance Interfaces.....	80
7.30 Restricting Physical Access.....	81
7.31 Securing Server Edition Servers.....	82
7.32 Securing Application Server/UCM.....	83

8. Monitoring the IP Office Platform

8.1 Checks and Tests.....	87
8.2 Activating Reporting.....	89
8.3 Response to Incidents.....	90

9. Appendices

9.1 Appendix A - Avaya Product Security Support.....	92
9.1.1 Accessing Avaya Security Advisories.....	93
9.1.2 Interpreting an Avaya Security Advisory.....	94
9.1.3 Organization of an Advisory.....	95
9.1.4 Target Remediation Intervals.....	96
9.2 Appendix B - Default Trusted Certificates.....	97
9.3 Appendix C - Windows Certificate Management.....	99
9.3.1 Windows Certificate Store Organization.....	99
9.3.2 Certificate Store Import.....	101
9.3.3 Certificate Store Export.....	101
9.3.4 Certificates Console.....	101
9.4 Appendix D- SRTP Troubleshooting.....	102
9.4.1 Troubleshooting Tools	102

9.4.2 Troubleshooting Tips	102
9.5 Appendix E - IP Office Interface Certificate Support...	103
9.6 Appendix F - IP Office VoIP Endpoint Security.....	106
9.7 Appendix G - Using the IP Office Certificate Authority	108
9.7.1 Generating the CA Server's Own Identity Certificate.....	108
9.7.2 Generating Identity Certificates for Other Devices.....	109
9.7.3 Exporting the Signing Certificate.....	109
9.7.4 Renewing/Replacing the Signing Certificate....	110
9.8 Appendix H - Certificate Signing Requests.....	111
9.8.1 Creating a CSR using Microsoft MMC Certificates Snap-in.....	112
9.8.2 Creating a CSR using the OpenSSL Package..	115
9.8.3 Converting Certificate Files.....	117
9.9 Appendix I - Application/Client Security Dependencies.....	118

10.Document History

Index	0
-------------	---

Chapter 1.

Overview

1. 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.

1.1 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.

1.2 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.

1.3 Intended Audience

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

1.4 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 which may disclose both confidential and proprietary information and require a non-disclosure agreement (NDA) with Avaya.

1.5 Applicability

The following information is applicable to IP Office IP500 V2, IP Office Server Edition, IP Office applications and endpoints for release 9.1 and 10.0.

IP Office Technical Bulletin 169 covers releases 9.0 and prior, and can be found at:

<http://marketingtools.avaya.com/knowledgebase/businesspartner/ipoffice/mergedProjects/bulletins/techbulls/tb169.pdf>.

The following areas are not covered in this document:

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

1.6 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.

1.7 Responsibility for Security Updates

When security-related applications or operating software updates become available, Avaya tests the updates if applicable before making them available to customers. In some cases, Avaya modifies the updated software before making updated software available to customers.

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 [Avaya Product Security Support](#)^[92].

When IP Office software security updates become available, the customer can install the updates 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.

1.8 Document Changes since Last Issue

Updates for IP Office Release 10.0:

- H175 and H.323-TLS endpoints
- PIN/Login code strength suggestions
- Communicator Windows/iPad cannot use extension number to log in; username/password at all times
- IP Office Services Section added
- Improvements to the certificate chapters including wildcard certificate support, selecting the PKI approach
- Hardening steps when SIP registrar or H323 gatekeeper exposed.
- Securing CTI Interfaces, WebLM, IPOCC and ACCS chapters added
- New Telephony API rights; DevLink3, Location API
- Suggested port and default account tests
- New default trusted certificate
- PKCS#7 file conversion added

Chapter 2.

IP Office Security Fundamentals

2. 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

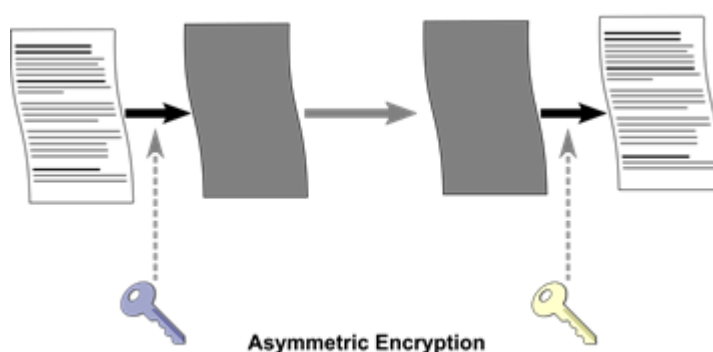
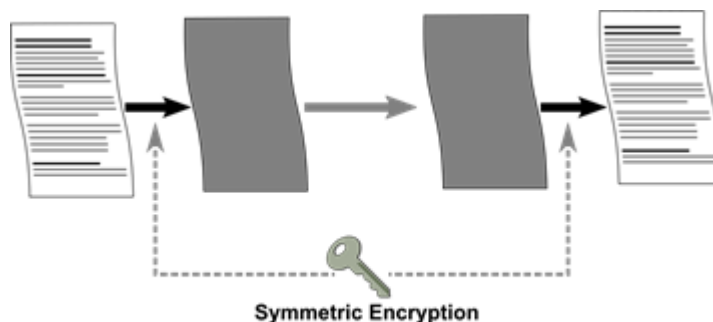
The following table lists methods and techniques used to help counter security threats:

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

2.1 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 is the application of a mathematical process at the originating end, and a reverse process at the receiving end. The process at each end use 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. See [Certificates and Trust](#)^[34] for more information.



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

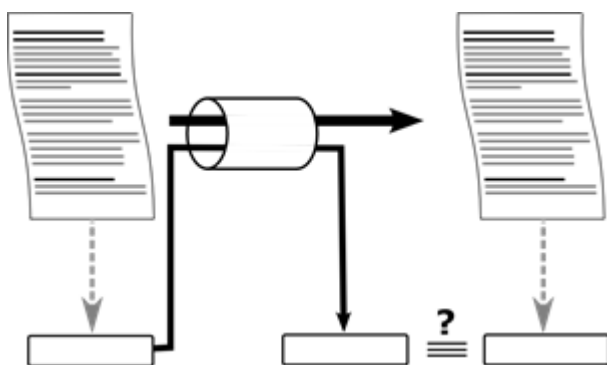
Algorithm	Effective key size (bits)	Use
DES-40	40	Not supported – insufficient strength
DES-56	56	Not supported – insufficient strength
3DES	112 (AKA two key DES)	Not supported – insufficient strength
3DES	168 (AKA three key DES)	'Low' security.
RC4-128	128	'Low' security.
AES-128	128	'Medium' security.
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.

2.1.1 Message Authentication

Message authentication ensures that all data sent by either the system or Manager cannot be tempered with (or substituted) by anyone else without detection. This involves the originator of the data producing a signature (termed a hash) of the data sent, and sending that as well. The receiver gets the data and the signature, and checks 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.

2.1.2 Security Database

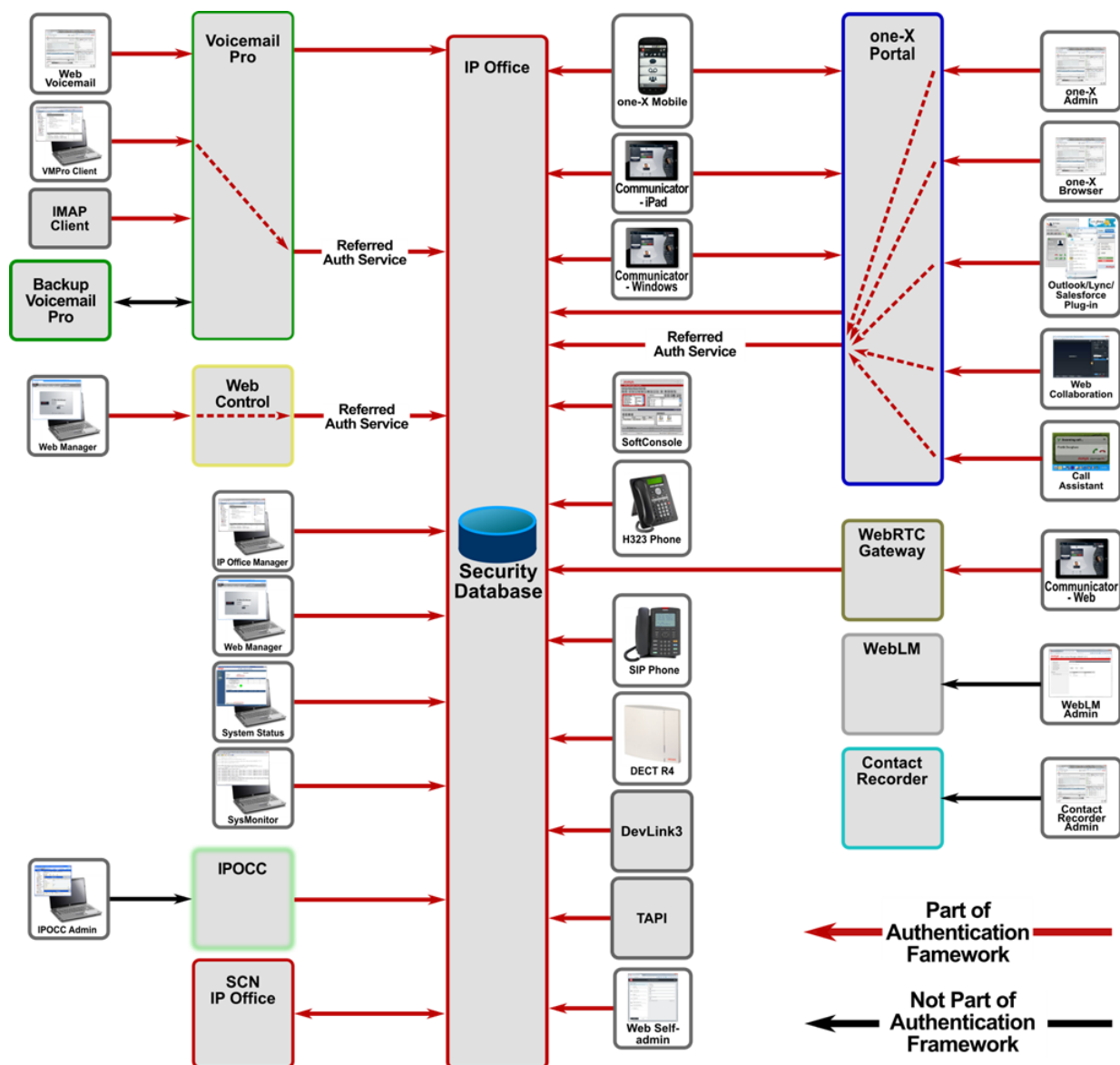
A security database is located on the IP Office which controls all local access, plus remote access to other IP Office components. These security settings have initial default values, can be modified by IP Office Manager or Web Manager, and cover the following areas:

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

The security settings are separate to the IP Office configuration, always secured and cannot be saved or edited offline.

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](#)^[20].

The following diagram shows the service interfaces covered by this framework:



Authentication and Authorization Framework

There are some legacy interfaces which do not pass through the AA framework:

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

2.3 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 because of the 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 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 anti-virus and other security packages for Linux are available, however Avaya does not support the use of such software on the IP Office product 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*" which can be found at <https://downloads.avaya.com/css/appmanager/css/P8Secure/documents/100156571>.

2.4 IP Office Services

All IP Office administrative and maintenance service interfaces are controlled by the security database for availability and security level. These services include:

Service	Usage
Configuration	IP Office Manager and Server Edition Manager configuration access
Security Administration	IP Office Manager and Server Edition Manager security settings (database) access
System Status Interface	System Status Application (SSA) access
Enhanced TSPI	one-X Portal CTI access
HTTP	Phone and IP Office Manager file access, Voicemail Pro, IP Office Line, SysMonitor (secure)
Web Services	Web Manager and SMGR
External	Services external to the IP Office application.

Each service has a configurable Service Security Level:

Service Security Level	Usage
Disabled	The service and corresponding TCP ports are inactive
Unsecure Only	This option allows only unsecured access to the service. The service's secure TCP port, if any, is disabled. This or Disabled are the only options supported for the Enhanced TSPI service
Unsecure + Secure	This option allows both unsecured and secure (Low) access.
Secure, Low	This option allows secure access to that service using TLS, and demands weaker (for example 3DES) encryption and authentication or higher. The service's unsecured TCP port is disabled.
Secure, Medium	This option allows secure access to that service using TLS, and demands moderate (for example AES-128) encryption and authentication or higher. The service's unsecured TCP port is disabled.
Secure, High	This option allows secure access to that service using TLS and demands stronger (for example AES-256) encryption and authentication, or higher. In addition, a certificate is required from the client (for Mutual Authentication). See Certificate Check Controls ⁴⁵ for tests made on the received certificate. If no certificate is received from the client, the connection is rejected. The service's unsecured TCP port is disabled.

Other service interfaces are controlled for activity.

2.5 Default Security Settings

Defaults values for IP Office security settings are loaded on first start-up 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 via a management interface, 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 Administrative Users and Rights Groups](#)^[22]. For information about certificate defaults see [Initial Certificate Settings](#)^[39].

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

Interface	Default Setting	Default Security?	Notes
Configuration	Secure, Medium	✓	IP Office Manager configuration access
Security Administration	Secure, Medium	✓	IP Office Manager security settings access
System Status Interface	Secure, Medium	✓	SSA access
Enhanced TSPI	Unsecure Only	✗	one-X Portal CTI access
HTTP	Unsecure + Secure	✗	Phone and IP Office Manager file access, Voicemail Pro, IP Office Line, SysMonitor (secure)
Web Services	Secure, Medium	✓	Web Manager and SMGR
TFTP Server	Active (IP500 V2) Inactive (Linux)	✗	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 (IP500 V2) Inactive (Linux)	✗	Manager upgrade access
Devlink	Active	✗	DevLink and SysMonitor UDP/TCP access
TAPI	Inactive	n/a	1st and 3rd party TAPI interfaces only.
HTTP Directory Read	Active	✗	one-X Portal directory access, external directory feature
HTTP Directory Write	Active	✗	one-X Portal directory access

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

Chapter 3.

User Accounts and Rights of Access

3. 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.

3.1 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 example illustrated above:

- 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 account can only access the security settings.

3.1.1 Changing Administrative Users, Rights Groups and Authentication

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 should have consistent Service Users and Rights Groups. IP Office Manager and Web Manager have synchronisation tools to assist.
- For All Linux servers, enable Referred Authentication to allow IP Office application to use the local IP Office
- All changes should follow security best practices such as password policy and minimal rights of access.

3.1.2 Default Administrative Users and Rights Groups

The following **Security Administrator** account is present on first start-up 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

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

Account 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
EnhTcpsService	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) access in a branch deployment	SMGR Admin	Enable only when SMGR deployed; will be enabled when the Initial 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

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

Group Name	Usage	Rights Group Users	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 Can use embedded file manager
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 Can use embedded file manager
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 Cannot use embedded file manager
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.	EnhTcpservice	
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

The following **Rights Group** assignments are present on first start-up and security settings reset:

Service	Rights Group > Access Right V	Administrator Group	Manager Group	Operator Group	System Status Group	TCPA Group	IPDECT Group	SMGR Admin
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				✓			
Telephony APIs	Enhanced TSPI Access					✓		
	DevLink 3							
	Location API							
HTTP	DECT R4 Provisioning						✓	
Web Services	Security Read All							✓
	Security Write All							✓
	Security Write Own Password							✓
	Config Read All							✓
	Config Write All							✓
	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							

Service	Rights Group > Access Right V	Administr ator Group	Manager Group	Operator Group	System Status Group	TCPA Group	IPDECT Group	SMGR Admin
	WebRTC Administrator							

3.2 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.

