AVAYA

IP Office 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 in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. 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 or on the express behalf of 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. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

"**Hosted Service**" means an Avaya 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 ONLY IF YOU PURCHASE AN AVAYA 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 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.

Licenses

The Global Software License Terms ("Software License Terms") are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

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, 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. Unless otherwise stated, 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

The following applies only 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.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE 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 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.

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply 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, please contact your Avaya Sales Representative.

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).

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: 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 Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud 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

Comments on this document?

Part 1: Overview

Chapter 1: Introduction

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.

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.

Related links

Change history

Updates for IP Office Release 11.1 FP1

- The voicemail password used to secure the connection between the IP Office and Voicemail Pro services is now fixed to 31-characters in length.

  - On new installs, a suitable 31-character password is automatically generated on first connection between the two services.

  - Existing systems can continue with existing shorter passwords. However, on any password change, the 31-character password length requirement is enforced.

Updates for IP Office Release 11.1 FP3

- **H.323/SIP Cipher Level Settings**

  The **H.323 Security Level** and **SIP Security Level** settings have been added to the certificate security settings. These control the minimum accepted cipher strength for H.323/SIP phone and trunk connections. They replace the previous NUSN options added for IP Office R11.1.2.x systems.

- **Enhanced Certificate Checks**

  The following enhancements have been made to received certificate checks performed by the IP Office:

  - The **Medium** and **High** certificate check levels now include the following additional checks:

    - Check that the certificate has a key usage defined.

    - If the certificate has extended key usage settings, check they match the purpose for which the certificate is being used.

- Check that the certificate does not include any unknown critical extension.

- Note: For systems upgraded to R11.1.3, these additional checks are not used unless the existing **Enhanced Certificate Checks** settings is changed.

  - The certificate checks can now include hostname validation, and verifying that the certificate source is authoritative for the SIP domain (RFC5922). This is done by changing the **Medium** and **High** certificate checks options to **Medium + Remote Checks** and **High + Remote Checks** respectively.

- **SIP Trunk Server Name Indication (SNI) Support**

  For SIP trunks, two new SLIC entries (`SLIC_ADD_SIP_SAN` and `SLIC_ADD_SAN`) can be used to add the IP Office **ITSP Domain Name** or **ITSP Proxy Address** as an SNI value where required by the ITSP during initial TLS connection.

Related links

Comments on this document?

Chapter 2: Overview

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

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

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

Related links

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.

Table continues…

Classification	Description
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 nonsensitive 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.

Related links

Applicability

The following information is applicable to IP Office IP500 V2, IP Office Server Edition, IP Office applications and endpoints for release 11.1.

The following areas are not covered in this document:

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

Related links

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.

Related links

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.

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.

Related links

Comments on this document?

Chapter 3: IP Office Security Fundamentals

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

- Unauthorized access or modification of data
- Theft of data
- Denial of Service (DoS) attacks
- Viruses and Worms
- Web-based attacks such as Cross-Site Scripting and Cross-Site Forgery
- Detection 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

Related links

IP Office Security Guidelines

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 processes 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.

Symmetric Encryption

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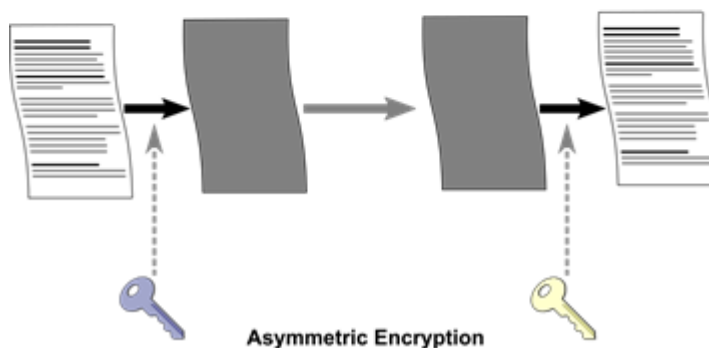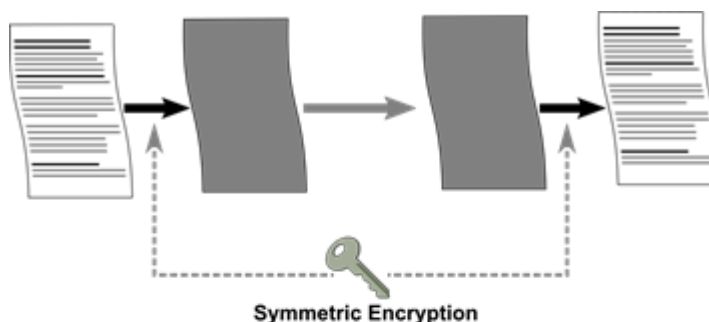
Most message data encryption is symmetric. The data sent may be optionally encrypted using a number of well known algorithms:

Algorithm	Effective key size (bits)	Use
DES-40	40	Not supported – insufficient strength

Table continues…

Comments on this document?

Algorithm	Effective key size (bits)	Use
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:

- Transport Layer Security (TLS v1.2 with v1.0 and v1.1 for legacy)
- Secure Shell (SSH v2)
- Secure RTP (SRTP)

Related links

IP Office Security Fundamentals on page 16
Message Authentication on page 18
Security Database on page 19

Message Authentication

Message authentication ensures that all data sent by either the system or IP Office 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.
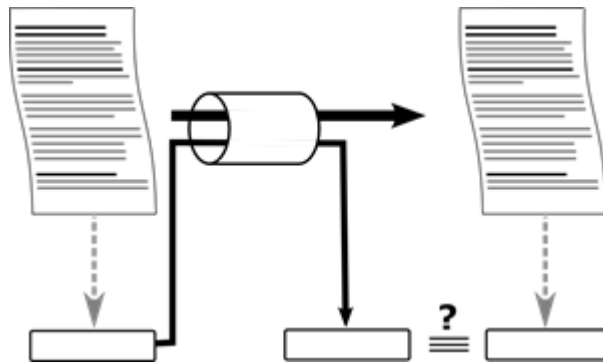
Any data sent may be optionally authenticated using a number of well-known and cryptographically secure algorithms:

Comments on this document?

Algorithms	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 v1.0, v1.1, and v1.2), Secure Shell (SSH v2), Secure RTP (SRTP) and IPsec protocols.

Related links

[Encryption](#) on page 17

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 IP Office 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, Avaya one-X® Portal for IP Office, Voicemail Pro, WebLM and Web Control have local administrative accounts used under fall-back conditions.

Related links

[Encryption](#) on page 17

Data Privacy

In recent years legislation such as the California Consumer Privacy Act (CCPA) and the European General Data Protection Regulation (GDPR) have highlighted the need to keep personal data – that is, information that can be traced back to an individual – under a high degree of control.

IP Office can under certain conditions process and save personal data. Some examples are:

- Call Detail Records (SMDR) may contain an individual's personal telephone number

- Call Recordings might contain personal information spoken by a caller

Responsibility to keep such data protected is ultimately the responsibility of the 'Data Controller'. For IP Office the Data Controller typically would be the company using the system. that is, the customer or their agent. Under CCPA this is referred to as a 'Business'.

Avaya IP Office, when used as part of a solution to process and save personal data on behalf of the customer is termed the 'Data Processor'. Under CCPA this is referred to as a 'Service Provider'. Note that IP Office will form only part of the Data Processor aspects, usually combined with other automated or manual processes.

IP Office cannot be individually certified to adhere to a specific data privacy requirement, but can be configured and operated by the Data Processor to achieve compliance with various data privacy regimes such as GDPR and CCPA.

The IP Office Platform adheres to the following set data privacy principles:

- Architectured and designed with data privacy in mind

- No personal data captured by default

- Controls over what personal data can be captured, and how long it is retained.