Chapter 4.

Password and PIN Management

4. Password and PIN Management

In general, password and PIN 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. at least 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

A strong PIN/Login Code is typically one that:

- Is long; a 13 digit PIN is similar in strength to an 8 character case-sensitive password
- Does not contain sequences or repeated digits
- Does not contain keypad sequences (for example 2580)
- Is not easily guessable. Guessable PINs include:
 - PIN same as extension number (or reversed)
 - Personal or corporate information
 - Date, prevalent when 4, 6 or 8 digit minimum length is enforced
 - Default login codes

Password and PIN strength and management is not covered in detail here, but many publications exist including:

- 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

4.1 Password and PIN Policy

On a new installation of IP Office, when you ignite a Linux server or first login to Manager or Web Manager, you are required 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 timeout
- Separate set of IP Office User policy settings to allow differentiation

PINs are used on IP Office for telephony user login (Login Code), VoIP extension registration (Phone Password) and voice mailbox access (Voicemail Login Code). The policy is configured using **System | Voicemail | Voicemail Code Complexity** and **System | Telephony | Login Code Complexity**:

- Minimum login code & extension registration length
- Minimum login code & extension registration complexity
- Minimum voicemail code length
- Minimum voicemail code complexity

4.1.1 Administrative User Passwords

There are various accounts used for administrative, maintenance and machine/service access. The following tables cover those interfaces, their password attributes, and where the account settings are located:

Login Interface	Account Settings	Notes
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • Manager upgrade 	System password Password: 1-31 ASCII printable characters	Change using Manager in security settings mode
<ul style="list-style-type: none"> • SysMonitor* • DevLink 	Sysmon password Password: 1-31 ASCII 0-9, 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
<ul style="list-style-type: none"> • Voicemail Pro client 	Three admin roles: - Administrator - Standard - Basic Password: 5-31 ASCII printable characters except \ / : * ? < > , ; .	Change using VMPro client, Voicemail Pro Administrators tab Used for Windows Voicemail Pro at all times Used for Linux Voicemail Pro as a fall-back when IP Office Referred Authentication is not available
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • 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 fall-back when IP Office Referred Authentication is not available
<ul style="list-style-type: none"> • Linux Secure Shell (SSH) 	One admin role: 'Administrator' Password: 1-31 ASCII printable characters	Change using Web Control login screen Can only change password
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • VMPro <> 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
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • TAPI Link Pro (3rd party TAPI) 	System password Password: 1-31 ASCII printable characters	Change using Manager in security settings mode TAPI Link Lite is covered in IP Office Users' Passwords and Login Codes 324.

Login Interface	Account Settings	Notes
<ul style="list-style-type: none"> 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

4.1.2 IP Office Users' 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 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. A new field in release 9.0+ allows VoIP phone login against the extension, not user record: **Extension | Extn | Phone Password**.

All passwords and login codes can be changed in IP Office and Web Manager.

Login Interface	Account Setting	Notes
<ul style="list-style-type: none">• SoftConsole• one-X Portal browser• one-X Mobile Preferred• Communicator Windows/iPad• IP Office Video Softphone• Outlook plugin, Call Assistant• Salesforce & Lync plugin• TAPI Link Lite (1st party TAPI)• RAS (dial in) Users• Web Self-Administration• Web Collaboration conference owner	<ul style="list-style-type: none">• 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 User Passwords ⁽³⁰⁾ .
<ul style="list-style-type: none">• Voicemail Pro mailbox• Embedded Voicemail mailbox	<ul style="list-style-type: none">• User extension: User User Extension• Voicemail Code: User Voicemail Voicemail Code• Attributes: 0-15 ASCII digits	Voicemail settings for password/PIN policy apply: System Voicemail Voicemail Code Complexity . User's voicemail code input not required if accessing voicemail from a trusted extension
<ul style="list-style-type: none">• IP Office User phone login	<ul style="list-style-type: none">• User extension: User User Extension• Login Code: User Telephony Supervisor Settings Login Code• Attributes: 0-31 ASCII digits	System settings for password/PIN policy apply: System Telephony Login Code Complexity . Temporary lock out upon number of consecutive failed attempts
<ul style="list-style-type: none">• H323 Phone registration• SIP Phone registration	<ul style="list-style-type: none">• Phone extension: Extension Extn Base Extension• Login Code: User Telephony Supervisor Settings Login Code• Attributes: 0-31 ASCII digits	System settings for password/PIN policy apply: System Telephony Login Code Complexity . Temporary lock out upon number of consecutive failed attempts For R9.0+, H323 Extension Extn Phone Password field is used if set

Chapter 5.

Certificates and Trust

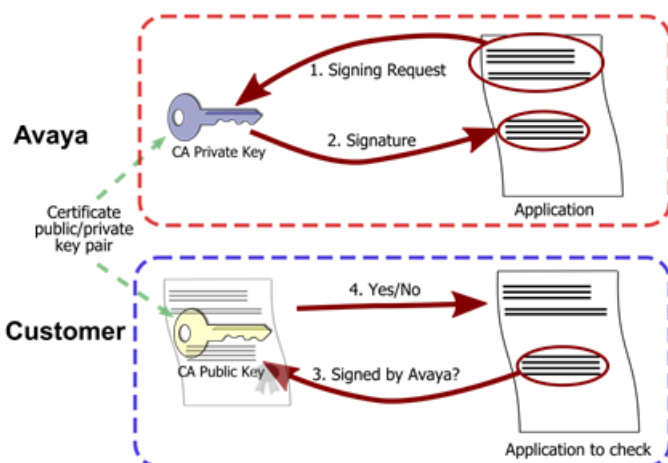
5. Certificates and Trust

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.

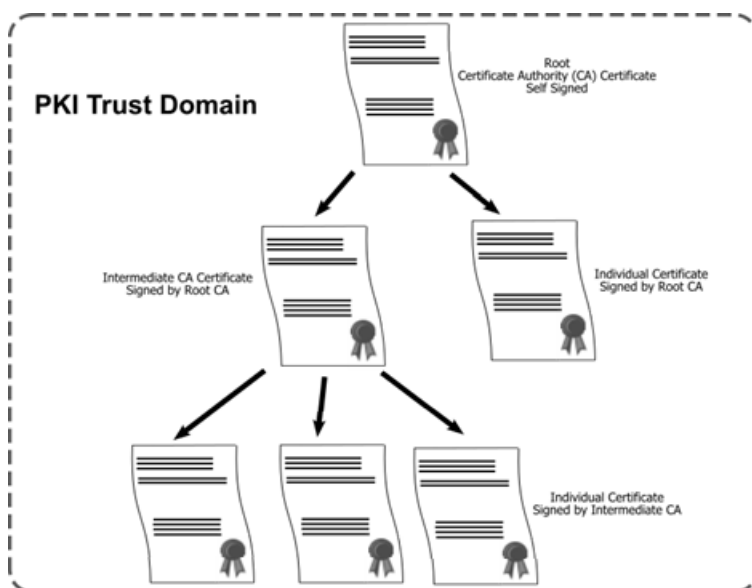
Digital certificates are defined by the X509v3 format and have become the de facto standard for most security operations that involve identity verification. The identity of individuals, systems and applications can be asserted by a certificate with a 'public' key and its corresponding 'private' key. 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. Anyone wishing to check the application can take the certificate and use the public key to unlock the signature and verify:



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):



5.1 Certificate Terminology

Throughout this document the following terms and definitions will be 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 a 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.
- **Trust Store (Trusted Certificate Store):** 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.
- **Single Domain Certificate:** A certificate created for a single server with just one name field/domain (i.e. one identity).
- **Multi Domain Certificate (AKA 'Multi-SAN' or 'Unified Communications' certificate):** A certificate created for a single server with many domains/identities, each identity is one name entry.
- **Wildcard Certificate:** A certificate created for a multiple servers or a single server with many domains/identities. The name entry is of the form '*.exampledomain.com'. Wildcard certificates carry additional security risks. See [Certificate Name Content](#)^[43].

5.1.1 Components of a Certificate

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.

5.1.2 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 now determine that certificates with MD5 and SHA-1 thumbprint algorithms, or public keys of less than 2048 bits are not secure.

5.1.3 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, strength of public key, etc.
- 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 been 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.

5.1.4 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 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 certificate(s). Without such checks TLS can be susceptible to man-in-the-middle attacks.

5.1.5 Certificate File Naming and Format

Like so many other 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 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 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 one certificate, and its associated private key, but can also include other certificates such as the signing certificate(s).
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 PKCS7-----` & `-----END PKCS7-----` statements. It can contain only Certificates & Chain certificates but not the private key. Can be identified by viewing the file in a text editor.

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, care should be taken not to expose any private key. See [Converting Certificate Files](#)^[117] for information on OpenSSL format conversion.

5.2 IP Office Certificate Support

The IP Office platform supports certificates in a number of ways, most of which are configurable via 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-generated by all systems when required.
- Identity certificate can be administered via 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 Primary and Application Server including Subject Alternative Name support.
- The certificate processing can support 1024, 2048 and 4096 bit public RSA keys, and SHA-1, SHA-256 and SHA-512 hashes.
- 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. i.e. 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. i.e. 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 3rd party tool to create a CSR can be used. See [Signing Requests](#)^[11] for more information on how to generate a CSR for IP Office.

5.2.1 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 the Transport Layer Security \(TLS\)](#)^[37].

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

The table in [IP Office Interface Certificate Support](#)^[103] lists all TLS links in the IP Office platform solution and their security capabilities including certificate support.

The table in [IP Office VoIP Endpoint Security](#)^[106] lists VoIP clients in the IP Office platform solution and their security capabilities.

5.2.2 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 hence 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 L = Basking Ridge S = New Jersey C = US E = support@avaya.com	Where: - nnnnnnnnnn is the LAN 1 mac address, e.g. ipoffice-00e00705918e.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	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, 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
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 unique 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/Application Server

The Primary and Application Server have an inbuilt certificate authority. During the ignition process the installer can choose 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
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	

Note 1: The field SubjectName is set according to the following process:

- If Web Manager | Platform | Settings | System | Network | Host Name set to something other than:
 - localhost
 - localhost.localdomain
 - the installer default (mac address)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 hostname 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= SubjectName 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, nonRepudiation, dataEncipherment	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
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	

Note 1: The field SubjectName is set according to the following process:

- If Web Manager | Platform | Settings | System | Network | Host Name is set to something other than:
 - localhost
 - localhost.localdomain
 - the installer default (mac address)
 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-server-00e007057307.avaya.com'
- The correct hostname should be set during ignition, if not the identity certificate will need to be regenerated. This is done automatically if the Web Manager | Platform | Settings | General | Certificates | Renew automatically setting is left at default.

Note 2:

- The correct LAN 1 and LAN 2 address should be set during ignition, if not the identity certificate will need to be regenerated.
- Identity certificate regeneration is done automatically if the Web Manager | Platform | Settings | General | Certificates | Renew automatically setting is left at default.

Server Edition Secondary/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	

5.2.3 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 [IP Office VoIP Endpoint Security](#)^[106] 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 possible future systems connected within the lifetime of the certificate. If in doubt, all possible name entries should be included.

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 used as this field can be displayed to users. The Name field should never be empty.
Example: example.com
- 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. This entry is typically used by web browsers and other clients when accessing IP Office using DNS resolution. When used by SIP endpoints, starting in IP Office release 10.0, this entry typically should have the value configured in Manager | LANx | VoIP | SIP Registrar | SIP Registrar FQDN.
Example: DNS:example.com
- Any other domain name or FQDN of the system as one SAN entry in DNS format. This entry is typically used when the system can be accessed using 'split' DNS.
Example: DNS:ipoffice.example.com
- The IP Address of LAN 1 as one SAN entry in IP format. This entry is typically used by web browsers and other clients when accessing IP Office using the LAN 1 IP Address.
Example: IP:192.168.42.1
- The IP Address of LAN 2 as one SAN entry in IP format. This entry is typically used by web browsers and other clients when accessing IP Office using the LAN 2 IP Address.
Example: IP:192.168.43.1
- Any NAT or public IP Address as one SAN entry in IP format. This entry is typically used by 96x1 H.323 phones in Cloud or Remote Worker deployments, web browsers and other clients when accessing IP Office using the external/public direct IP Address.
Note that this entry is not added by default to identity certificates generated by the IP Office Primary Server CA. This entry is needed if phones or other clients are configured to connect to the IP Office's public IP address and not it's FQDN.
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 | SIP Registrar FQDN. This entry is typically used by SIP endpoints, such as the H175, which verifies the server certificate against the SIP Domain it is registering to.
Example: DNS:sip.example.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 | SIP Registrar FQDN. This entry is typically used by SIP endpoints when accessing IP Office using DNS resolution.
Example: URI:sip:sip.example.com
- Any SIP IP Address in use as one SAN entry for each SIP domain, in URI format. This entry is used by the Avaya E129 SIP endpoint when accessing IP Office using an IP Address.
Example: URI:sip:135.11.53.53
- Under certain circumstances, the use of 'wildcard' names might be considered. A wildcard name field contains an asterisk in the name (e.g. '*.example.com') and covers all sub-domains; this can be useful where there are many separate but related name entries.
IP Office can support such fields in both Subject Name and SAN wildcard name fields, but carry additional security risks and are not recommended. See the notes below.

Notes:

- Many public Certificate Authorities do not support IP address and private domains. DNS and public domains should be used for all clients if a public CA is to be used. Not using IP address can compromise the administration of 96xx, 11xx/12xx and other endpoints.
- Wildcard certificates (or certificates with wildcard name fields) carry the following additional risks:
 - Security: If one server or sub-domain is compromised, all sub-domains may be compromised.
 - Security: If used for more than one server, private key may become exposed.
 - Management: If the wildcard certificate needs to be revoked, all sub-domains will need a new certificate.
 - Compatibility: Wildcard certificates may not work with all server-client configurations.
 - Protection: Wildcard Certificates are not protected by CA extended validation or warranty.

-
- Security: They must not be used to secure more than one IP Office server in a deployment; each server must have a unique identity certificate.

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](#)^[39] 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 or H323 endpoints with secure signalling, SANs will typically be required.

5.2.4 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 (in date) and strength (public key ≥ 1024 bits). This has no value in determining trust.
- **Medium:** The received certificate is checked for validity (in date) and strength (public key ≥ 1024 bits), 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 the public key ≥ 2048 bits, and 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 one is received, certificate checks will be applied. This is the main mechanism used to enforce trust checks by IP Office.

- **Note:** At present, IP Office never requests certificates from SIP or H323 endpoints connecting via TLS.

Mutual authentication is activated with the settings:

- **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 & 411, typically H323 phones, DECT R4, IP Office lines, Voicemail Pro, SysMonitor, etc.
- **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 WebSocket Server Lines

See [IP Office Interface Certificate Support](#) ⁽¹⁰³⁾ for more information.