- Notifications to individuals before personal data is captured, along with a record of acceptance.

- All personal data secure both at rest and in transit

- Personal data remains local to the servers; IP Office Cloud storage remains within the geographic region.

- Access to all personal data controlled via the IP Office Authentication and Authorization framework

- Personal data can be exported, modified or deleted in response to data privacy requests.

- Access to personal data logged. These logs may be viewed by the customer to provide an audit trail of personal data access.

A Product Privacy Statement for IP Office can be found at: https://downloads.avaya.com/css/P8/documents/101049410.

Securing the IP Office Platform Solution contains information for securing the IP Office solution and must be followed from both a security and Data Privacy perspective. In addition, the following documents must be read prior to solution deployment:

- Avaya IP Office Product Privacy Statement

- Avaya Workplace Product Privacy Statement

- Avaya Collaboration Product Privacy Statement

- Avaya Contact Center Select Product Privacy Statement

       • Avaya Call Reporting For IP Office Product Privacy Statement

It is useful when reviewing these documents to understand the following terms. These definitions are broad in scope and may vary according to the data privacy regulations in force in a particular country/region.

Category	Description
Personal Data	Means any information relating to an identified or identifiable natural person. This could include personal phone numbers, information recorded during calls, email addresses, location data, home address.
Data Subject	An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name
Data Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. An example could be the customer operating the IP Office system.
Data Processor	A natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller. The IP Office system could form part of data processing.

Related links

Authentication and Authorization Framework

IP Office has its own Authentication and Authorization (AA) framework, and requests to IP Office services are routed through the AA framework. The AA framework prevents unauthenticated, unauthorized access to IP Office services and data.

The following diagram shows the service interfaces covered by this framework:
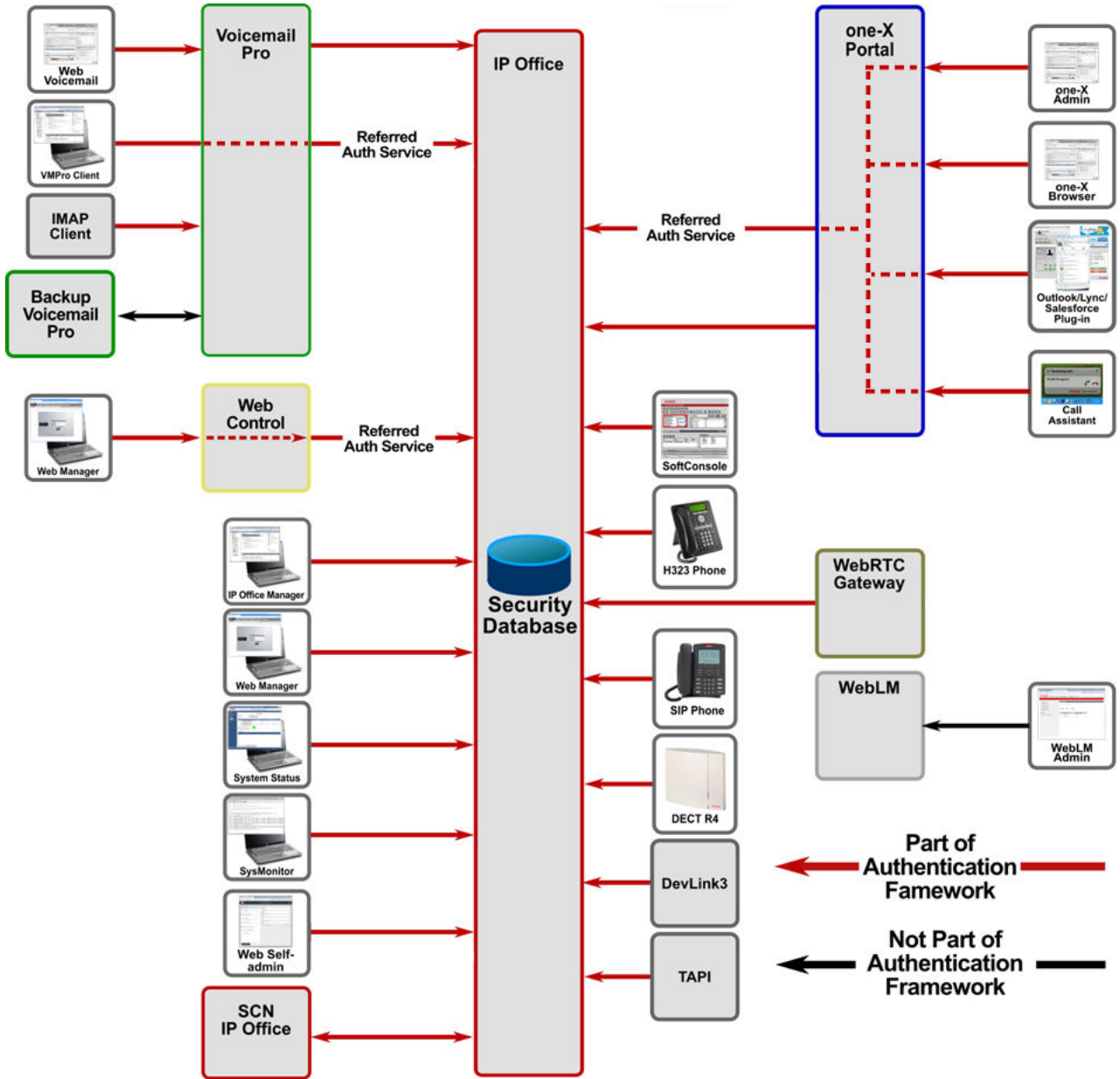
Avaya one-X® Portal for IP Office, Voicemail Pro and Web Control refer any administrative login to IP Office via an authentication/authorization web service.

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

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

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

Related links

Linux Platform Security

A number of IP Office products run on the Linux operating 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.
- **Enhanced Access Security Gateway (EASG) support:** EASG is a certificate based authentication system that replaces passwords for technical support accounts.
- **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.

Related links

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 Application Interface	System Status Application (SSA) access
Enhanced TSPI	Avaya one-X® Portal for IP Office CTI access
HTTP	Phone and IP Office Manager file access, Voicemail Pro, IP Office Line, System Monitor (secure)
Web Services	IP Office 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). 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.

Related links

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.

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.

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 Application Interface	**Secure, Medium**	✓	SSA access
Enhanced TSPI	**Secure, Medium**	✕	Avaya one-X® Portal for IP Office CTI access
HTTP	**Unsecure + Secure**	✕	Phone and IP Office Manager file access, Voicemail Pro, IP Office Line, System Monitor (secure)
Web Services	**Secure, Medium**	✓	IP Office Manager and SMGR
TFTP Server	Active (IP500 V2) Inactive (Linux)	✕	Allows access for IP Office 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)	✕	IP Office Manager upgrade access
Devlink	Inactive	n/a	DevLink and System Monitor UDP/TCP access
Devlink3	Active	✓	DevLink3 access
TAPI	Inactive	n/a	1st and 3rd party TAPI interfaces only
HTTP Directory Read	Active	✕	Avaya one-X® Portal for IP Office directory access, external directory feature
HTTP Directory Write	Active	✕	Avaya one-X® Portal for IP Office directory access

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

Related links

IP Office Security Fundamentals on page 16

Chapter 4: User Accounts and Rights of Access

There are two main types of user accounts 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. LinuxAvaya one-X® Portal for IP Office, Voicemail Pro and IP Office Web Manager use this service to 'Refer' administrative logins to the database.

Related links

Changing Administrative User and Rights Groups

IP Office Manager and IP Office 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 IP Office Web Manager have synchronization tools to assist.

For all Linux-based 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.

Related links

Default Administrative Users and Rights Groups

The following default service user settings are present on first start-up or following a security settings reset.