5.2.5 Certificate Distribution

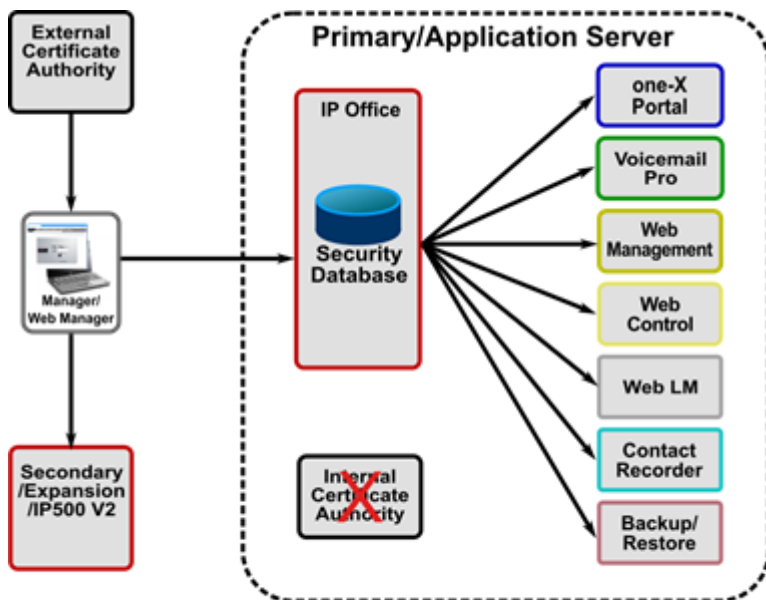
5.2.5.1 Identity Certificate Distribution

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.

Manual from an External CA

A Manual certificate 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:



**Certificate Distribution -
External Certificate Authority**

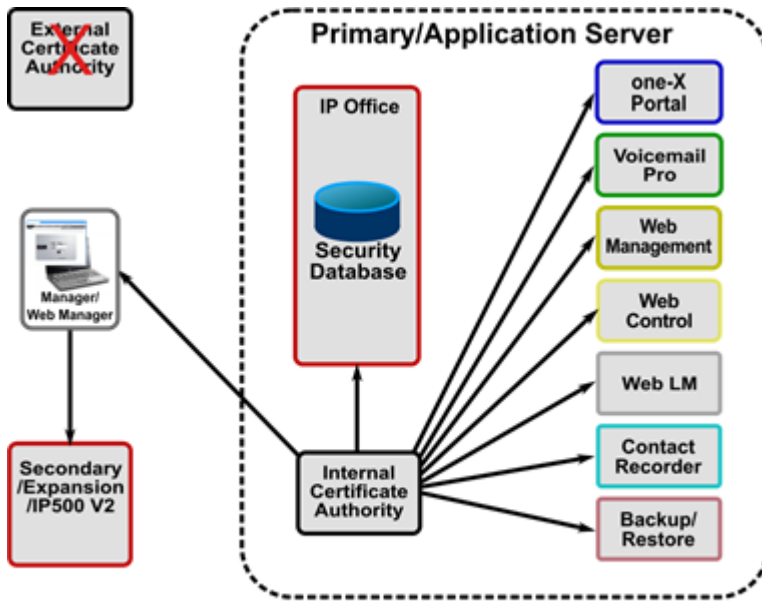
For more information on creation of a PKI based on an External CA, see [Implementing IP Office PKI](#)^[52].

For more information on external Certificate Authorities, see [Certificates from External Certificate Authorities](#)^[54].

Manual from the Primary or Application Server

The internal certificate authority can be used to create a set of unique identity certificates 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



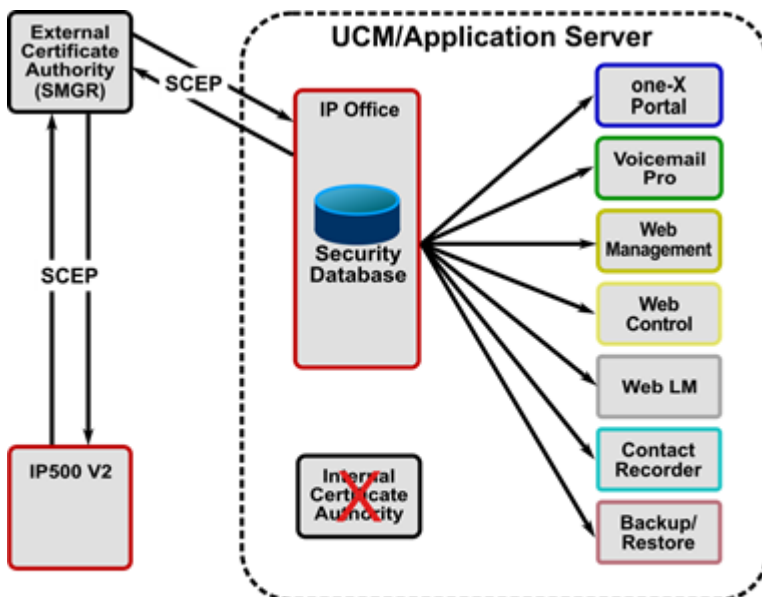
**Certificate Distribution -
Internal Certificate Authority**

For more information on creation of a PKI based on an internal CA, see [Implementing IP Office PKI](#) ⁵².

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).



**Certificate Distribution -
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](#) ⁵².

5.2.5.2 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](#) ⁵².

5.2.5.3 Intermediate CA Certificate Distribution

If the trust implementation additionally uses Intermediate CA certificate(s), 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](#) ⁵².

5.2.6 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**
Document number 18-603853, <https://downloads.avaya.com/css/P8/documents/101004861>
- **Administering Centralized Users for an IP Office™ Platform Enterprise Branch**
Document number 15-604263, <https://downloads.avaya.com/css/P8/documents/101004857>
- **Avaya IP Office™ Platform in a Branch Environment Reference Configuration**
Document number 15-604253, <https://downloads.avaya.com/css/P8/documents/101004855>

When considering a trust policy for IP Office, the following questions can be considered:

- 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, 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 by no means exhaustive, for further information see [Assessing IP Office Security Requirements](#) ⁶⁵.

5.2.7 IP Office PKI Trust Approaches

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

1. PKI Trust domain based on the Primary or Application Server internal root CA.
2. PKI Trust domain based on the Primary or Application Server internal Intermediate CA.
3. PKI Trust domain based on an external Certificate Authority.
4. PKI Trust domain based on an external Certificate Authority via SCEP.
5. No PKI trust domain.

Approach 1: PKI Trust Domain based on Primary or Application Server 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 Primary or Application Server 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.
- Many public certificate authorities will not issue intermediate CA certificates for private domains or IP address ranges.
- 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 3rd parties and therefore does not need to be distributed.

Potential disadvantages include:

- Public certificate authorities will not issue certificates for private domains or IP 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 Avaya Aura System Manager (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 used where a single IP500 V2 or Primary Server has no external/public interfaces and is completely within a secure/closed environment.

Installation/Creation is achieved by retaining the default identity certificate.

No trust relationships are active, 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.

5.2.8 Selecting IP Office PKI

Existing customer security policy may already define the necessary approach. Where this has not yet been defined, an assessment of requirements should help identify the appropriate option. The following guidance may be helpful:

- A deployment with external interfaces and many external clients would suggest an external, public Certificate Authority (Approach 3).
- A deployment with no external interfaces, or few external clients would suggest an internal Certificate Authority (Approach 1).
- A deployment that requires IP Addresses or private domain names in the certificate fields cannot use a public Certificate Authority, therefore Approach 1 may be suitable.
- A deployment that offers any service to the public should use an external, public Certificate Authority (Approach 3).
- A branch deployment with System Manager will typically use SCEP (Approach 4)

Although five approaches are outlined above, a mix may be appropriate; for example external, public CA for public facing servers, internal CA for all others. A hybrid approach cannot be used when VoIP endpoint resilience is active; the root CA for both home and backup server must be the same.

5.2.9 Implementing IP Office PKI

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

Approach 1: PKI Trust Domain based on Primary or Application Server root CA

1. 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.
2. 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](#)^[43] for more information. See [Using the IP Office Certificate Authority](#)^[108].
3. 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)**.
4. Use Web Manager or IP Office Manager to save the CA certificate in each TCS.
5. Use Web Manager or IP Office Manager to save the ID certificate on the relevant IP Office server. See [Update Certificates](#)^[68].
6. If SIP or H.323 phones are using HTTPS for provisioning or TLS for signalling, the IP Office root CA certificate must be present on each phone. See [VoIP Security](#)^[58].
7. 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.
8. Verify that the correct ID certificate has been applied on each device using a browser or other diagnostic tool.
9. Enable certificate checking in the IP Office security settings and IP Office lines.
10. Verify using SE Manager that all IP Office systems are online with no alarms.
11. Enable secure connections for clients.
12. Verify each client can connect successfully.
13. Ensure all ID certificate files are stored securely.
14. Once all checks have been carried out, a configuration backup should be taken.

Approach 2: PKI Trust Domain based on Primary or Application Server Intermediate CA

1. 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.
2. 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](#)^[54].
3. Request an Intermediate CA certificate/private key pair from a trusted Certificate Authority in PKCS#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](#)^[54].
4. Download the root CA certificate (and any further intermediate CA certificates) from the Certificate Authority in PEM and DER format to a local directory.

5. Install Intermediate CA certificate 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**.
6. 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](#)^[43] for more information. See [Using the IP Office Certificate Authority](#)^[108].
7. 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)**.
8. 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.
9. Use Web Manager or IP Office Manager to save the ID certificate on the relevant IP Office server. See [Update Certificates](#)^[68].
10. 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.
11. 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.
12. Once all checks have been carried out, a configuration backup should be taken.

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

1. The CA on the Primary or Application Server is not used; disable the setting **Platform | Settings | General | Certificates | Identity Certificates | Renew automatically**.
2. 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](#)^[54].
3. 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](#)^[43] for more information. For more information on external public authorities, see [Certificates from External Certificate Authorities](#)^[54].
4. Download the root and any intermediate CA certificate from the Certificate Authority in PEM and DER format to a local directory.
5. 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.
6. Use Web Manager or IP Office Manager to save the ID certificate on the relevant IP Office server. See [Update Certificates](#)^[68].
7. 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.
8. 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.
9. Once all checks have been carried out, a configuration backup should be taken.

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

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

5.2.10 Certificates from External Certificate Authorities

An external Certificate Authority (CA) provides a way of obtaining identity certificates that are trusted by 3rd 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-256 identity certificates for web servers? Code signing and other certificate type are not used by IP Office.
- Does the Certificate Authority support a secure web form based Certificate Signing Request (CSR)? If not, external tools are required to provide the CA with a text-based CSR. See [Certificate Signing Requests](#)^[117] 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](#)^[37] for more information on certificate file formats.
 - See [Converting Certificate Files](#)^[117] 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 'wildcard' certificates (certificates with wildcard name fields)?
- 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](#)^[37] 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. Due to their security concerns, Wildcard certificates are not allowed for 'Extended Validation'.
- 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' 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 interoperability with clients; see [Certificate Name Content](#)^[43] for more information.
- The certificate should be RSA2048 bit, with SHA-256 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 3rd 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 [Certificate Signing Requests](#)^[11] 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](#)^[37].

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 [Certificate Signing Requests](#)^[11].

5.2.11 Certificate Maintenance

Regardless of the certificate/trust structure used, all certificates expire and may under exceptional circumstances be compromised. In 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 (the **Renew existing** option).

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 release 10.0 and onwards will raise an alarm – a daily system event in SSA, SNMP, syslog, email – whenever any certificate is within 60 days of expiry.

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 the default values will be 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 setting Web Management Platform | **Settings | General | Certificates | Renew automatically** determines whether the creation and application is automatic due to expiry or change hostname 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 one can be created using Web Management Platform | Settings | General | CA Certificate | Create new. This command must be used with caution as it will create a completely new root CA certificate – it will also require new ID certificates for all entities, and CA certificate distribution to all devices. To keep all existing ID certificates Renew existing should be selected; 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 [Using the IP Office Certificate Authority](#)^[108].

Recovering an ID, CA or TCS Certificate

All certificates are part of the security settings backup/restore process. To recover an ID certificate, the latest backup set should 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 IP Office Manager](#)^[75].

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 workaround may be to remove any IP address entries subject to NAT.

Chapter 6.

VoIP Security

6. VoIP Security

VoIP 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](#)^[80], 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 end to end.

6.1 IP Office Platform Media Security

IP Office support both SRTP and IPsec for VoIP media security. IP Office's IPsec feature can be utilised, 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, H175, 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
- 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	✓	✓	All SRTP settings are per system with a per line and per extension override
	On: Best Effort	✓		
	On: Enforce	✓		
RTP Encryption	Off	✓		
	On: AES128-CTR	✓	✓	
	On: AES128-F8	✗		
RTP Authentication	Off	✓		RTP Authentication should not be disabled
	On: SHA-1/32	✓		
	On: SHA-1/80	✓	✓	SHA-1/80 provides stronger authentication for a small bandwidth increase
RTCP Encryption	Off	✓	✓	
	On: AES128-CTR	✓		Some Avaya and 3rd party endpoints do not support encrypted RTCP
	On: AES128-F8	✗		
RTCP Authentication	On: SHA-1/32	✓		RTCP Authentication always active
	On: SHA-1/80	✓	✓	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 a 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](#).

6.2 VoIP Signalling Security

Securing the signalling of VoIP links is necessary when SRTP is enabled and is a security measure in itself: It should be enabled when the SIP registrar or H323 Gatekeeper is exposed on a public interface, with the other unsecure options disabled.

The security mechanism is dependent upon the type of link:

Link Type	Key Security Mechanism	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-TLS	Supported from R10.0. Additional configuration is required to enable H.323-TLS.
	H.323-Annex H	No additional configuration required This does not secure the complete H.323 signalling channel, just the registration, key exchange and dialled 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](#)^[34].

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 [IP Office VoIP Endpoint Security](#)^[106]. For further details, see the relevant client documentation.

6.3 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 [IP Office VoIP Endpoint Security](#)^[106].

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.

6.4 SRTP Performance & 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 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 SHA1/32: 84.5 kbps	SHA1/80: 86 kbps SHA1/32: 85 kbps	2.4% increase 1.2% increase
G.729	25 kbps	SHA1/80: 26 kbps SHA1/32: 25.5 kbps	SHA1/80: 27 kbps SHA1/32: 26 kbps	8% increase 4% increase
G.722	84 kbps	SHA1/80: 85 kbps SHA1/32: 84.5 kbps	SHA1/80: 86 kbps SHA1/32: 85 kbps	2.4% increase 1.2% increase

6.5 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 [SRTP Troubleshooting](#) ^[102].

6.6 VoIP Security Planning Considerations

Secure media and signalling must be considered whenever VoIP endpoints or IP Office VoIP interfaces transit or are potentially accessible by untrusted networks, including the Internet.

Prior to deploying secure media or signalling using IP Office, the following should be reviewed:

- 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 media or signalling security 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:
 - Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager, Document number 18-603853, <https://downloads.avaya.com/css/P8/documents/101004861>
 - Administering Centralized Users for an IP Office™ Platform Enterprise Branch, Document number 15-604263, <https://downloads.avaya.com/css/P8/documents/101004857>
 - Avaya IP Office™ Platform in a Branch Environment Reference Configuration, Document number 15-604253, <https://downloads.avaya.com/css/P8/documents/101004855>

Chapter 7.

Securing the IP Office Platform Solution

7. Securing the IP Office Platform Solution

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 help 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.

7.1 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 threat.