Related links

Default Service Users and Rights Groups

The following information is applicable for IP Office R11.1FP2.

Security Administrator Account

This is the default security administration account and has all rights to all security settings. You cannot remove or disable this account.

Default Service User Accounts

The following service user accounts are present on the first start-up, and after a security settings reset:

Name	Account Status	Description/Default Rights	Default Rights Group Membership
Administrator	**Enabled**	This service user is the default account for IP Office configuration. Do not remove, disable, or rename this service user.	**Administrator Group** **System Status Group** **Business Partner**
AdjunctServer	**Disabled**	Subscription mode IP Office systems use this service user to enable COM support for an IP Office application server.	**Adjunct Server**
BranchAdmin	**Disabled**	The IP Office uses this service user for IP Office branch systems managed by SMGR.	**SMGR Admin**
BuisnessPartner	**Disabled**	The IP Office uses this service user for configuration access by business partners.	**Business Partner**
COMAdmin	**Enabled**	Subscription mode IP Office systems using this service user for connection to COM.	**COM Admin**
DirectoryService	**Enabled**	The IP Office uses this service user for HTTP directory access.	**Directory Group**

Table continues…

Name	Account Status	Description/Default Rights	Default Rights Group Membership
EnhTcpaService	**Enabled**	The IP Office uses this service user for connection with the Avaya one-X® Portal service.	**TCPA Group**
IPDectService	**Disabled**	The IP Office uses this service user for DECT R4 system provisioning.	**IPDECT Group**
Maintainer	**Disabled**	The IP Office uses this service user for back up, restore and upgrade connections.	**Maintainer**
MCMAdmin	**Disabled**	The IP Office uses this service user for connection to Customer Operations Manager.	**MCM Admin**
TURNServer	**Disabled**	The IP Office uses this service user fto support User Portal WebRTC users using TURN.	**TURN Server**

Related links

Default Rights Groups

The following information is applicable for IP Office R11.1FP2 SP4 and higher. The following rights groups are present on first start-up and after a security settings reset.

Rights Group Settings

Rights Group	Rights Set		Rights Enabled
Administrator Group	**Configuration**	**IP Office Service Rights**	All
		Manager Operator Rights	**Administrator**
	External	**IP Office Service Rights**	**Media Manager Administrator**, **Reporter Administrator**
System Status Group	**System Status**	**IP Office Service Rights**	All
TCPA Group	**Telephony APIs**	**IP Office Service Rights**	**Enhanced TSPI Access**, **DevLink3**
	HTTP		**Directory Read**, **Directory Write**
IPDECT Group	**HTTP**	**IP Office Service Rights**	**DECT R4 Provisioning**, **Directory Read**
SMGR Admin	**Web Services**	**IP Office Service Rights**	All except **Service Monitor Read**
		Web Manager Rights	All except **Service Change**
Business Partner	**Configuration**	**IP Office Service Rights**	All

Table continues…

Rights Group	Rights Set		Rights Enabled
	Security Administrator		All
	System Status		All
	Web Services		All except **Service Monitor Read**
			All except **Service Change**
	External	**Web Manager Rights**	**Voicemail Pro Administrator**, **one-X Portal Administrator**, **Web Control Administrator**, **WebRTC Gateway Administrator**, **Authentication Module Server Administrator**
Maintainer	Configuration	**IP Office Service Rights**	**Read All Configuration**
	System Status		All
	Web Services		**Configuration Read All**, **Backup**, **Restore**, **Upgrade**
	External		**Voicemail Pro Basic**, **one-X Portal Super User**, **Web Control Administrator**, **Web Control Security**
Directory Group	HTTP	**IP Office Service Rights**	**Directory Read**, **Directory Write**
COM Admin	Web Services	**IP Office Service Rights**	**Security Write Own Password**, **Backup**, **Restore**, **Upgrade**
MCM Admin	Security Administrator	**IP Office Service Rights**	**Write Own Service User Password**
	Web Services		**Backup**, **Restore**, **Upgrade**
Adjunct Server	External	**IP Office Service Rights**	**Adjunct Server**
TURN Server	External	**IP Office Service Rights**	**TURN Server Connection**

Additional Rights Groups for Non-Subscription Systems

The IP Office creates these additional default rights groups on non-subscription mode systems. They have no associated default service users.

Rights Group	Rights Set		Rights Enabled
Manager Group	Configuration	**IP Office Service Rights**	All
		Manager Operator Rights	**Manager**
Operator Group	Configuration	**IP Office Service Rights**	All

Table continues…

Comments on this document?

Rights Group	Rights Set		Rights Enabled
		Manager Operator Rights	Operator
Security Admin	Security Administrator	IP Office Service Rights	All
Backup Admin	Web Services	IP Office Service Rights	Backup, Restore
	External	IP Office Service Rights	one-X Portal Super User
Upgrade Admin	Web Services	IP Office Service Rights	Upgrade
System Admin	Configuration	IP Office Service Rights	Read All Configuration, Write All Configuration, Merge Configuration
	Web Services	IP Office Service Rights	Security Write Own Password, Configuration Read All, Configuration Write All
		Web Manager Rights	All except Service Change
	External	IP Office Service Rights	Voicemail Pro Standard, one-X Portal Administrator, WebRTC Gateway Administrator
Maint Admin	Web Services	IP Office Service Rights	Backup, Restore, Upgrade
Customer Admin	Web Services	IP Office Service Rights	Security Write Own Password, Configuration Read All, Configuration Write All, Backup, Restore, Upgrade
		Web Manager Rights	All except Service Change
	External	IP Office Service Rights	Voicemail Pro Standard, one-X Portal Super User
Management API Group	Web Services	IP Office Service Rights	Management API Read, Management API Write
TURN Server	External	IP Office Service Rights	TURN Server Connection

Related links

> [Default Administrative Users and Rights Groups](#)

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.

Related links

[User Accounts and Rights of Access](#) on page 26

Chapter 5: 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) is improved implementing 'strong' passwords and a password change policy.

Related links

Password strength

	Definition
A strong password is typically one that:	• Is long (for example at least 8 characters)
	• Complex (for example 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

Table continues…

	Definition
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
	  - Dates, prevalent when 4, 6 or 8 digit minimum length is enforced
	  - Default login codes

Additional Information

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

- **Center 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

- **US-CERT Security Tip (ST04-002), Choosing and Protecting Passwords:**

  https://www.us-cert.gov/ncas/tips/ST04-002

Related links

Password and PIN Policy

Service User and User Password Policies

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

The policy applied to service users is configured in the system's security settings. This is done in the **Service User Details** section of the **General** tab.

The policy settings for each include:

- Service user minimum name and password length.
- Password complexity.

- Number of consecutive failure attempts and the subsequent action on failure.
- Ensure no previous passwords are reused.
- Enforced password change – both immediate and periodic.
- Idle account timeout.

User Password Policies

The policy applied to user passwords is configured in the system's security settings. This is done in the **IP Office User Details** section on the **General** tab.

The policy settings for each include:

- Minimum password length.
- Password complexity.
- Number of consecutive failure attempts and the subsequent action on failure.

Login Codes and Phone Passwords

PINs are used on IP Office for telephony user login (Login Code) and VoIP extension registration (Phone Password). The policy is configured using the **Telephony** > **Login Code Complexity**:

Mailbox Access Code

PINs are used on IP Office for voice mailbox access (Voicemail Code). The policy for this is configured using **System** > **Voicemail Code Complexity**:

Related links

[Password and PIN Management](#) on page 32

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 Setting	Notes
IP Office Manager IP Office Web Manager System Status Application Web Control Voicemail Pro client SysMonitor*	Service User name and password. Various rights of access Password: 1-31 Unicode characters	Change using IP Office Manager or Web Security Manager Security settings for Service User password policy apply Temporary or permanent lock out upon number of consecutive failed attempts. Current lockout status can be viewed in Manager under **Security** > **Service Users** > **Service User Details**. *SysMonitor will use this account when the **Security** > **System** > **Use Service User Credentials** setting is active.
Manager upgrade	System password Password: 1-31 ASCII printable characters	Change using IP Office Manager.
SysMonitor* DevLink	SysMonitor password Password: 1-31 ASCII 0-9, a-z, A-Z characters	Change using IP Office Manager. *SysMonitor will use this account when the **Security** > **System** > **Use Service User Credentials** setting is active.
Voicemail Pro client	Three admin roles: - Administrator - Standard - Basic Password: 5-31 ASCII printable characters except \ / : * ? < > | , ;.	Change using Voicemail Pro client, Voicemail Pro Administrators tab Used for Voicemail Pro as a fallback account when IP Office Referred Authentication is not available.
Avaya one-X® Portal for IP Office admin	Two admin roles: - Administrator - Backup/restore Password: 1-31 Unicode characters	Change using Avaya one-X® Portal for IP Office admin web page, Configuration | Users panel. Used for Avaya one-X® Portal for IP Office as a fall-back when IP Office Referred Authentication is not available
Linux Secure Shell (SSH)	One admin role: 'Administrator' Password: 1-31 ASCII printable characters	Change using Web Control login screen. Can only change password
Linux Console interface (CLI)	Two admin roles: - Administrator - root Password: 1-31 ASCII printable characters	Change using Web Control login screen: **Platform View** > **Settings** > **System Settings** tab. Can only change passwords

Table continues…

Login Interface	Account Setting	Notes
Voicemail Pro <-> IP Office service interface	VMPro password Password: 31 ASCII printable characters	Change using IP Office Manager and to match Voicemail Pro client.
Avaya one-X® Portal for IP Office <-> IP Office service interface	Service User name and password Password: 1-31 Unicode characters	Change using IP Office Manager or IP Office Web Manager. Change using Avaya one-X® Portal for IP Office admin web page, **Configuration** > **Providers** > **Default-CSTA-Provider** > **Edit** > .
TAPI Link Pro (3rd party TAPI)	System password Password: 1-31 ASCII printable characters	Change using IP Office Manager. TAPI Link Lite is covered in IP Office Users' Passwords and Login Codes.
DECT R4 Provisioning	Service User name and password Password: 1-31 Unicode characters	Change using IP Office Manager. Change using base station web admin interface
DevLink3 API Location API Service Monitoring API Web Management SDK API	Service User name and password Password: 1-31 Unicode characters	Change using IP Office Manager.

Related links

User Passwords and Login Codes

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

- Password is defined by the configuration field **User** > **User** > **Password** and 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 Manager and IP Office Web Manager.

Login Interface	Account Setting	Notes
IP Office SoftConsole Outlook plugin, Call Assistant TAPI Link Lite (first-party TAPI) RAS (dial in) Users User Portal	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. Temporary or permanent lock out upon number of consecutive failed attempts.
Voicemail Pro mailbox Embedded Voicemail mailbox	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.
IP Office User phone login	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.
H323 Phone registration SIP Phone registration	Phone extension: **Extension** > **Extn** > **Base Extension** Login Code: **User** > **Telephony** > **Supervisor Settings** > **Login Code** Attributes: 0-31 ASCII digits	System settings for password/PIN policy apply: **System** > **Telephony** > **Login Code Complexity**. Temporary lock out upon number of consecutive failed attempts **Extension** > **Extn** > **Phone Password** field is used if set. Current lockout status can be viewed and reset in SSA under **System** > **VoIP Security** > **Blacklisted Extensions** and **Blacklisted Addresses**.

Related links

Additional information

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

- **Center 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

- **US-CERT Security Tip (ST04-002), Choosing and Protecting Passwords:**

  https://www.us-cert.gov/ncas/tips/ST04-002

Related links

Part 2: Certificates

Chapter 6: Certificates

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.

Related links

Certificates and Trust

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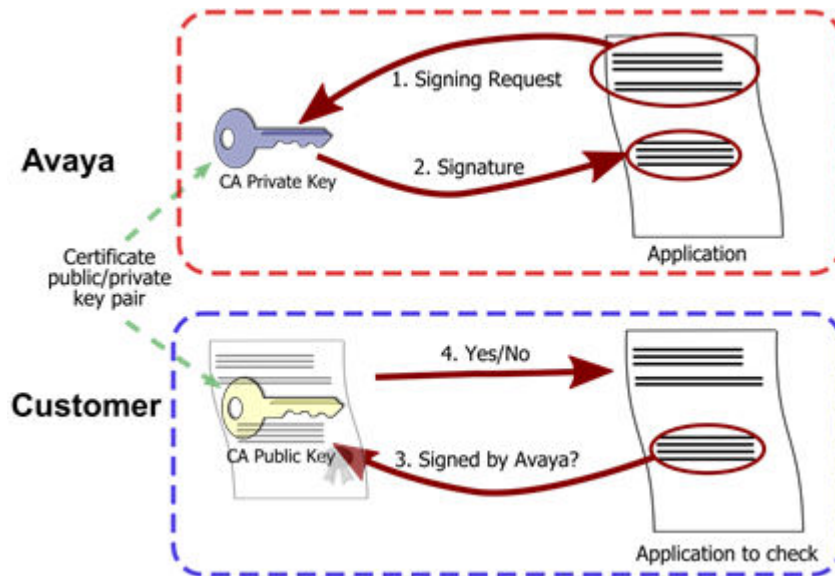
One point from the above example is that the private key must remain private; anyone with access to the key can masquerade as Avaya.

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):
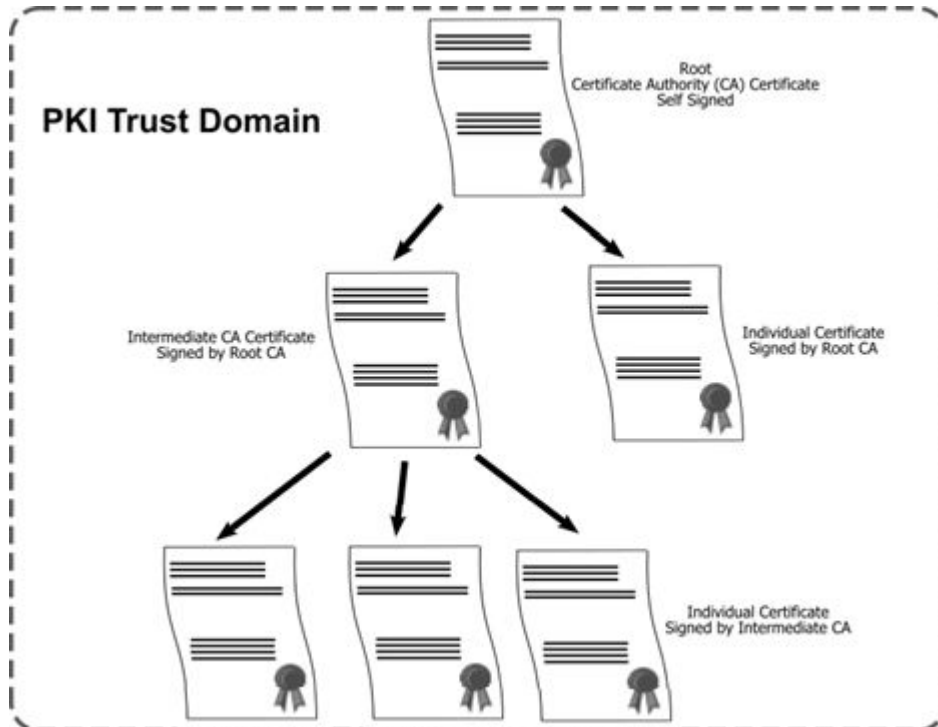
Related links

Certificate Terminology

Throughout this document the following terms and definitions will be used in the context of certificates:

Term	Description
Certificate	A digital certificate containing identity information, a public key and other digital security data conforming to the X.509 v3 standard.
Certificate Authority	An entity that can issue identity certificates signed by another certificate.
Root CA Certificate	A 'self-signed' certificate (that is, 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 and 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.
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, for example, 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, and so on) 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 (that is, one identity).
Multi Domain Certificate	Also called 'Multi-SAN' or 'Unified Communications' certificate. A certificate created for a single server with many domains/identities, each identity is one name entry.