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
- Update Identity Certificates and PKI
- Secure users and extensions
- Secure trunks/lines
- Secure voice media
- 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

7.2 Assessing IP Office 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 differentiator 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, including for example:

- **US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Risk Management Guide for Information Technology System**
<http://dx.doi.org/10.6028/NIST.SP.800-30r1>
- **UK British Standards Institute (BSI) ISO/IEC 27001, Self-assessment questionnaire**
<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>

7.3 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.

7.4 Change security defaults

All default passwords must be changed to a unique and 'strong' password. See [Password and PIN Management](#)^[28] for more information on password strength.

In IP Office Manager **Security Settings | General** tab:

1. For Security Administrator account:
 - a. Change **Password** to a 'strong' password of 8 or more characters.
 - b. Set **Minimum Password Complexity** to **high**.
2. Change service user account '**Administrator**' password to a 'strong' password of 8 or more characters.
3. 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 (i.e. during customer/ engineering Installation).
4. Change the System, VM Pro and Monitor passwords to 'strong' passwords of 8 or more characters.

7.5 Remove unnecessary 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](#)^[20] for more information on the differing account types and locations.

1. In IP Office Manager | **Security Settings | Service User** tab, remove all unnecessary service user accounts; only retain accounts that are essential. The service user may be deleted or the account status set to Disabled.
2. For all remaining active Service User accounts, change password to a strong one of 8 or more characters. If using Server Edition, see [Securing Server Edition Servers](#)^[82] for alternative Service User administration using Web Manager
3. In **Configuration | Users**: Delete any RAS telephony user accounts (for example 'RemoteManager') that are not required. For any that are required, change the password to a strong one of 8 or more characters.

7.6 Disable Unused Services/Interfaces

All interfaces and services not required must be disabled. Additionally, consider enabling interfaces and services only when required.

1. In IP Office Manager **Security Settings | System | Unsecured Interfaces** tab: 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* TAPI Install**	Also used for legacy applications: IP DECT*, Analog DECT, Conferencing Centre, CRM, MMM * 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 prior 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/S access method.
TAPI	TAPI Link Lite (1st party TAPI) TAPI Link Pro (3rd party TAPI) Avaya Contact Center Select IP Office Contact Center	Enable only when TAPI required; note that TAPI driver installation will fail if the TAPI interface is not active. This setting will affect the IPOCC and ACCS CTI Link; when inactive, any IPOCC and ACCS sessions will require TLS and a trusted certificate from IPOCC/ACCS. This setting will not affect the one-X Portal CTI Link.
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.

7.7 Ensure Minimum Rights of Access

Restrict Service Users' rights of access to the minimum necessary. See [User Accounts and Rights of Access](#) ^[20] for more information on the differing access levels.

1. In IP Office Manager | **Security Settings** | **Rights Groups**, remove all unnecessary access rights; only retain rights that are essential.
2. In IP Office Manager | **Security Settings** | **Service Users** | **Rights Group Membership**, remove all unnecessary rights group membership.
3. If necessary, create new rights groups with minimum access.
4. Rights groups that are defined but not assigned to any Service User do not present a security risk.
5. In IP Office Manager **Security Settings** | **Services** tab: 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
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

6. In IP Office Manager Configuration | System | System tab, 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.

7.8 Enforce a Password Policy

Change the security settings to enforce minimum password complexity, disable service users temporarily and IP Office users permanently on bad logins.

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.

In IP Office Manager Security **Settings | General** tab:

1. Set Service User Details:

- **Minimum Name Length** to 6.
- **Minimum Password Length** to 8.
- **Password Reject Action** to '**Log and Temporary Disable**'.
- **Minimum Password Complexity** to '**Medium**'.
- **Previous Password Limit (Entries)** to 4.

2. Set IP Office User Details:

- **Password Enforcement** to on.
- **Minimum Password Length** to 8.
- **Minimum Password Complexity** to 'Medium'.
- **Password Reject Limit** to 5.
- **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 and PIN Management](#)^[28] for more information.

7.9 Update Certificates

1. It is essential to understand the information and recommendations of [Certificates and Trust](#)^[34] to determine the certificate and trust requirements of the system prior to installation.
2. If required, administer a new platform identity certificate using Manager Security | System | Certificates | Identity Certificate; this identity certificate will be automatically propagated to all TLS/HTTPS interfaces of the server. If an intermediate CA is used to create the identity certificate, the root CA should be placed in the Trusted Certificate Store and then the setting **Security | System | Certificates | Offer ID Certificate Chain** activated. This root CA should also be added to the **system/primary/certificates/tcs/add** directory.
3. If a separate telephony identity certificate is required, it should be administered using Manager security settings.
4. The two default certificates trusted by IP Office should be removed if not required. This is achieved by placing a copy of the certificate in the **system/primary/certificates/tcs/delete** directory using the Manager or Web Manager's File Manager.
Any default certificates to be trusted by IP Office should be added to the **system/primary/certificates/tcs/add** directory. See [Default Trusted Certificates](#)^[97] for more information and how to create the certificate files.
5. 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)**.

7.10 Securing Telephony Users & Extensions

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

1. All unused Users should be deleted – except NoUser.
2. The following auto-create settings must be disabled when not required:
 - **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**
3. If any auto-create feature is used to assist installation, the settings must be deactivated as soon as possible. Note that from 9.1, these settings will automatically be deactivated 24 hours after being set to avoid inadvertent exposure.
4. If no H.323 extensions are supported, the **LAN1/LAN2 | VoIP | H323 Gatekeeper Enable** must be set disabled. If H.323 extensions are supported, only the relevant LAN's gatekeeper should be enabled.
5. If no H.323 remote workers are supported, the **LAN1/LAN2 | VoIP | H323 Gatekeeper | H323 Remote Extn Enable** must be set disabled. If H.323 remote workers are supported, only the relevant LAN's Remote Extn should be enabled.
6. If no SIP extensions are supported, the **LAN1/LAN2 | VoIP | SIP Registrar Enable** must be set disabled. If SIP extensions are supported, only the relevant LAN's registrar should be enabled.
7. If no SIP remote workers are supported, the **LAN1/LAN2 | VoIP | SIP Registrar | SIP Remote Extn Enable** must be set disabled. If SIP remote workers are supported, only the relevant LAN's SIP Remote Extn should be enabled.
8. Enforce a Login Code (PIN) policy for all users and extensions by setting **System | Telephony | Login Code Complexity | Minimum length** to the minimum acceptable length, and activating Complexity tests. For more information on PIN and Login Code security see [Password and PIN Management](#)^[28].
9. All VoIP (SIP, H323, DECT) users' **User | Telephony | Supervisor Settings | Login Code** or **Extension | Extn | Phone Password** must be set.
10. If any SIP registrar or H323 gatekeeper is exposed directly or indirectly to an unsecure network, even via an SBC, the additional steps of [Hardening for Remote Worker Operation](#)^[70] must be followed.
11. All SIP extensions' **Extn | Force Authorisation** setting must be enabled.
12. All auto-created VoIP users must have their **User | Telephony | Supervisor Settings | Login Code** changed from the default. All auto-created non-VoIP (Digital, Analog) users should have their name and extension changed from the default.
13. Each user should have only the necessary **User | User | Profile** features enabled, all others disabled.
14. Each user should have only the minimum necessary **User | Web Self-Administration** interface features enabled, all others disabled. Web Self-Administration is a new feature from R9.1 and disabled by default. Each tab of the Web Self-Administration page may be controlled for view and edit on a per-user basis:

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)

15. For IP Office release 8.1 and prior, disable all **User | Phone Manager Options** unless required. This can be achieved via the application of User Rights (User Rights | Phone Manager).
16. If different from the system-wide setting, change the **Extn | VoIP | Media Security** setting. See [VoIP Security](#)^[58].

-
- 17.If the VoIP extension is to be 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](#)^[34].

7.11 Hardening for Remote Worker Operation

Whenever SIP or H323 remote worker operation is supported, or if any SIP registrar or H323 gatekeeper is exposed directly or indirectly to an unsecure network even via an SBC, 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.

- 1.The RTP port range on the LAN interface must be set to no more than 50750. If more RTP ports are required, the minimum value may be changed.

- **LAN1/LAN2 | VoIP | Port Number Range | Maximum**

- **LAN1/LAN2 | VoIP | Port Number Range (NAT) | Maximum**

- 2.Any exposed SIP Registrar or H323 Gatekeeper should have the TLS option enforced and any unsecure options disabled. See [VoIP Security](#)^[58]. To reduce the overhead of security and certificate management, one LAN's registrar can be used for the external interface, the other LAN for internal extensions.
- 3.The SIP registrar ports should be changed from the default 5060/5061
- 4.Any settings file supplied by IP Office must be conveyed via HTTPS not HTTP. This will additionally require certificate administration; see [Certificates and Trust](#)^[34].
- 5.SRTP for media security should be considered, see [VoIP Security](#)^[58].
- 6.If any H323 Gatekeeper is exposed directly or indirectly to an unsecure network, all H323 remote worker's **Extension | Extn | Phone Password** must be set. The code must not be a sequence, repeated digits, or same as the extension number. It must not be less than 9 digits, preferably 13 digits. For R8.1 and prior, the setting **User | Telephony | Supervisor Settings | Login Code** can be used.
- 7.Each H323 remote worker extension's **Extension | VoIP | IP Address** should be set to the public IP Address of the phone.
 - **Note:** This cannot be used if more than one phone is behind the same firewall/NAT, or the remote IP address changes.
- 8.If any SIP registrar is exposed directly or indirectly to an unsecure network, ALL SIP extensions must have default users who's Login Codes are not less than 9 digits, preferably 13 digits.
- 9.If any SIP registrar is exposed, ALL SIP extension's **Extension | VoIP | IP Address** should be set to the IP Address of the phone.
 - **Note:** The SIP extension must have a static IP address.
- 10.The steps of [Securing Telephony Users & Extensions](#)^[69] must be followed.
- 11.The steps of [Preventing Unwanted Calls](#)^[72] must be followed.
- 12.A Session Border Controller (SBC) must 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 Border Controller for IP Office Remote Workers" in "Administering Avaya IP Office Platform™ with Manager".

7.12 Securing Trunks/Lines

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.

1. If using SIP trunks, IP Office must be connected externally via a properly configured Firewall; see [Limiting IP Network Exposure](#)^[80] for more information. IP Office must never be connected directly.
2. Unless SIP trunks are configured for a particular LAN interface, the **LAN1/LAN2 | VoIP | SIP Trunk Enable** setting must be disabled.
3. 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: <http://www.avaya.com/usa/product/avaya-session-border-controller-for-enterprise>.
4. Off-switch forwards/transfers should be disabled on a per-system or per-user basis, with the system setting taking precedence over the user.
 - Per-user setting is: **User | Telephony | Supervisor Settings | Inhibit Off-Switch Forward/Transfer**. This can also be set via User Rights.
 - System-wide setting is: **System | Telephony | Telephony | Inhibit Off-Switch Forward/Transfer**.
5. Analog trunks-to-trunk forwards/transfers should be disabled on a per-line basis unless required, using **Line | Analog Options | Analog Trunk to Trunk Connection**.
6. Other changes to restrict calls are contained in [Preventing Unwanted Calls](#)^[72].
7. IP Office Lines (AKA 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. The Primary and Secondary should always be the WebSocket server.
 - For the **High** setting, certificate configuration is required; see [Certificates and Trust](#)^[34] for more information.
8. For Server Edition deployments, secure IP Office Lines should always be used.

7.13 Secure Voice Media

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

- **Note:** 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 Security](#)^[58]. This should be reviewed prior to enabling any IP Office VoIP media security.

7.14 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.

- **Note:** It is strongly recommended that all IP Office deployments be protected from unwanted calls regardless of the perceived risk.

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 and monitoring
- 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
- Correct error handling in Voicemail Pro call flows.

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
Feature	Barred	Barred

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 Caller ID presentation, (*67(US)/141(UK) to Withhold Caller ID, *82(US)/1470(UK) to present Caller ID) 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 config, and can be part of user rights templates, centralises the routing/barring config, and 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 un-restricted, in real operation it is unlikely that there will be totally un-restricted out-dialling.

The Default system short code for dialling is Unchanged:

The screenshot shows a configuration window titled '9N: Dial'. It has a 'Short Code' tab selected. Below the tab are five fields: 'Code' with the value '9N', 'Feature' with a dropdown menu showing 'Dial', 'Telephone Number' with the value 'N', and 'Line Group ID' with a dropdown menu showing '50: Main'.

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 Users of the phones but people who have physical access to the phone but you don't want them to use phones. There are several mechanisms that can be used to 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 will leave 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 force a User to be logged out if their phone is idle for a period of time.

- **Out of Hours Call Routing**

A time profile can be associated to an ARS so that when the time Profile is inactive a different ARS is used for routing calls - for our example above we will 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**

Where a phone is in an un-controlled area it is also 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. Since release 5.0 it has been 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 **Personal Options 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 unauthorised access.

SMDR Reporting of Barred Calls

To enable the detection of unauthorized call attempts, the string 'SMDR' can be included in the telephone field of the Barred short code. When included, an SMDR report will be generated with the relevant field indicating the calling party, call destination etc. The call will be zero duration, zero ring time, with the word 'Barred' in the 2nd party info field.

Error Handling in Voicemail Pro Call Flows

All call flows that can make internal or external calls, transfers or other potential call operations must ensure only the expected call destinations from valid users are allowed. All possible invalid operations should be detected and prevented by the use of call flow logic.

7.15 Securing CTI Interfaces

1. If not required, disable TAPI Link Lite/Pro (1st /3rd party TAPI) as per [Disable Unused Services/Interfaces](#)^[66].
2. To secure the link between ACCS or IPOCC and IP Office, the setting IP Office Manager | **Security Settings** | **System** | **Unsecured Interfaces** | **TAPI** should be disabled. This will enable TLS and request a trusted certificate from IPOCC/ACCS.
3. Administer IPOCC/ACCS with an identity certificate. See the relevant IPOCC/ACCS documentation.
4. Administer the IP Office Trusted Certificate Store (TCS) with the root CA certificate of the IPOCC/ACCS.

7.16 Securing IP Office Manager

1. Apply the following configuration settings on the Manager **File** | **Preferences** | **Security** tab to ensure more secure IP Office communications and help 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

2. 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.
3. For more information see [Certificates and Trust](#)^[34] and [Windows Certificate Management](#)^[99].
4. 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 [Windows Certificate Management](#)^[99]. 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.
5. 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.
6. In IP Office Manager's **File** | **Preferences** | **Directories** tab, change the **Working Directory (.cfg Files)** to be different to 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.
7. Ensure all offline configuration files, exported files or other configuration data are controlled.

7.17 Securing Web Manager/Web Control

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

1. 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](#)^[34].
2. Ensure all offline configuration files, exported files or other configuration data are controlled.

7.18 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.

1. Change the password of the default account as soon as possible.
2. All passwords must be 'strong' and of 8 or more characters (See [Password and PIN Management](#)^[28]). Any unused accounts must be deleted.
3. 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](#)^[34].

7.19 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.

1. 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.
2. 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.
3. 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.
4. 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.

7.20 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	Enabled	Disabled	Disabled
Enabled	Enabled	Enabled	Enabled	Enabled

1. 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 Administrative Users and Rights Groups](#)^[22].
2. 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.
3. 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](#)^[34].
4. 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.
5. 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.

7.21 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 threat or privacy issue.