Table continues…

Comments on this document?

Term	Description
Wildcard Certificate	A certificate created for a multiple servers or a single server with many domains/identities. The name entry is of the form '*.example.com'. Wildcard certificates carry additional security risks and limitations. See Certificate Name Content on page 49.

Related links

Certificate Components

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

Components	Description
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 serialized, just that it is unique.
Subject (Issued to)	The entity (person, system and so on) identified by the certificate. This is divided into a number of sub fields: Common Name (CN), Organization Unit (OU), email, etc. Typically the CN is referred to as the 'Name' of the certificate.
Subject Alternative Name(s)	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 (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 (Issued to)**.
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 (for example, certificate signing, encryption).
Signature Algorithm	The cryptographic algorithm used to create the signature.
Subject Key Identifier	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 (for example, RSA, DSA.).
Public Key	The public key.

There are other fields that may be present, see RFC5280 for more information.

Related links

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.

Related links

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 and so on.

- 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 (that is, certificate has be canceled 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.

Related links

Certificates and Transport Layer Security (TLS)

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.

The IP Office platform supports TLS v1.0, v1.1 and v1.2. All TLS interfaces start with TLS v1.2 but can allow negotiation down to v1.1 or v1.0 for compatibility. There are IP Office, Voicemail Pro, IP Office Web Manager and Avaya one-X® Portal for IP Office admin settings for 'Minimum TLS version' that enforce v1.2.

Note that some Avaya clients do not support v1.2 at present. See <u>IP Office VoIP Endpoint Security</u> on page 161.

Related links

Certificate File Naming and File Formats

Like so many other aspects of certificates, there are various options and standards (both formal and informal) associated with certificate files.

File Formats

There are four main encodings/internal formats for certificate files. Note these are encodings, not file naming conventions:

Format	Description
DER	Distinguished Encoding Rules (DER) format. This 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 (that is, ASCII text) encoding of DER: • The certificate is enclosed between `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` statements. • The file contain a private key enclosed between `-----BEGIN PRIVATE KEY-----` and `-----END BEGIN PRIVATE KEY-----` statements. More than one certificate can be included. • PEM certificates can be identified by viewing the file in a text editor. This is an unsecure format and not recommended for private key use unless it is protected with a password.
PKCS#12	Public Key Cryptography Standard (PKCS) #12. A secure, binary format, encrypted with a password. Typically used to describe 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 (that is, ASCII text) encoding defined by RFC 2315. One or more certificates are enclosed between `-----BEGIN PKCS-----` and `-----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.

Filename Extensions

There are many common filename extensions in use:

Format	Description
`.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 Creating a CSR using the OpenSSL Package on page 186 for information on OpenSSL format conversion.

Related links

Certificates on page 40

Chapter 7: IP Office Certificate Support

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

Related links

IP Office Certificate Support

The IP Office platform can be configured to use certificates as follows:

- 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 IP Office Web Manager, or obtained automatically using the Simple Certificate Enrollment Protocol (SCEP) or PKCS#10 (IP Office Linux only).

- 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 Linux 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, SHA-224 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.

Related links

IP Office Certificate Support

Currently IP Office certificate support does not include the following:

- Linux Applications (including Avaya one-X® Portal for IP Office and Voicemail Pro) cannot be configured for mutual authentication. That is, they cannot check any received certificate against the TCS.
- SIP clients' certificates are not requested.
- The received certificate tests of IP Office do not include revocation checks such as OCSP or CRLs.
- 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.
  - The IP500 V2 servers does not support the manual generation of a Certificate Signing Request (CSR) where the private key is retained within the server. Use either a web form based request or a third-party tool to create a CSR. See Certificate Signing Requests on page 179 for more information on how to generate a CSR for IP Office.

Related links

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 Transport Layer Security (TLS) on page 44.

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

- The table in IP Office Interface Certificate Support lists all TLS links in the IP Office platform solution and their security capabilities including certificate support. See IP Office Interface Certificate Support on page 155.
- The table in IP Office VoIP Endpoint Security lists VoIP clients in the IP Office platform solution and their security capabilities. See IP Office VoIP Endpoint Security on page 161.

Related links

Certificate Name Content

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

- Although the IP Office does not process the **Subject Alternative Name(s)** 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 on page 161 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:

FQDN Options	Description
System FQDN as the Subject Name	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 **Subject Name** field should never be empty. • **Example:** `ipo.example.com`
System FQDN as a SAN DNS Entry	The system's FQDN as a 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, this entry typically should have the value configured in **System** > **LAN1/2** > **VoIP** > **SIP Registrar** > **SIP Registrar FQDN**. • **Example:** `DNS:ipo.example.com`
Other Domain Names and FQDNs as SAN DNS Entries	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`
SIP Domains as SAN DNS Entries	Any SIP domains in use as one SAN entry for each SIP domain, in DNS format. This is typically the value configured in **System** > **LAN1/2** > **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`

Table continues…

FQDN Options	Description
SIP Domains as SAN DNS SIP Entries	Any SIP domains in use as one SAN entry for each SIP domain, in URI format. This is typically the value configured in IP Office Manager **System** > **LAN1/2** > **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`
LAN1 IP Address as a SAN IP Entry	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 Note: Most public Certificate Authorities do not support IP Address fields.
LAN2 IP Address as a SAN IP Entry	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` Note: Most public Certificate Authorities do not support IP Address fields.
NAT and Public IP Addresses as SAN IP Entries	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` Note: Most public Certificate Authorities do not support IP Address fields.
SIP IP Address as SAN URI Entries	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` Note: Most public Certificate Authorities do not support IP Address fields.
Wildcard Entries	Under certain circumstances, the use of 'wildcard' names might be considered. A wildcard name field contains an asterisk in the name (for example, '*.example.com') and covers all sub-domains. IP Office can support such fields in both Subject Name and SAN wildcard name fields, but carry additional security risks and limitations and hence are not recommended. See the notes below.

Certificate Name Content Notes

- Most public Certificate Authorities do not support IP address and private domains. For a public CA, only DNS resolvable and public domains should be used for all clients.
    - Note that using IP address can compromise the administration of 96xx and other endpoints.

- 11xx/12xx series phones do not support FQDNs and hence cannot be used with certificates provided by public Certificate Authorities.

• The certificate **Subject Alternative Name** can be a domain name or IP address. For Transport Layer Security (TLS) connections, browsers may check that the connection to the site is using a valid, trusted server certificate. If the certificate does not have the correct **Subject Alternative Name** entry or has an invalid Domain name, the connection can be compromised.

• Wildcard certificates (or certificates with wildcard name fields) carry the following additional risks:

- If one server or sub-domain is compromised, all sub-domains can be compromised.

- If used for more than one server, the private key can become exposed.

- If the wildcard certificate is revoked, all sub-domains need a new certificate.

- Wildcard certificates do not work with all server-client configurations.

- Wildcard Certificates are not protected by CA extended validation or warranty.

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

• IP Office does not support wildcard certificates for use with Avaya SIP clients. That includes Avaya Workplace Client, Avaya Vantage™ or J100 Series endpoints.

IP Office and Server Edition Primary/Linux Application Server support the creation of certificates with up to 8 SAN fields with the following options:

• **DNS** – used for hostname or FQDN

• **URL** – used for URLs and URIs

• **IP** – IP Address in v4 format

• **Email** – email address

These SAN fields can also be used for Certificate Signing Requests via SCEP.

See Initial Certificate Settings on page 60 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 a Linux Application Server where DNS always resolves itself to the same FQDN.

Other deployments where the identity of the system differs depending upon access (for example, LAN or WAN) or the use of SIP or H323 endpoints with secure signaling, SANs will typically be required.

Related links

IP Office Certificate Support on page 47

Certificate Check Controls

Where IP Office acts as the TLS or HTTPS server for a connection, it requests a certificate from the client.

- If no certificate is received, the IP Office rejects the connection.
- If a certificate is received, the IP Office applies certificate checks. If the checks are successful, the IP Office enables the connection.

The following are levels of received certificate checks can be used for various IP Office TLS/HTTPS connections. See IP Office Interface Certificate Support on page 155 for more information.

Settings	Description
None	• Check that the certificate is in date.
Low	The same **None** plus: • Check the certificate's public key is 1024 bits or greater.

Medium	The same as **Low** plus:
	
	• Check there is a trust chain from the Trusted Certificate Store (TCS) to the root Certificate Authority (CA).
	
	• For IP Office R11.1.3 and higher, also:
	
	  - Check that the certificate has a key usage defined.
	
	  - If the certificate has extended key usage settings, check that they match the purpose for which the certificate is being used.
	
	  - Check that the certificate does not include any unknown extensions marked as critical.
	
	  - Note: For systems upgraded to R11.1.3, these additional checks are only used after the existing setting is changed. For example, changed from **Medium** to **High** and then back to **Medium**. Backup the configuration before making any change.

High	The same as **Medium** plus: • Check the certificate's public key is 2048 bits or greater • Check the certificate is not a self-signed certificate. • Not reflected. • Check there is a copy of the certificate in the IP Office system's **Trusted Certificate Store**. This settings enables implementation of a strict trust domain where only known certificates are accepted. This is a form of 'certificate pinning' and overcomes the limitation of the standard tree structure PKI where any certificates issued by the root CA are always trusted.
Medium + Remote Checks	Use the same checks as **Medium** plus: • Perform hostname validation to verify that one of the SAN entries matches the connection's FQDN. If necessary, the SAN entry used can be an IP address. • For SIP, verify that the certificate source is authoritative for the SIP domain as in accordance with RFC5922.
High + Remote Checks	Use the same checks as **High** plus the same additional checks as **Medium + Remote Checks**.

The certificate check levels are applied using the following IP Office settings:

Function	Description
Administrator Access Checks	This setting is used for HTTPS/TLS administration connections to the system by applications such as IP Office Manager when the **Service Security Level** of the service being used is set to **High**. • **Certificates** > **Received Certificate Checks (Management Interfaces)** - The services to which this applies are: <table><tr><th>Service</th><th>Usage</th></tr><tr><td>**Configuration**</td><td>Applies to IP Office Manager configuration settings and Configuration Web Service (XO) DevConnect interfaces.</td></tr><tr><td>**Security Administration**</td><td>Applies to IP Office Manager security settings.</td></tr><tr><td>**HTTP**</td><td>Applies to HTTPS clients connecting to port 443 & 411. Typically H323 phones, DECT R4, IP Office lines,Voicemail Pro, SysMonitor. Also applies to the IP Office Web Manager interface on port 8443.</td></tr></table>
SIP Lines SM Lines	This security setting sets the certificate check level the IP Office uses for certificates it receives SIP and SM line TLS telephony connections: • **Certificates** > **Received Certificate Checks (Telephony Endpoints)** - An identity certificate is not installed in all SIP phones. Therefore, for SIP, the IP Office does not require a client certificate from SIP phones, only from SIP and SM trunks.

IP Office Lines	This configuration setting sets the certificate check level used by an **IP Office** line:
	
	• (**Line** or **System Settings** > **Line**) | **IP Office Line** > **Line** > **Security** = **High**
	
	  - This setting is available for IP Office lines with their **Transport Type** set to **WebSocket Client** or **WebSocket Server**. It applies regardless of the **Received Certificate Checks (Management Interfaces)** checks setting.
	
	  - The **Medium + Remote Checks** and **High + Remote Checks** options are not available for this setting.
	
	  - Applies to port 443.

Related links

Chapter 8: Certificate Distribution

This section covers the processes of certificate distribution.

Related links

Identity Certificate Distribution

The following methods can be used for identity certificate distribution.

Related links

Manual ID Certificate Distribution 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, IP Office Manager or IP Office Web Manager can be used to administer it on IP Office:
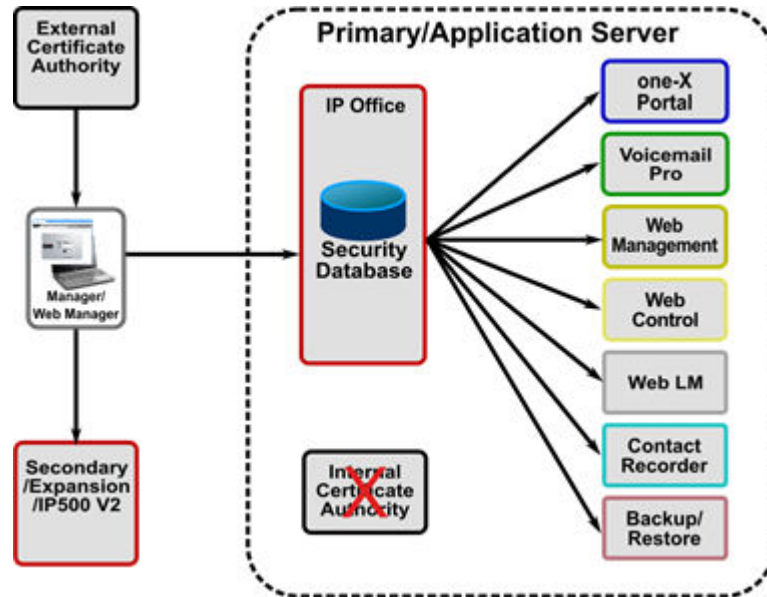
For more information on creation of a PKI based on an External CA, see Implementing IP Office PKI on page 74.

For more information on external Certificate Authorities, see Certificate from External Certificate Authorities on page 78.

Related links

Manual ID Certificate Distribution from the Primary or Linux Application Server

The internal certificate authority can be used to create a set of unique identity certificates in the 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, IP Office Manager PCs and so on. Once the identity certificate/private key file is saved to the local PC, IP Office Manager or IP Office Web Manager can be used to administer it on IP Office.
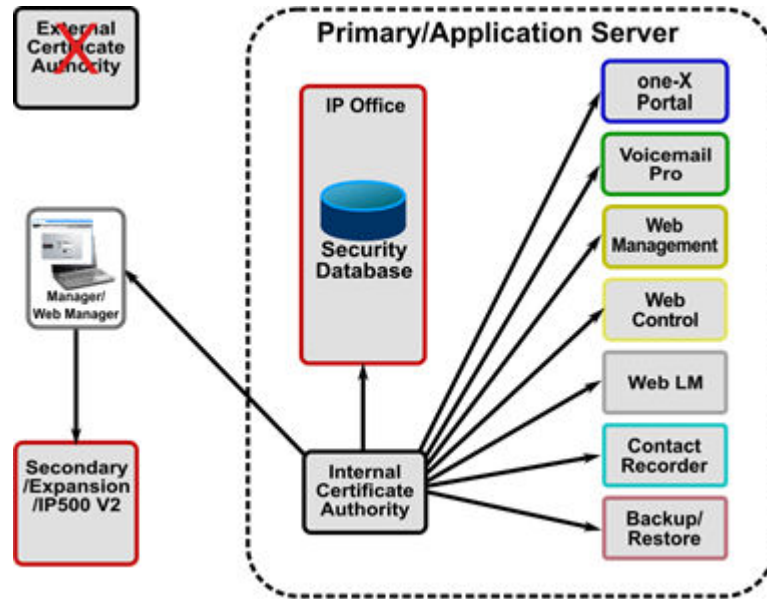
For more information on creation of a PKI based on an internal CA, see Implementing IP Office PKI on page 74.