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

7.22 Securing Voicemail Pro

1. Using the Voicemail Pro client, the password for the default administration account 'Administrator' must be changed to a 'strong' password of 8 or more characters. Any unused accounts must be deleted.
 - **Note:** For Voicemail Pro R9.0 and higher on Server Edition, UCM and Application Server, all authentication is referred 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. See [User Accounts and Rights of Access](#) [20] for more information.
2. Using the Voicemail Pro client, configure the password used to access the IP Office in **Administration | Preferences | General | Voicemail Password**. This password must match the password entered in the Manager setting **Security | System | Unsecured Interfaces | Voicemail Password**. The password should be 'strong' and 8 or more characters.
3. The IP Office configuration setting **System | Voicemail | Voicemail IP Address** must not be left at 255.255.255.255, but set to the IP Address of the Voicemail Pro server.
4. 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 feature.
 - **Note:** Disabling the mailbox will also disable IMAP, MAPI, email and Web Voicemail integrations for that user
5. All mailboxes must be protected by password/Voicemail Code access, except when connecting from trusted extensions (by the use of the **User | Source Numbers** field). The recommended minimum is 4 digits for internal use, 9 when the mailbox can be accessed externally.
6. The mailbox password/Voicemail Code policy should be enforced by setting the voicemail Default Telephony Interface to Intuity in the Voicemail Pro client, and minimum PIN Length to 4 or 9 using the Manager setting **System | Voicemail | Voicemail Code Complexity**.
 - **Note:** If IP Office voicemail TUI is used, the users are not forced to set a new password/Voicemail Code on initial mailbox access.
7. To prevent Toll fraud via the outdialling feature, it can be disabled on the IP Office Configuration **System | Voicemail** tab in IP Office Manager. Where Outcalling is required, the call barring steps of [Preventing Unwanted Calls](#) [72] must be used.
8. To prevent Toll fraud via call flows, all call flows must have adequate protection against dialling unauthorized numbers. Where external calling is required, the call barring steps of [Preventing Unwanted Calls](#) [72] must be used.
9. Where 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.
10. Disable all unused services such as SMTP and MAPI.
11. If the SMTP send feature is used, TLS and authentication should be used.
12. If the IMAP4 server feature is used, TLS should be used.
13. If the host server operating system is Microsoft Windows, consult the relevant Microsoft OS security guidelines, which can be found at <https://technet.microsoft.com/en-us/library/windows-server-security.aspx>. More general information can be found at <https://technet.microsoft.com/en-us/security/default.aspx>

7.23 Securing Embedded Voicemail

1. Only users and groups that are entitled to use voicemail should have their mailbox activated.
2. All mailboxes must be protected by password/Voicemail Code access, except when connecting from trusted extensions (by the use of the **User | Source Numbers** field). The recommended minimum is 4 digits for internal use, 9 when the mailbox can be accessed externally.
3. The mailbox password/Voicemail Code policy should be enforced by setting the **System | Voicemail | Voicemail Mode** to **Intuity Mode**, and minimum PIN Length to 4 or 9 using the Manager setting **System | Voicemail | Voicemail Code Complexity**.
 - **Note:** If IP Office voicemail TUI is used, the users are not forced to set a new password/Voicemail Code on initial mailbox access.
4. Where 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.

7.24 Securing Contact Recorder

1. Contact Recorder gives full administrator rights to the first access of the web administration page, therefore it is important to configure the name and password as soon as possible. See the section General Setup > Recorder in Administering Avaya IP Office™ Platform Contact Recorder.
2. All passwords must be 'strong' and of 8 or more characters (See [Password and PIN Management](#)^[28]). Any unused accounts must be deleted.
3. The unsecure administrative interface (HTTP) should be disabled using the web admin interface and set **System | Manage Users | Allow unencrypted (http) access** to **No**. See the section "General Setup > Recorder" in Administering Avaya IP Office™ Platform Contact Recorder.
4. The Advanced Security section of the Contact Store documentation should be reviewed, however the changing of Contact Recorder ports is not recommended.
5. Note: Contact Recorder does not support referred authentication; local user accounts are used at all times.

7.25 Securing one-X Portal

1. Log in to the default one-X Portal Administrator account and 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](#)^[20] for more information.
2. For subsequent password management, go to the one-X Portal **Configuration | Users** page. Any unused administrator accounts must be deleted.
3. 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 EnhTcpservice.
4. If one-X Portal clients are to be used externally, follow [Hardening for Remote Worker Operation](#)^[70].
5. If external one-X Portal clients are configured to support VoIP calls, follow [Limiting IP Network Exposure](#)^[80].
6. 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)**.
7. To administer an Identity Certificate for the HTTPS interfaces of Linux-based one-X Portal servers see [Update Certificates](#)^[68].
8. 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.
9. Log in to the default Superuser backup and restore account and change the password to a strong password of 8 or more characters. For subsequent password management, go to the one-X Portal AFA page **Configuration | Edit** page.
10. If the host server operating system is Microsoft Windows, consult the relevant Microsoft OS security guidelines, which can be found at <https://technet.microsoft.com/en-us/library/windows-server-security.aspx>. More general information can be found at <https://technet.microsoft.com/en-us/security/default.aspx>

7.26 Securing Web License Manager (WebLM)

- Log in to the default WebLM account and change the password to a strong password of 8 or more characters.
- For subsequent password management, go to the WebLM Manager Users page. Any unused administrator accounts must be deleted.
 - **Note:** WebLM does not support referred authentication; local user accounts are used at all times.

7.27 Securing Avaya Contact Center Applications

1. Whenever IP Office Contact Centre (IPOCC) and Avaya Contact Center Select (ACCS) are deployed with IP Office, the CTI link between IP Office and the application should be secured according to [Securing CTI Interfaces](#)^[72].
2. Please refer to the relevant application documentation for all other security aspects:
 - Avaya IP Office Contact Center Feature Description
 - Avaya Contact Center Select Solution Description

7.28 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 the following 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 (e.g. VPN, MPLS). It 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 should be inspected for any gateway routes that may have been unintentionally acquired via DHCP. These should be deleted if not required and the DHCP settings modified 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:

<http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf> provides background information, including other helpful resources.

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 and SIP inspection should be turned off as this will interfere with IP Office operation.

Session Border Controller

The Avaya SBCE is recommended to be located behind the Enterprise firewall, and serves as a security and demarcation device between the IP-PBX and the Carrier facility. Avaya also supports an implementation of the Avaya SBCE parallel to the firewall, although it is better as 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

Both System Status Application and SysMonitor access to IP Office can be secured, and events/alarms sent to syslog servers (including the IP Office Primary Server) using the TLS protocol.

IP Office SNMP should not be used without additional security measures such as Virtual Private Network (VPN).

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

For IP Office deployment in an enterprise or branch environment, Avaya's Secure Access Link (SAL) gateway can be utilised.

7.29 Secure 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 System Status Application and SysMonitor access to IP Office can be secured. See [Securing System Status Application](#)^[76] and [Securing Sys Monitor](#)^[76].

SNMP should not be used as this is not secure.

- **Note:** 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 this instance local monitoring via unsecured interfaces or external secure solution are required. See [Limiting IP Network Exposure](#)^[80].

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

7.30 Restricting Physical Access

Any unauthorized physical access to the system could present attackers with an opportunity to reset the configuration and security settings, modify BIOS, access the unsecure serial port, install or modify software via the SD Card or other mechanisms.

It is essential to secure physical access to the IP Office platform; mechanisms of controlling such access outside the scope of this document.

7.31 Securing Server Edition Servers

1. It is important to understand the information and recommendations of [Certificates and Trust](#)^[34] to determine the certificate and trust requirements of the server as options are offered during the initial ignition process.
2. 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).
3. 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.
4. 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**.
5. Apply a password policy to the Web Control application using Web Manager Platform **Settings | System | Password Rules Settings**.
6. 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.
7. Disable the HTTP backup/restore server using Web Manager setting **Platform | Settings | System | HTTP Server**. From R9.1, an HTTPS backup/restore server is always active for this purpose.
8. 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](#)^[80].
9. 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.
10. 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>.

11. If not required, disable the syslog receiver on the **Primary Settings | General** tab.
12. 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.
13. If not required, disable the Access Security Gateway (ASG) support using the Web Manager setting **Platform | Settings | ASG Settings | Status**.
14. 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](#)^[34].
15. Follow [Securing the IP Office Platform Solution](#)^[64].
 - a. If Voicemail Pro is installed, follow [Securing Voicemail Pro](#)^[77].
 - b. If Contact Recorder is installed, follow [Securing Contact Recorder](#)^[78].
 - c. If one-X Portal is installed, follow [Securing one-X Portal](#)^[78].
16. Do not activate the server's Intelligent Platform Management Interface (IPMI) – this effectively grants physical access to the server.

7.32 Securing Application Server/UCM

The Application Server and Unified Communications Module (UCM) run a 'Management' IP Office instance. A management IP Office 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.

1. It is important to understand the information and recommendations of [Certificates and Trust](#)^[34] to determine the certificate and trust requirements of the server as options are offered during the initial ignition process.
2. 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).
3. Apply a password policy to the Web Control application using **Settings | System | Password Rules Settings**.
4. Enable the setting **Settings | System | Authentication | Enable referred authentication**. This will refer all Web Control logins to the management IP Office. The local Linux Administrator account credentials are only used under failure conditions.
5. 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.
6. Follow [Securing the IP Office Platform Solution](#)^[64].
7. Disable the HTTP backup/restore server using **Settings | System | HTTP Server**. From R9.1, an HTTPS backup/restore server is always active for this purpose.
8. 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](#)^[80].
9. If not required, disable the Access Security Gateway (ASG) support using the Web Manager setting **Platform | Settings | ASG Settings | Status**.
10. 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](#)^[34].
11. 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](#)^[34].
12. If Voicemail Pro is installed, follow [Securing Voicemail Pro](#)^[77].
13. If Contact Recorder is installed, follow [Securing Contact Recorder](#)^[78].
14. If one-X Portal is installed, follow [Securing one-X Portal](#)^[78].
15. Do not activate the server's Intelligent Platform Management Interface (IPMI) – this effectively grants physical access to the server.

Chapter 8.

Monitoring the IP Office Platform

8. Monitoring the 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](#) ⁸⁹.
- 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' in SMDR reports
 - The syslog tag of 'IPTables-Rejected' 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

8.1 Checks and Tests

Thorough checks and tests should be carried out to ensure the deployment is secure and no previous attacks have compromised the system:

- Note: Care must be taken not to inadvertently expose sensitive data as a by-product of testing activities.
- Check LAN1/LAN2 do not have public IP addresses i.e. directly accessible from the internet.
- Check the IP Office for unsecure internet or inbound IP access by identifying the public IP address of the Firewall (e.g. by using <http://whatismyipaddress.com>), then attempting access to the IP Office ports defined by the Port Matrix document. The following table contains some example ports that should be tested.

Note: This port list is not exhaustive and can vary from release to release. A link to the port matrix document is located on the Avaya Product Security page at <https://support.avaya.com/security>.

Port	Protocol	Use	Possible test Tool	Notes
22	TCP	SSH	SSH, Nmap or other port scanner	Linux servers only
69	UDP	TFTP	Nmap or other port scanner	A TFTP RRQ of 'nasystem/who_is' can be used
80	TCP	HTTP	Browser, Nmap or other port scanner	http://[IP Address] can be used
143	TCP	IMAP	Nmap or other port scanner	Voicemail Pro only
161	UDP	SNMP	SNMP test tool, Nmap or other port scanner	
411	TCP	HTTP	Nmap or other port scanner	
443	TCP	HTTPS	Browser, Nmap or other port scanner	https://[IP Address] can be used
993	TCP	IMAP-TLS	Nmap or other port scanner	Voicemail Pro only
1300	TCP	H323-TLS	Nmap or other port scanner	
1720	TCP	H323	Nmap or other port scanner	
5060	UDP	SIP	Nmap or other port scanner	
5061	TCP	SIP	Nmap or other port scanner	
5443	TCP	HTTPS	Nmap or other port scanner	Linux servers only
7070	TCP	HTTPS	Browser, Nmap or other port scanner	Linux servers only https://[IP Address]:7070 can be used
7071	TCP	HTTPS	Browser, Nmap or other port scanner	Linux servers only https://[IP Address]:7071 can be used
8000	TCP	HTTP	Nmap or other port scanner	Linux servers only
8069	TCP	HTTP	Nmap or other port scanner	one-X Portal only
8080	TCP	HTTP	Browser, Nmap or other port scanner	https://[IP Address]:8080/onexportal-admin.html can be used
8086	TCP	HTTP	Nmap or other port scanner	one-X Portal only
8411	TCP	HTTPS	Nmap or other port scanner	
8443	TCP	HTTPS	Nmap or other port scanner	
9443	TCP	HTTPS	Nmap or other port scanner	one-X Portal only
50791	TCP		VMPro Client, Nmap or other port scanner	
50792	UDP		Nmap or other port scanner	
50793	TCP		Nmap or other port scanner	IP500 V2 only
50794	UDP + TCP	SysMonit or	SysMonitor, Nmap or other port scanner	
50796	TCP	TLS	Nmap or other port scanner	
50804	TCP		IP Office Manager, Nmap or other port scanner	
50805	TCP	TLS	IP Office Manager, Nmap or other port scanner	
50808	TCP		SSA, Nmap or other port scanner	
50809	TCP	TLS	SSA, Nmap or other port scanner	
50812	TCP		IP Office Manager, Nmap or other port scanner	

Port	Protocol	Use	Possible test Tool	Notes
50813	TCP	TLS	IP Office Manager, Nmap or other port scanner	
50814	TCP		Nmap or other port scanner	

If access is successful, it can indicate a misconfigured Firewall or other network protection system.

- Attempt to log into the servers using the set of default administrator accounts and passwords in the following table.
- Note: Default accounts from previous releases are not removed on upgrade.

Default Account Name	Domain	Possible test Tool	Notes
security Administrator Manager Operator BusinessPartner Maintainer IPDECTService SMGRB5800Admin BranchAdmin	IP Office	Web Manager IP Office Manager	All servers, including IP500 V2 and UCM
Administrator	Voicemail Pro	VMPro client	Voicemail Pro only
Administrator	one-X Portal	Browser	one-X Portal only
Administrator	Web Control	Browser	Linux servers only
root	Linux	Console interface	Linux servers only

If access is successful, the account credentials should be changed or the account removed. See [Remove unnecessary accounts](#)^[65] for more information on account removal

- 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 and review all warnings; none should be present.
- Log on to one-X Portal administration page, if a warning is displayed 'Change Administrator Default Password' the administrator account is at default.
- For R9.0+, if login to Web Control, one-X Portal or Voicemail pro fails unexpectedly, check the IP Office security settings for the account being used; it must have a rights group assigned which contains the correct 'External' rights.
- Check successful and failed logins produce the expected reports and results.
- Test the call barring, emergency calls, authorisation codes, Voicemail Pro outcalling and call flows. 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.

8.2 Activating Reporting

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, blacklisted IP Addresses, 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 more 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.
 - The file 'IP_Office_Alarms_N_N_N.xlsx' contained on the IP Office Admin DVD.
- Audit trail of administrative logins, their source and result. Available as syslog events, also displayable in SSA and Manager. NOTE that user/phone based changes are not currently captured. For more 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.
- Detailed audit trail of all administrative changes, including security settings. Available as syslog events only.
- 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 more information see: "Voicemail Pro Syslog" in Administering Avaya IP Office™ Platform Voicemail Pro. By default for Server Edition, all events are active and send via syslog to the Primary.
- Voicemail box login failures are reported via the IP Office failed login alarms, see above.