Related links

Identity Certificate Distribution on page 54

ID Certificate Distribution using Simple Certificate Enrollment 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 enrollment 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).

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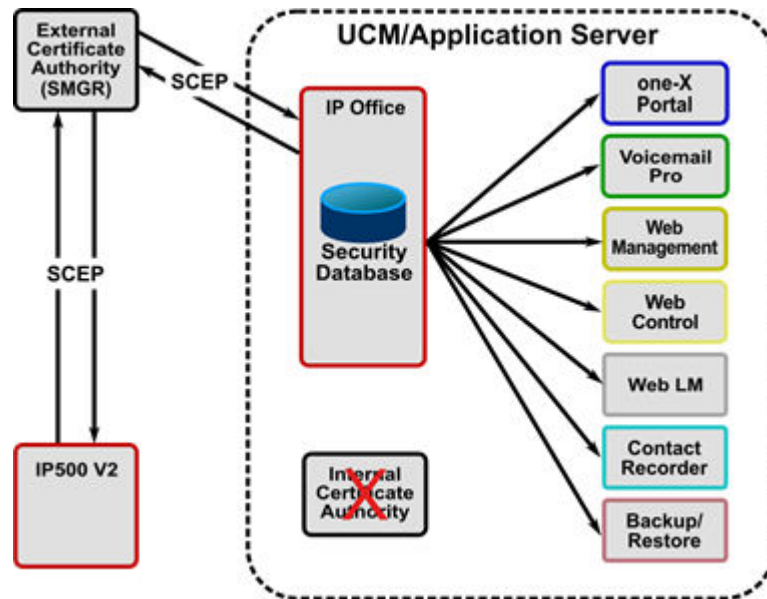
In all cases (External CA, Internal CA, SCEP), when a new identity certificate is received by IP Office, all relevant interfaces/applications are updated.

For more information on creation of a PKI based on SCEP, see Implementing IP Office PKI on page 74.

Related links

Identity Certificate Distribution on page 54

ID Certificate Distribution Using a PKCS#10 CSR

A PKCS#10 certificate Signing request (CSR) is created on the IP Office Linux server via the command line interface (CLI). The private key is retained within the server. The CSR is sent to an external CA who verifies the contents and creates an identity certificate signed by the CA.

Once the identity certificate is returned the CLI is used to combine with private key and distributed with the server.
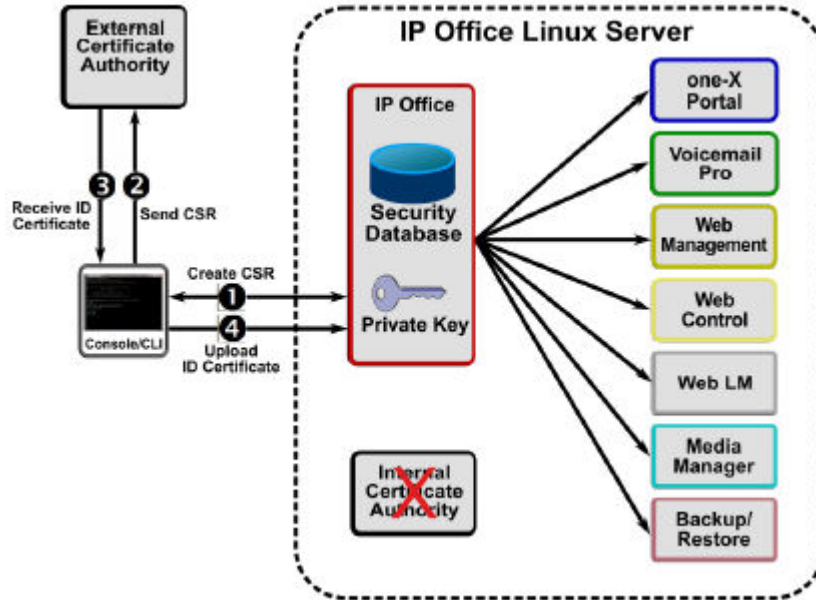
For more information on creation of a PKI based on an External CA, see Implementing IP Office PKI on page 74.

For more information on external Certificate Authorities, see Certificate from External Certificate Authorities on page 78.

Related links

Identity Certificate Distribution on page 54

Root CA Certificate Distribution

If the trust policy selected uses a well-known public CA (such as VerisignTM), their root certificates are typically already installed in the relevant operating 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 IP Office Manager or IP Office Web Manager for each IP Office.

For more information on Root CA Certificate distribution, see Implementing IP Office PKI on page 74.

Related links

Certificate Distribution on page 54

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 on page 74.

Related links

Certificate Distribution on page 54

Chapter 9: Initial Certificate Settings

New IP Office automatically install a number of certificates.

Related links

IP500 V2 Initial Certificate Settings

IP500 V2 creates a unique self-signed CA certificate at initial start-up and when the security settings are defaulted. The initial certificate contains the fields listed below.

- This certificate can be used for PKI operations but only in a limited manner. It has some security value, but is not part of a wider PKI and so will not be 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-nnnnnnnnn.avaya.com`
	`O = Avaya Inc`
	`OU = GCS`
	`L = Basking Ridge`
	`S = New Jersey`
	`C = US`
	`E = support@avaya.com`
		Where `nnnnnnnnn` is the LAN 1 mac address, for example `ipoffice-00e00705918e.avaya.com`

Subject Alternative Name(s)	`DNS Name=ipoffice-nnnnnnnnn.avaya.com`
	
	`IP Address=a.b.c.d`
	
	`IP Address=e.f.g.h`
		Where:
		
		• `nnnnnnnnn` 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

Table continues…

Certificate Field	Contents	Notes

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`	Matches the UTC certificate creation time/date minus 24 hours. 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 825 days	–

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`	–
Subject Key Identifier	Signature data	–
Public Key Algorithm	RSA	–
Public Key	Size 2048 bits	–

Note

- The correct LAN 1 and LAN 2 address should be set during initial installation and the identity certificate manually regenerated.

Related links

Linux Servers Prior to Ignition

Before ignition is completed, the default Server Edition distribution does not have a unique certificate. Instead it has a self-signed certificate with the subject and issuer of 'ipoffice-default.avaya.com'. In order to connect a browser for ignition, temporarily accept the certificate but do not store it permanently.

Once ignition has completed, the default certificate it is replaced by an server specific identity certificate generated according to the selected server role.

Related links

Server Edition Primary/Linux Application Server Initial Certificate Settings

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

Table continues…

Certificate Field	Contents	Notes

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 as follows:
		
		• Use the IP Office Web Manager option **Platform View** > **Settings** > **System Settings** > **Network** > **Host Name** field if it is set to something other than:
		
		  - `localhost`
		
		  - `localhost.localdomain`
		
		  - the installer default (mac address)
		
		• 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' for example, 'ipoffice-root-00e007057307.avaya.com'
		
		The correct hostname should be set during ignition, if not the root CA certificate will need to be regenerated.

Subject Alternative Name(s)	`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`	Matches the UTC certificate creation time/date minus 24 hours. 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.