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 of administrative logins. Available as syslog events only. By default for Server Edition, all events are active and send via syslog to the Primary.
- one-X client login failures are reported via the IP Office failed login alarms, see the IP Office section above.

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 where they can be stored, viewed and forwarded to external syslog servers. For more information see **Logs | Syslog Event Viewer** and **Settings | General | Syslog** in the Web Control application.

Other Components

- Firewall intrusion detection and reporting should be activated.
- SBC intrusion detection and reporting should be activated.
- Call logger unusual call activity detection and reporting should be activated.

Avaya Security Advisories and IP Office Updates

1. Register for Avaya Security Advisory notifications by using the E-Notification subscription procedures. See [Avaya Product Security Support](#)^[92].
2. 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>.

8.3 Response to Incidents

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

- Attacked/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 [Avaya Product Security Support](#)^[92] 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. In addition the IP address or subnet can be blocked by the firewall.
- 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>.

Chapter 9.

Appendices

9. Appendices

9.1 Appendix A - Avaya Product Security Support

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 security at 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 susceptibility of Avaya products to those vulnerabilities and assigns one of four risk levels: High, Medium, Low, and None (see [Interpreting an Avaya Security Advisory](#)^[94]). 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.

9.1.1 Accessing Avaya Security Advisories

Avaya Security Advisories are posted on the Security Support web site at <http://support.avaya.com/security>. Customers can register at 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
Medium	Within 2 weeks
Low	Within 30 days
None	At the discretion of Avaya

To sign up to receive advisories by email on the Avaya Security Support website:

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 receiving notification when new and updated Security Advisories are available.

9.1.2 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 at <https://support.avaya.com/css/P8/documents/100066674>.

The following table summarizes the three main categories:

Vulnerability classification	Criteria for classification
High	<p>A product's risk to a particular vulnerability is categorized as HIGH if the following criteria are met:</p> <ul style="list-style-type: none">• 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. <p>OR</p> <ul style="list-style-type: none">• 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. <p>For example, see the advisory at http://support.avaya.com/css/P8/documents/100062710.</p>
Medium	<p>A product's risk to a particular vulnerability is categorized as MEDIUM if no higher criteria are met, but the risk does meet the following criteria:</p> <ul style="list-style-type: none">• 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. <p>OR</p> <ul style="list-style-type: none">• 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. <p>OR</p> <ul style="list-style-type: none">• An exploit can be performed which allows a local user account to escalate privileges. <p>For example, see the advisory at http://support.avaya.com/css/P8/documents/100064239.</p>
Low	<p>A product's risk to a particular vulnerability is categorized as LOW if no higher criteria are met, but the risk does meet the following criteria:</p> <ul style="list-style-type: none">• 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. <p>OR</p> <ul style="list-style-type: none">• An exploit can be performed which causes non-critical applications to shutdown, reboot, or become unusable <p>For example, see the advisory at http://support.avaya.com/css/P8/documents/100064944.</p>
None	<p>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 package(s), module(s), or configuration(s) are not utilized on an Avaya product.</p> <p>For example, see the advisory at http://support.avaya.com/css/P8/documents/100064240.</p>

9.1.3 Organization of an Advisory

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.

9.1.4 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	<p>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).</p> <p>If a software patch is available, recommended actions will be described in the Avaya Security Advisory.</p> <p>Any recommended actions which can be pursued by the customer will be included in the Avaya Security Advisory when it is issued.</p>
Medium	<p>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).</p> <p>If a software patch is available, recommended actions will be described in the Avaya Security Advisory.</p> <p>Any recommended actions which can be pursued by the customer will be included in the Avaya Security Advisory when it is issued.</p>
Low	<p>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).</p> <p>If a software patch is available, recommended actions will be described in the Avaya Security Advisory.</p> <p>Any recommended actions which can be pursued by the customer will be included in the Avaya Security Advisory when it is issued.</p>
None	No remedial actions will be required.

9.2 Appendix B - Default Trusted Certificates

There are three certificates that are trusted by IP Office and are present on initial default and security settings 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.
Symantec Class 3 Secure Server CA – G4	30 October 2023 23:59:59	ff67367c5cd4de4ae18bcce1d70fdabd7c866135	A Symantec 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 and should not be used in production systems

VeriSign Class 3 International Server CA – G3 in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGTCCBRGgAwIBAgIQZBvoIM4CCBPzLU0tldZ+ZzANBgkqhkiG9w0BAQUFADCB
yJELMAkGA1UEBhMCVVMxZzAVBgNVBAAoTD1Zlcm1TaWduLCBjbmuMR8wHQYDVQQL
ExZWZlbnBiUcnVzdCB0ZXN3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBwZXJp
U2lnbiwgSW5jLiAtIEZvciBhdXR0b3JpemVkIHVzZSBvbm5MUUwQwYDVQQDEzW
ZXJpU2lnbiBDbGFzcyAzIFB1Ym9yYyBQcm1tYXJ5J5IENlcnRpZmljYXRpb24gQXV0
aG9yaXR5IC0gRzUwHhcnMTAwMjA4MDAwMDAwHhcnMTAwMjA3MjMlOTU5WjCBvDEL
MAkGA1UEBhMCVVMxZzAVBgNVBAAoTD1Zlcm1TaWduLCBjbmuMR8wHQYDVQQLExZW
ZXJpU2lnbiBDbGFzcyAzIFB1Ym9yYyBQcm1tYXJ5J5IENlcnRpZmljYXRpb24gQXV0
aHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYykgMDEMDQGA1UEAxMtVmVya
aVNPZ24gQ2xhc3MgMyBjb2Nrcm1tYXJ5IFNlcnZlcjB0QSA0IEc3MIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmDACyAV9IGaQQhZjxOdF8mfUdza
sVLv/+NB3eDfxcJg4615HycQmLi7IJfBKERBD+qpgFLPTU4bi7u1xHbZzFYG7rNV
ICreFY1xy1TibxfNiQDk3P/hwB9ocenHKS5+vDv85burJlSLZpDN9pK5MSSAvJ5s
1fx+0uFLjNxc+kRLX/gYtS4w9D0SmNNiBXNUPpyiHb5SgzoHRSQ7AlYhv/JRT9Cm
mTnprqU/iZucff5NYAcIIPe712mDK4KTQzfZg0EbwurSmaET0q03n40mY5o1so5
BptMs5pITRNGtFghBMT7oE2sLktiEuP7TfbJUQABH/weaoEqOOC5T9YtrQIDAQAB
o4ICF7TCCAhEwEgYDVR0TAQH/BAgwBgEB/wIBADBwBgNVHSAEATBnMGUGC2CGSAGG
+EUBBxcDMFYwKAYIKwYBBQUHAQEWHGh0dHBzOi8vd3d3LnZlcm1zaWduLmNvbS9j
cHMwKgYIKwYBBQUHAQIwHhocaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYTA0
BgNVHQ8BAf8EBAMCAQYwBQYIKwYBBQUHAQEWEYTBf0V2gWzBZMFcwVRYJaW1hZ2Uv
Z2lmMCEwHhZAHBgUrDgMCGGUj+XTGoasjY5rw8+AatrIGCx7GS4wJRYjaHR0cDov
L2xvZ28udmVyaXNpZ24uY29tL3ZzbG9nb3Y5naWYwNAYDVR0lBC0wKwYIKwYBBQUH
AwEGCCsGAQUFBwMCAgglghkgBhvhCBAAEGCmCGSAGG+EUBCAEWNAIKwYBBQUHAQEE
KDAmMCQGCCsGAQUFBzABhhodHRwOi8vb2Nzc5Z2ZXJpc2lnbi5jb20wNAYDVR0f
BC0wKzApoCegJYYjaHR0cDovL2Nybc5Z2ZXJpc2lnbi5jb20vcGNhMy1nNS5jcmww
KAYDVR0RBCEwH6QdMBsxGTAXBgNVBAMTEFZlcm1TaWduTVBLSS0yLTcwHQYDVRO0
BBYEFNeBfNgioBX33a1fzimbWMO8RgC1MB8GA1UdIwQYMBaAFH/TZafC3ey78DAJ
80M5+gKvMzEzMA0GCSqGSIb3DQEBBQUAA4IBAQBxtX1zUkrd1000Ky6v1Ea1SVAC
T/gvF3DyE9wfIYaqwk98NzzURniuXXhv0bpavBCrWDbFjGIVRWAXIELVQqh3oVXY
QwRR9m66SOZdTLdE0z6klDyZmp8N5td0lksVWmzWoxZTDphDzqS4w2Z6BVxiEOgb
EttLznZQ/9/XaxvMisxx+rNAVnwzeneUW/ULU/sOX7xo+68q7jA3eRaTJX9NEP9X
+79u0ZMh3nnchhdZLUNkt6Zmh+q8lkYZGoaLb9e3SQBb260/KZru99MzrqP0nkzK
XmnUG623kHdq2FlveasB+1XwiiFm5WVu/XzT3x7rfj8GkPsZC9MGAht4Q5mo
-----END CERTIFICATE-----
```

Symantec Class 3 Secure Server CA - G4 in PEM format:

-----BEGIN CERTIFICATE-----

```
MIIFODCCBCCgAwIBAgIQUT+5dDhwtzRAQY0wkwaZ/zANBgkqhkiG9w0BAQsFADCB
yJELMAkGA1UEBhMCVVMxZzFzAVBgNVBAoTDlZlcm1TaWduLCBjbmuMR8wHQYDVQQL
ExZWZlXJpU2lnbiBUCnVzZCB0ZXRR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBwZXJp
U2lnbiBwSW5jLiAtIEZvcjBhdXR0b3JpemVkIHVzZSBvbm90b3R5YXN0YXN0YXN0
ZXJpU2lnbiBDbGFzcyAzIFB1Ym9pYyBQcm1tYXJ5IENlcnRpZmljYXRpb24gQXV0
aG9yaXR5IC0gRzUwHhcnMTMxMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMD
CQYDVQGEwJVUzEdMBsGA1UEChMUU3ltYW50ZWMMGQ29ycG9yYXRpb24xH2AdBgNV
BAsTF1N5bWVudGVjIFRydXN0IE51dHdvcmsxLzAtBgNVBAMTJ1N5bWVudGVjIENs
YXNzIDMgU2VjZDZlIFNlcnZlcjBDQSA0IENlcnRpZmljYXRpb24xH2AdBgNV
AQ8AMIIBCGKCAQEAstgFyhx0LbUXVjnFSlIjLuhL2AzxaJ+aQihw6UwU35VEYJb
A3oNL+F5BMm0lncZgQGUWfm893qZJ4Itt4PdWid/sgN6nFMl6UgfRk/InSn4vn1W
9vf92Tpo2otLgJNBESPIPMzWlnqEIROIbAMnF4scaGGTDw5RgDMdtLX0637QYqzu
s3sBdO9pNevK1T2p7peYyo2qRA4lmUoVlqTObQJUHypqJuIGOmNlrLRM0XWTUP8T
L9ba4cYY9Z/JJV3zAdReJk20KQnNDz0jbxZKGRb78oMQw7jW2FUYpFG9D72MUPVK
Fpd6UiFjds8W+cRmvvW1CdJ/JwDNRHxvSz+w9wIDAQAB04IBYzCCAV8wEgYDVR0T
AQH/BAGwBgEB/wIBADAwBgNVHR8EKTAnMCWgI6Ahhh9odHRwOi8vczEu3ltY2Iu
Y29tL3BjYTMtZzUuY3J5MA4GA1UdDwEB/wQEAwIBBjAvBggrBgEFBQcBAQJjMCEw
HwYIKwYBBQUHMAIGE2h0dHA6Ly9zMj5zeW1jYi5jb20wawYDVR0BGQYwYjBgBgpg
hkgBhvFAQc2MFIwJgYIKwYBBQUHAGEWGmh0dHA6Ly93d3cuc3ltYXV0aC5jb20v
Y3BzMCgGCCsGAQUFBwICBWA6Gmh0dHA6Ly93d3cuc3ltYXV0aC5jb20vcnBhMCKG
A1UdEQQIMCCkHjAcMR0wGAYDVQQDExFTEW1hbnRlY1BLSS0xLTUzNDAdBgNVHQ4E
FgQUX2DPYZBV34RDFIpGKrL1evRDG08wHwYDVR0jBBgwFoAUF9Nlp8Ld7LvwMANz
Qzn6Aq8zMTMwDQYJKoZIhvcNAQELBQADggEBAF6UVkndji1l9cE2UbYD49qecny
HlmrWH5sJgUs+oHXXCMXiW3k/eG7IXmsKP9H+IyqEVv4dn7ua/ScKAYQmW/hP4W
Ko8/xabWo5N9Q+10IzElKPRj6S7t9/Vcf0uatSDpCr3gRRAMFJSaXaXjS5HoJtG
QGx0InLnmfiIEfXzf+YzguaoxX7+0AjiJVgIcWjmaLmFN5OUiQt/ev5E1PnXi8t
TRttQBVSKEHiXgSgW7ZTaoteNtCLD0IX4eRnh8OsN4wUmSGiaqdZpwOdgyA8nTY
Kvi4Os7Xlg8RvmurFPW9QaAiY4nxug9vKWNmLT+sJHLf+8fk1A/y00+MKcc=
```

-----END CERTIFICATE-----

SIP Product Certificate Authority in PEM format:

-----BEGIN CERTIFICATE-----

```
MIIEntTCA4WgAwIBAgIBADANBgkqhkiG9w0BAQUFADB6MQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEgEgMCgGA1UECmMhU0lQIFByb2RlY3QgQ2VydGlm
aWNhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVjdCBBDXJ0aWZpY2F0
ZSBBDXR0b3JpdHkwHhcnMTMxMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
CQYDVQGEwJVUzETMBEGA1UEChMKQXZheWEgSW5jLjEgEgMCgGA1UECmMhU0lQIFBy
b2RlY3QgQ2VydGlmYWVhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVj
dCBBDXJ0aWZpY2F0ZSBBDXR0b3JpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC0OytYx7YRzT7VYJov8FGe6g1GJ0h+4Y7YZzzmgHPqpgn+2jluQilN
NHlmlLbYLnrvf6s3+X/zh7ZND2tyrKZMCYai8FX6X3tYTONZ9ErTYngSJCpLeCu
c+qgt1SmRsyal+1F9i5jvrFxoOuRb5N05Yv3cI85SFLw7kEr41cQDvshRBWZfo6r
f3bBJj1qRTHc5yGbXXeEs+JrtIveECFB2Q/w3Eg/GbcWGHPluqHgQPH76aNMyyQP
GMzDBtpCfGh7HkD7jkt2El+AiBKJy0cOcj22+AKbLvh5bfffJMTcCPX2Bax2CD2I1
usQ+osTG+FdvuhRBx+WPqBOWsQ0wRKGNAgMBAAGjggESMIIBKDA/BgNVHSAEODA2
MDQGC2CGSAGG/ASHAgEBMCUwIwYIKwYBBQUHAGEWf21haWx0bzpzaXBjYUBhdmF5
YS5jb207MB0GA1UdDgQWBBSgggpcXDqgxcm4PcMduQZVE75WKjASBgNVHRMBAf8E
CDAGAQH/AgEBMAsGA1UdDwQEAwIBBjCBpAYDVR0jBIGcMIGZgBSgggpcXDqgxcm4
PcMduQZVE75WKqF+pHwweJELMAkGA1UEBhMCVVMxZzFzAVBgNVBAoTCkF2YXlhIElu
Yy4xKjAoBgNVBAsTIFN1JUCBQcm9kdWN0IENlcnRpZmljYXRlIEF1dGhvcml0eTEq
MCgGA1UEAxMhU0lQIFByb2RlY3QgQ2VydGlmYWVhdGUgQXV0aG9yaXR5ggEAMA0G
CSqGSIb3DQEBBQUAA4IBAQBGPraSto+++KAFMtUSGvm4jsbknWwazR5yFxlTWrgo
osMN+1t351AEJed1DCvUWibbfSylh13PNzYLhSiImKPR98LVQ4P5126C2suJPaye
EUX87wDCHe8eNNG93v154U4aQDum98FSTR1YjdSiL9R3trKLOiiY1LBE1oJHBGPi
FzRXgc0XVGWXMfAqunQ01pzKqu7ET09AWsYbUS4c+J5tdYk9nYk35Y1WtKwOz8MS
gwkB2ncy1rI6IuWvLAUdd9BKcBYGLSMVulVGj130i0V35xxNoyIKQ98RPIb9RcME
zhiIkhUoktmeYHe9BYn8En76q5oXh0CAIQ0ld9Vood/
```

-----END CERTIFICATE-----

To remove that default trust a file can be used with the IP Office Trusted Certificate Store delete feature:

- Create a text file with an extension '.pem', open and copy the above PEM data including the 'BEGIN CERTIFICATE' and 'END CERTIFICATE' lines. The line termination can be Windows or Linux.
- One .pem, file per certificate
- Using the IP Office or Web Manager File Manager feature, copy the file to the **system/primary/certificates/tcs/delete** directory
- Restart IP Office

To add a default trusted certificate, the above steps can be followed, 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](#)^[34] for more information on certificate file formats.

9.3 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:

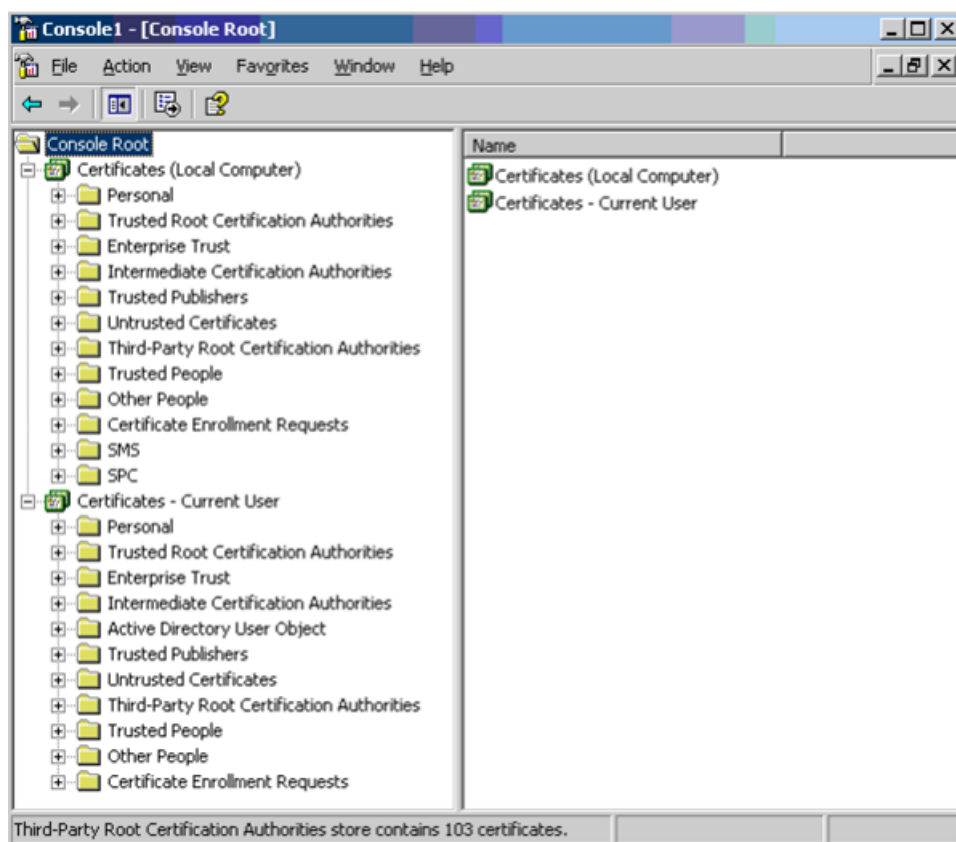
- IP Office SoftConsole – uses a local certificate file
- Firefox Browser – uses its own internal certificate store
- Java Runtime environment 1.6, 1.7 and 1.8 – uses its own internal certificate store
- one-X Portal for Windows server – uses a local certificate file

- **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.

9.3.1 Windows Certificate Store Organization

By default, certificates are stored in the following structure:



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 and other Windows applications only access some of the certificate sub folders:

Certificates (Local Computer) Folder	Usage
Personal Certificates	<p>Folder searched by Manager and some Web Browsers 1st for a certificate to send to the IP Office when requested.</p> <p>Certificate matched by the subject name contained in File Preferences Security Certificate offered to the system.</p> <p>Folder accessed whenever 'Local Machine certificate store' used for Security Settings.</p> <p>Folder searched by Manager for matching certificate when certificate received from the system, and File Preferences Security Manager Certificate Checks = Medium or High.</p>
Trusted Root Certification Authorities Certificates	<p>Folder searched by Manager for matching root CA certificate when non-self-signed certificate received from IP Office, and File Preferences Security Manager Certificate Checks = Medium or High.</p> <p>Folder searched by some browsers and other applications for matching root CA certificate when a certificate received from IP Office.</p>

Certificates - Current User Folder	Usage
Personal Certificates	<p>Folder searched by Manager 2nd for a certificate to send to the IP Office when requested. Certificate matched by the subject name contained in File Preferences Security Certificate offered to the system.</p> <p>Folder accessed whenever 'Current User certificate store' used for Security Settings.</p> <p>Folder searched by Manager for matching certificate when certificate received from IP Office, and File Preferences Security Manager Certificate Checks = Medium or High.</p>
Trusted Root Certification Authorities Certificates	<p>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.</p> <p>This folder is not used by non-Microsoft applications such as Chrome or Safari browsers – the corresponding Local Computer folder is used.</p>
Other People Certificates	<p>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.</p> <p>This folder is not used by non-Microsoft applications such as Chrome or Safari browsers – the corresponding Local Computer folder is used.</p>

9.3.2 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 imported certificate is to trust the IP Office, the Trusted Root Certification Authorities folder should be used, and the certificate imported should be the root CA certificate.
- If the certificate is to subsequently identify the Manager, the Personal folder should be used, and the associated private key saved as well.

9.3.3 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.

9.3.4 Certificates Console

The Windows Certificates Console is a Microsoft Management Console (MMC) snap-in that can be used to manage the Windows certificate store including viewing, importing and exporting.

For more information on the Certificates Console, see:

<http://social.technet.microsoft.com/wiki/contents/articles/2167.how-to-use-the-certificates-console.aspx>

9.4 Appendix D- SRTP Troubleshooting

9.4.1 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 **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.

9.4.2 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**.

9.5 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 which can be found 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	✓	Tel	Bi	✓	
SM Line	SIP-TLS	✓	Tel	Bi	✓	
SIP Extension	SIP-TLS	✓	Tel	Cli	✗	See IP Office VoIP Endpoint Security 1001 for more details.
H323 Extension – signalling	H323-TLS	✓	Man	Cli	n/a	TLS option from R10.0 onwards See IP Office VoIP Endpoint Security 1001 for more details.
H323 Extension – provisioning	HTTPS	✓	Man	Bi	✓	See IP Office VoIP Endpoint Security 1001 for more details.
DECT R4 Provisioning	HTTPS	✓	Man	Bi	✓	See IP Office VoIP Endpoint Security 1001 for more details.
D100 Provisioning	HTTP	✗	n/a	n/a	n/a	
IP Office Line	HTTPS	✓	Man	Bi	✓	WebSocket
IP Office Manager – Security	TLS	✓	Man	Bi	✓	Manager and SE Manager
IP Office Manager – Configuration	TLS	✓	Man	Bi	✓	Manager and SE Manager
SoftConsole	HTTPS	✓	Man	IPO	✓	WebSocket
SSA	TLS	✓	Man	IPO	✗	
Web Manager (single)	HTTPS	✓	Man	Bi	✓	Web Manager single instance management over port 8443
Web Manager (solution)	HTTPS	✓	Man	Cli	✗	Web Manager Server Edition management over port 7070
System Directory	HTTPS	✓	Man	Bi	✓	Central external directory feature
one-X Portal CTI	TCP	✗	n/a	n/a	n/a	
IPOCC CTI	TLS	✓	Man	Srv	✓	IP Office is the server
ACCS CTI	TLS	✓	Man	Srv	✓	IP Office is the server
one-X Portal Directory	HTTPS	✓	Man	Srv	✓	IP Office is the server
Voicemail Pro	HTTPS	✓	Man	Srv	✓	IP Office is the server
Backup/Restore client	HTTPS	✓	Man	Cli	✓	
SysMonitor	HTTPS	✓	Man	Srv	✓	IP Office is the server
Voicemail Pro						
one-X Portal status	TCP	✗	n/a	n/a	n/a	Message Status
one-X Portal VM play	HTTPS	✓	Man	✗	✗	
Exchange WS client	HTTPS	✓	Man	Srv	n/a	
SFTP Client	SSHv2	✓				Exporting voicemail and recording data
one-X Portal						
one-XP Browser/ Call Assistant	HTTPS	✓	Man ⁴	Cli	✗	
Outlook, Salesforce, Lync Plugin	HTTPS	✓	Man ⁴	Cli	✗	

Link	Protocol	Cert Support	ID Cert Offered ¹	Cert Trust Checks ²	Cert check Control ³	Notes
one-X Mobile Android	HTTPS	✓	Man ⁴	Cli	✗	See IP Office VoIP Endpoint Security ^[106] for more details.
one-X Mobile iOS	XMPP-TLS	✓	Man ⁴	Cli	✗	See IP Office VoIP Endpoint Security ^[106] for more details.
Communicator Windows	HTTPS	✓	Man ⁴	Cli	✗	See IP Office VoIP Endpoint Security ^[106] for more details.
Communicator iOS	XMPP-TLS	✓	Man ⁴	Cli	✗	See IP Office VoIP Endpoint Security ^[106] for more details.
Linux Server						
Backup/Restore server	HTTPS	✓	Man	Cli	✗	
Web Control	HTTPS	✓	Man	Cli	✗	
SSH Server	SSHv2	✓				
SFTP Server	SSHv2	✓				
WebLM Server						
Web Admin	HTTPS	✓	Man	Cli	✗	WebLM is the server
Contact Recorder						
Web Admin	HTTPS	✓	Man	Cli	✗	Contact Recorder is the server

Notes:

1. Type of ID certificate presented:
 - **Tel** – Telephony or Management (configurable).
 - **Man** – Management certificate.
2. Support and direction of certificate trust checks:
 - **Bi** – Mutual certificate checks can be enabled.
 - **Svr** – Only the server can check certificates.
 - **Cli** – Only the client can check certificates.
3. The color indicates the grouping for the certificate check controls on the IP Office server component:

Color	Control	Notes
✓	Manager Security: System Certificates Received Certificate Checks (Telephony)	Any setting other than None will request a client certificate See Certificate Check Controls ^[45] for further information.
✓	Manager Security: System Services HTTP Service Security Level Manager Security: System Certificates Received Certificate Checks (Management)	See Certificate Check Controls ^[45] for further information.
✓	Manager Configuration: Line Line Security	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
✓	Manager Security: System Services Security Administration Service Security Level Manager Security: System Certificates Received Certificate Checks (Management)	See Certificate Check Controls ^[45] for further information.
✓	Manager Security: System Services Configuration Service Security Level Manager Security: System Certificates Received Certificate Checks (Management)	See Certificate Check Controls ^[45] for further information.
✓	Manager Security: System Services Web Services Service Security Level Manager Security: System Certificates Received Certificate Checks (Management)	See Certificate Check Controls ^[45] for further information.
✓	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 See Certificate Check Controls ^[45] for further information.

Color	Control	Notes
	Manager Security: System Unsecured Interfaces TAPI = unchecked	IP Office will check the ACCS or IPOCC server certificate against the TCS as per a setting of Medium See Certificate Check Controls ⁴⁵ for further information.

4. one-X Portal for Windows uses a separately administered ID certificate

9.6 Appendix F - IP Office VoIP Endpoint Security

The following table provides an overview of the 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]
Avaya H.323 Endpoint								
96x1	✓	✓ or partial [2]	✓	✓ [10]	n/a	✓	✓	DNS.1: FQDN of IP Office IP.1: IP address of IP Office LAN1 IP.2: IP address of IP Office LAN2 IP.3: Public IP Address if remote
96x0	✗	✗	✓	✓	n/a	✓	✓	✗
16xx	✗	✗	✗	✓	n/a	✓	✓	✗
DECT R4	✗	✗	✓	✓	n/a	✓	✓	✗
IP Office [3]	✓	✓	✓	n/a	n/a	✓	✓	✗
Voicemail Pro [4]	✗	✗	✓	n/a	n/a	✗	✗	✗
Avaya SIP Endpoint								
96x15	✓	✓	✓	✗	✓	✓	✓	✗
11xx/12xx [9]	✓ [11]	✓	✓	✓	✗	✓	✓	IP.1: IP address of IP Office LAN1 IP.2: IP address of IP Office LAN2 IP.3: Public IP Address if remote
B179	✓ [11]	✓	✓	✓	✓	✓	✓	✗
E129	✓	✓	✓	✓	✓	✓	✓	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
H175	✓ [11]	✓	✓	✓ [10]	✓	✓	✓	DNS.1: FQDN of IP Office IP.1: IP address of IP Office LAN1 IP.2: IP address of IP Office LAN2
E159	✗	✗	✗	✓	✗	✗	✗	✗
E169	✗	✗	✗	✓	✗	✗	✗	✗
Radvision XT series	✓	✓	n/a	✗	✓ [6]	✓	✓	DNS.1: FQDN of IP Office IP.1: IP address of IP Office LAN1 IP.2: IP address of IP Office LAN2
Communicator iPad [12]	✓	✓	n/a	✗	✓ [6]	✓	✗	✗
Communicator Windows [12]	✓	✓	n/a	✗	✓ [6]	✓	✗	✗
one-X Mobile iOS	✓	✓	n/a	✗	✓ [6]	✓	✗	✗
one-X Mobile Android	✓	✓	n/a	✗	✗	✓	✗	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
D100 SIP DECT	✗	✗	✗	✓	✗	✗	✗	✗
IP Office Softphone (Mac)	✗	✗	✓	✓	✗	✓	✗	✗

Notes:

1. Ability for the phone to remotely download settings and configuration in a secure manner, typically via HTTPS.
2. When H323-TLS is not used, signalling is not fully secured, but registration, 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 may request a certificate for any HTTPS transfer according to the **Mutual Authentication** setting; see See [Certificate Check Controls](#)^[46] for further information..
8. This column indicates whether the client requires Subject Alternative Name support within the received identity certificate from IP Office.
Typically if DNS is used, the VoIP Endpoint only requires the FQDN of the IP Office in the SAN and no IP Address. IP Addresses and private domain names are not supported by public Certificate Authorities.
9. 11xx/12xx series phones do not support FQDNs and hence cannot be used with certificates provided by public Certificate Authorities.
10. The IP Office root CA certificate can be provisioned to the phone automatically by IP Office using the auto-generated settings file. See the Endpoint Configuration chapter of Deploying OnAvaya™ and Powered by Avaya IP Office and IP Office Contact Center For Business Partners for more information.
11. Direct media is disabled when SRTP is enabled.
12. Client does not fully support TLSv1.2; when one-X Portal admin setting 'TLS v1.2 clients only' is active, Communicator for Windows will not connect, Communicator for iPad will operate, but without XMPP presence.

9.7 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.

The CA feature can be accessed via Web Manager Platform | Settings | Certificates | Identity Certificates.

9.7.1 Generating the CA Server's Own Identity Certificate

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 hostname is changed. To prevent automatic regeneration, the Web Management setting **Platform | Settings | Certificates | Identity Certificates | Renew automatically** should be unchecked.

To manually create an identity certificate for the CA server:

1. Uncheck the setting **Platform | Settings | Certificates | Identity Certificates | Create certificate for a different machine**.
2. Enter a unique subject name if the default offered is not acceptable. See [Certificate Name Content](#)^[43] for more information.
3. Enter the subject alternative names if the default offered is not acceptable. See [Certificate Name Content](#)^[43] for more information.
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:example.com, IP:192.168.0.45, IP:192.168.1.45, IP:135.64.113.102, DNS:example.sip.com, URI:sip:example.sip.com, URI:192.168.0.45, URI:192.168.1.45, URI:sip:192.168.0.45
4. 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.
5. Enter the Public Key Algorithm. This should be RSA-2048.
6. Enter the Secure Hash Algorithm. This should be SHA-256.
7. Check the settings and then click **Generate and Apply**. This will cause the server to generate and apply the new certificate during which service loss will occur.

9.7.2 Generating Identity Certificates for Other Devices

To manually create an identity certificate for another device:

1. Check the setting **Platform | Settings | Certificates | Identity Certificates | Create certificate for a different machine**.
2. Enter the Machine IP. This is used to create the file name, but not the certificate itself; an IPv4 address of that device should be entered.
3. Enter the Password; this is used to secure the identity certificate file and must conform to the complexity requirements.
4. Enter a unique subject name for the device. See [Certificate Name Content](#)^[43] for more information.
5. Enter any subject alternative names. See [Certificate Name Content](#)^[43] for more information.
6. 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.
7. Enter the Public Key Algorithm. This should be RSA-2048 for all IP Office devices. RSA-1024 should only be used for legacy systems that cannot support RSA-2048.
8. 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.
9. Check the settings and then click Generate. This will cause the server to generate a PKCS#12 file containing the identity certificate, private key and signing certificate. The file is secured by the password entered and will be requested every time the file is opened.
10. A popup will prompt to save the file. Save the file to the local machine. Once the popup is close, the file will be deleted on the CA server.
11. The PKCS#12 file can now be imported into the IP Office deployment. See the relevant documentation and [Implementing IP Office PKI](#)^[52] for more information.
 - For one-X Portal Windows this is achieved via the one-X Portal admin web page.
 - For VMPro Windows the file is imported into IIS.
 - For IP Office and Linux servers use Web Manager.

9.7.3 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.

To export the CA certificate in PEM format:

1. Select **Platform | Settings | Certificates | CA Certificates | Download (PEM –encoded)**.
2. A popup will prompt to save the file which is named '**root-ca.pem**'. Save the file to the local machine for later distribution.

To export the CA certificate in DER format:

1. Select **Platform | Settings | Certificates | CA Certificates | Download (DER–encoded)**.
2. A popup will prompt to save the file which is named '**root-ca.crt**'. Save the file to the local machine for later distribution.

9.7.4 Renewing/Replacing the Signing Certificate

To create a new signing certificate:

1. Select **Platform | Settings | General | CA Certificate | Create new**.
2. This will create a completely new root CA certificate and will also require new ID certificates for all entities. The previous signing certificate will be deleted.

To keep all existing ID certificates but refresh the signing certificate:

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.

1. Select **Platform | Settings | General | CA Certificate | Renew existing**.
2. This will create a new certificate with the same content and public/private keys, but a different serial number and start/end date.
3. Only this new root CA requires distribution, in-date existing ID certificates signed by the previous CA will still be valid.

To replace the existing signing certificate:

1. Select **Platform | Settings | General | CA Certificate | Import**.
2. The format must be PKCS#12.
3. This will replace the signing certificate and may require new ID certificates for all entities

To back-up the signing certificate:

1. Select **Platform | Settings | General | CA Certificate | Export**.
2. A password is requested to secure the PKCS#12 file
3. A popup will prompt to save the file which is named '**root-ca-p12**'. Save the file to the local machine and add a '**.p12**' extension.

To restore the signing certificate:

1. Select **Platform | Settings | General | CA Certificate | Import**.

9.8 Appendix H - 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](#) ^[112]
- [OpenSSL Package](#) ^[113]

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 are procedures for converting certificate files.

9.8.1 Creating a CSR using Microsoft MMC Certificates Snap-in

9.8.1.1 Create the CSR

1. 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.
2. 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 active on any machine interface by default.
3. All steps must be carefully followed to avoid errors.
4. Further information on the snap-in and certificate operations can be found at:
<https://technet.microsoft.com/en-us/library/cc771157.aspx>
5. Ensure all naming information has been identified (Common name, Alternate subject names, organization details etc.)
6. You must be logged in and run the console session as administrator.
7. To open the Microsoft Management Console (MMC):
 - a. Click **Start**.
 - b. In the Search box, type **mmc**.
 - c. Click **mmc.exe**.
8. Click **File > Add/Remove Snap-in**.
9. Click **Certificates > Add > OK**.
10. Select **Computer Account** and click **Next**.
11. Select **Local Computer** and click **Finish** then **OK**.
12. Expand **Certificates (Local Computer)**.
13. Right-click **Personal**, then click **Select All Tasks > Advanced Operations > Create Custom Request**.
14. Click **Next**.
15. Select **Proceed without enrolment policy** and click **Next**.
16. Select **(No Template) Legacy Key**.
17. Select **PKCS #10** and click **Next**.
18. In the Certificate Information section, click arrow button next to **Details** and click **Properties**.
19. On the **General** tab, type the domain name of the certificate in the **Friendly Name** field.
20. On the **Subject** tab, in the **Subject Name** field, enter the information below, clicking **Add** after entering each type:

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 ; 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

21. Any entries not required (for example Organizational Unit Name) or not requested by the CA should not be added.
22. 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

Type	Value	Notes
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

23. On the Extension tab, select **Key usage**.
24. Select **Non repudiation**, **Digital signature**, **Key encipherment**, **Data encipherment**, clicking **Add** after entering each option.
25. Unselect **Make these key usages critical**.
26. On the Extension tab, select **Extended Key Usage**.
27. Select **Server Authentication**, **Client Authentication**, clicking **Add** after entering each option.
28. Unselect **Make the Extended Key Usage critical**.
29. On the **Private Key** tab, select **Cryptographic Service Provider**, select **Microsoft Strong Cryptographic Provider (Encryption)** only.
30. On the Private Key tab, select **Key type**, select **Exchange**.
31. On the Private Key tab, select **Key options > Key size**, and set the value to **2048**.
32. Select **Make Private Key Exportable**. Note: This step is important.
33. If presented, select **Select Hash Algorithm**, select **Hash Algorithm** and set the value to **sha256**.
34. Review all entries; check the **Key options > Key size**, is still set to the value to **2048**.
35. Click **OK** then **Next**.
36. Enter the filename (e.g. yourdomain) and location to save the CSR to. Ensure **Base 64** is selected. Click **Finish**.
37. Open the CSR file yourdomain.req in a text editor and copy all of the text, including the start and end lines.
38. 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-256 should be selected for the hash algorithm. SHA-1 should not be used.

9.8.1.2 Download and Import the Signed Identity Certificate

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
2. The root certificate should be downloaded in PEM and DER format and put aside for later distribution to IP Office systems.
3. Copy all to the original CSR directory.
4. See [Certificate File Naming and Format](#) ^[37] for more information on certificate file formats.
5. On the same server the certificate request was created on, open the MMC Certificates snap-in for the Local Computer account.
6. Expand **Certificates (Local Computer)**.
7. Right-click **Personal**, then click **Select All Tasks > Import**.
8. Click **Next**.
9. Browse and select the signed identity certificate received from the CA, then click Open.
10. Ensure that these options are always selected:
 - **Mark the Private Key Exportable**
 - **Import all Extended Properties**
 - **Import all Certificates in the Chain**
11. Click **Next**.
12. Select **Place all certificates in the following store**. Under **Certificate Store**, make sure **Personal** is selected. and click **Next**.
13. Complete the Certificate Import Wizard and click **Finish**.

-
14. Check there is a key icon on the new certificate, if not the private key is not present.
 15. 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.
 16. Select the identity certificate and click **Open**, select **Details** and verify the content are as expected. Select **Certification Path** and verify all the certificates are present to the root certificate.

9.8.1.3 Export the Signed Identity Certificate

1. 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.
2. On the same server the certificate request was created on, open the MMC Certificates snap-in for the Local Computer account.
3. Expand **Certificates (Local Computer)**.
4. Right-click the identity certificate (the one with the key icon), then click **Select All Tasks > Export**, click **Next**.
5. Select **Yes, export the private key**, click **Next**.
6. Select: **Personal Information Exchange - PKCS #12 (.PFX)**, **Export all Extended Properties**, and **Include all Certificates in the certification path if possible**.
7. When prompted, a strong password should be used to secure the file. This password will be requested when later importing into IP Office.
8. Click **Next**.
9. Enter a filename (e.g. yourdomain) and then click **Next**, then **Finish**. The ID certificate file `yourdomain.pfx` should be renamed `yourdomain.p12`.
10. The PKCS#12 file `yourdomain.p12` now has the identity certificate, private key and all intermediate certificates.
11. `yourdomain.p12` can now be imported into the IP Office deployment; for one-X Portal Windows this is achieved via the one-X Portal admin web page. For VMPro Windows the file is imported into IIS. For IP Office and Linux servers use IP Office or Web Manager. See the relevant documentation and [Implementing IP Office PKI](#)^[52] for more information.
12. The `yourdomain.p12`, root and intermediate certificate files should be retained and used for recovery purposes.
 - **Note:** A password will always be required to open the PKCS#12 file.

9.8.2 Creating a CSR using the OpenSSL Package

9.8.2.1 Create the CSR

1. OpenSSL package is a third-party product and Avaya cannot provide assurance or warranty of purpose in any form.
2. 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.
3. All steps must be carefully followed to avoid errors.
4. 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.
5. Ensure all naming information has been identified (Common name, Alternate subject names, organization details etc.)
6. You must be logged in and run the console session as administrator.
7. Create a directory for the CSR and key and change to it.
8. Create a text file openssl.cfg with the following content, ensure no additional line breaks:

```
[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
URI.3 = sip:135.11.53.53
```

9. The items in red must be replaced with the information specific to the CSR. Ensure that the information requested by the CA is supplied accurately.
10. The Country Name is a 2 letter code defined by <https://www.iso.org/obp/ui/#home>; select Country codes, and click Search.
11. Any entries not required (for example Organizational Unit Name) or not requested by the CA can be removed by removing the whole line.
12. If the certificate is for a single domain, remove all lines from subjectAltName = @alt_names and onwards.
13. 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).
14. Create the CSR and private key using the command line, ensuring no line breaks. The items in red should be replaced with the domain name of the device.

```
openssl req -new -out example.csr -newkey rsa:2048 -sha256 -keyout example.key -config openssl.cfg
```
15. When requested ('Enter PEM pass phrase'), a strong password for the private key file should be entered. This will be requested later when combining the signed certificate.
16. Verify the CSR with the command line:

```
openssl req -text -noout -verify -in example.csr
```
17. Check the output is as expected.
18. Open the CSR file example.csr in a text editor and copy all of the text
19. Go to the CA and follow 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, SHA-256 should be selected for the hash algorithm. SHA-1 should not be selected.
20. Keep the example.key file for later use. Note a password will always be required to open the key file.

9.8.2.2 Download and Combine the Signed Identity Certificate

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 PEM format
 - Zero, one or more intermediate certificates which need to be in PEM format
2. If there are download options, selecting 'Other' or 'Apache' should provide the correct format.
3. Copy all to the original CSR directory. Rename the identity certificate to the domain name with a .crt extension.
4. The root certificate should be downloaded in PEM and DER format and put aside for later distribution to IP Office systems.
5. If there is more than one intermediate certificate file: In the original CSR directory , combine all the intermediate certificate files into one file using the single command line:

```
cat intermediate1.crt intermediate2.crt intermediate3.crt > intermediates.crt
```
6. In the original CSR directory , join the files into a single PKCS#12 file along with the intermediate certificate file using the single command line:

```
openssl pkcs12 -export -in example.crt -certfile intermediates.crt -inkey example.key -out example.p12
```
7. When prompted ('Enter pass phrase for example.key '), the password used to secure the private key file when creating the CSR should be entered.
8. When prompted ('Enter Export Password '), a strong password should be used to secure the output PKCS#12 file. This password will be requested when later importing into IP Office.
9. Review the PKCS#12 with the command line: `openssl pkcs12 -info -in example.p12`
10. The identity certificate, private key and all intermediates should be present.
11. The ID certificate file example.p12 and intermediates.crt can now be imported into the IP Office deployment. See the relevant documentation and [Implementing IP Office PKI](#)^[52] for more information.
 - For one-X Portal Windows this is achieved via the one-X Portal admin web page.
 - For VMPro Windows the file is imported into IIS.
 - For IP Office and Linux servers use IP Office or Web Manager.
12. The example.key, example.p12, root and intermediate certificate files should be retained and used for recovery purposes.
 - **Note:** A password will always be required to open the PKCS#12 and key file.

9.8.3 Converting Certificate Files

The intermediate.crt file can be in PEM or DER format; it is PEM format if viewable using a text editor.

If other formats are required OpenSSL can be used:

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
```

To convert PKCS#7 to PEM:

```
openssl pkcs7 -print_certs -in certificate.pb7 -out certificate.pem
```

To convert PKCS#7 and private key to PKCS#12:

```
openssl pkcs7 -print_certs -in certificate.pb7 -out certificate.pem
```

```
openssl pkcs12 -export -in certificate.pem -inkey privateKey.key -certificate.pfx -certfile CAcert.cer
```

See [Certificate File Naming and Format](#)^[37] for more information.

9.9 Appendix I - Application/Client Security Dependencies

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

Applications

IP Office Component	Interface Controls	Login Account	IP Office Certificate Use	Other Controls	Notes
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 read - HTTP directory write	Service User	No		
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
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 Component	Interface Controls	Login Account	IP Office Certificate Use	Other Controls	Notes
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

IP Office Component	Interface Controls	Login Account	IP Office Certificate Use	Other Controls	Notes
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		

Extension

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	Yes: - Management	Auto-create H323 extension	TLS only can be enabled
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

Chapter 10.

Document History

10. Document History

25th July 2016	01a	• First draft for R10 based on CID168370 Issue 0.9.
26th September 2016	01b	• Fix faulty HTML page links caused by invalid title characters.
17th November 2016	01c	• Republish to correct bad rendering of symbols in Appendix F table.
22nd November 2016	01d	• Minor layout corrections.
8th May 2017	01e	• Minor corrections.