Table continues…

Certificate Field	Contents	Notes
Subject Key Identifier	`Key Identifier`	This value is placed in the Authority Key Identifier of any signed certificates.
Signature Algorithm	`sha256RSA`	–
Subject Key Identifier	Signature data	–
Public Key Algorithm	RSA	–
Public Key	Size 2048 bits	–

Identity Certificate

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 during ignition as follows:
		
		• Use the IP Office Web Manager option **Platform View** > **Settings** > **System Settings** > **Network** > **Host Name** field if it is set to something other than:
		
		  - `localhost`
		
		  - `localhost.localdomain`
		
		  - the installer default (mac address)
		
		• 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' for example, 'ipoffice-root-00e007057307.avaya.com'
		
		The correct hostname should be set during ignition, if not the root CA certificate will need to be regenerated.

Table continues…

Certificate Field	Contents	Notes
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 1.
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 825 days	–
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	–
Subject Key Identifier	Signature data	–
Public Key Algorithm	RSA	–
Public Key	Size 2048 bits	–

Note 1:

- Identity certificate regeneration is done automatically if the IP Office Web Manager setting **Platform View** > **Settings** > **General** > **Certificates** > **Renew automatically** is active (default).
- The correct LAN 1 and LAN 2 address should be set during ignition. If not, the identity certificate needs to be regenerated.

Related links

Server Edition Secondary/Linux Expansion Initial Certificate Settings

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 either by one generated by the Primary Server or, if using external certificate, one from the 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 during ignition as follows:
		
		• Use the IP Office Web Manager option **Platform View** > **Settings** > **System Settings** > **Network** > **Host Name** field if it is set to something other than:
		
		- `localhost`
		
		- `localhost.localdomain`
		
		- the installer default (mac address)
		
		• 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' for example, 'ipoffice-root-00e007057307.avaya.com'
		
		• The correct hostname should be set during ignition, if not the root CA certificate will need to be regenerated.

Subject Alternative Name(s)	None	–

Table continues…

Certificate Field	Contents	Notes

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`	Matches the UTC certificate creation time/date minus 24 hours. 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	–
Subject Key Identifier	Signature data	–
Public Key Algorithm	RSA	–
Public Key	Size 2048 bits	–

Related links

Chapter 10: 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.

Related links

Certificate Trust Policy Considerations

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 (for example, client checks sever), or both-way (for example, 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

Related links

[Determining Trust Policy](#) on page 68

Branch System Certification

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

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

Related links

[Determining Trust Policy](#) on page 68

Approach 1: PKI Trust Domain based on Primary or Linux 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 – that is, 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.

Related links

[Determining Trust Policy](#) on page 68

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

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

Potential advantages for intermediate CA certificate on the Primary/Linux 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.

Related links

[Determining Trust Policy](#) on page 68

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 Linux Application Server exists.

- 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.

Related links

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.

Related links

[Determining Trust Policy](#) on page 68

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 IP Office Web Manager; this will create a new certificate for the next 7 years. Any existing browser exceptions will need to be re-asserted.

Related links

[Determining Trust Policy](#) on page 68

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.

Comments on this document?

Related links

Chapter 11: Implementing IP Office PKI

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

Related links

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

Procedure

1. The Primary Server CA should be used for Server Edition deployments. The Linux Application Server for non-Server Edition deployments. The same CA must be used for all systems in a deployment.

2. Enable the setting **Platform View** > **Settings** > **General** > **Certificates** > **Renew automatically** on the Primary/Linux Application Server.

3. For every device (server, IP500 V2 and so on) use the CA to create a unique ID certificate for each with the correct name content and save to a local directory. The name fields of the certificate are important for correct interoperation with clients; see [Certificate Name Content](#) on page 49 for more information. See [Using the IP Office Certificate Authority](#) on page 167.

4. Save the root CA certificate in both PEM and DER formats to a local directory using the IP Office Web Manager setting **Platform View** > **Settings** > **General** > **Certificates** > **CA Certificate** > **Download (PEM-Encoded)** and **Download (DER-Encoded)**.

5. Use IP Office Web Manager or IP Office Manager to save the CA certificate in each TCS.

6. Use IP Office Web Manager or IP Office Manager to save the ID certificate on the relevant IP Office server. See [Update Certificates](#) on page 102.

7. If SIP or H.323 phones are using HTTPS for provisioning or TLS for signaling, the IP Office root CA certificate must be present on each phone. See [VoIP Security](#) on page 85.

8. 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.

9. Verify that the correct ID certificate has been applied on each device using a browser or other diagnostic tool.

10. Enable certificate checking in the IP Office security settings and IP Office lines.

11. Verify using SE Manager that all IP Office systems are online with no alarms.

12. Enable secure connections for clients.

13. Verify each client can connect successfully.

14. Ensure all ID certificate files are stored securely.

15. Once all checks have been carried out, a configuration backup should be taken.

Related links

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

Procedure

1. The Primary Server CA should be used for Server Edition deployments. The Linux Application Server for non-Server Edition deployments. The same CA must be used for all systems in a deployment.

2. Enable the setting **Platform View** > **Settings** > **General** > **Certificates** > **Renew automatically** on the Primary/Linux Application Server.

3. Select an appropriate Certificate Authority that can fulfill the trust and certificate requirement of the deployment. For more information on external public authorities, see Certificate from External Certificate Authorities on page 78.

4. Request an Intermediate CA certificate/private key pair from a trusted Certificate Authority in PCKS#12 format. An intermediate CA certificate differs in content to a root CA or a device identity certificate.

5. Download the root CA certificate (and any further intermediate CA certificates) from the Certificate Authority in PEM and DER format to a local directory.

6. Install Intermediate CA certificate the on the Primary or Linux Application Server. This can either be done during ignition, or post ignition via the IP Office Web Manager setting **Platform View** > **Settings** > **General** > **Certificates** > **CA Certificate** > **Import**.

7. For every device (server, IP500 V2 and so on) use the CA to create a unique ID certificate for each with the correct name content and save to a local directory. The name fields of the certificate are important for correct interoperation with clients; see Certificate Name

Content on page 49 for more information. See Using the IP Office Certificate Authority on page 167.

8. Save the intermediate CA certificate in both PEM and DER formats to a local directory using the IP Office Web Manager setting **Platform View** > **Settings** > **General** > **Certificates** > **CA Certificate** > **Download (PEM-Encoded)** and **Download (DER-Encoded)**..

9. Use IP Office 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.

10. Use IP Office Web Manager or IP Office Manager to save the ID certificate on the relevant IP Office server. See Update Certificates on page 102.

11. Distribution of the root CA certificate to phones, clients and browsers is as per PKI Trust Domain based on Primary or Linux Application Server root CA section above.

12. Verification and enabling steps are as per PKI Trust Domain based on Primary or Linux Application Server root CA section above, with the note that many external CAs provide online verification tools.

13. Once all checks have been carried out, a configuration backup should be taken.

Related links

Implementing IP Office PKI on page 74

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

Procedure

1. The CA on the Primary or Linux Application Server is not used.

2. Enable the setting **Platform View** > **Settings** > **General** > **Certificates** > **Renew automatically**.

3. Select an appropriate Certificate Authority that can fulfill the trust and certificate requirement of the deployment. For more information on external public authorities, see Certificate from External Certificate Authorities on page 78.

4. For every device (server, IP500 V2 and so on) request the CA to create a unique ID certificate for each with the correct name content and save to a local directory. The name fields of the certificate are important for correct interoperation with clients; see Certificate Name Content on page 49 for more information.

5. For IP500 V2 devices, an external form based CSR must be used. For IP Office Linux devices, a PKCS#10 CSR can be created using the CLI. For more information on the CSR process, see Certificate Signing Requests on page 179.

6. Download the root and any intermediate CA certificate from the Certificate Authority in PEM and DER format to a local directory.

7. Use IP Office Web Manager or IP Office Manager to:

   • Save both the root and intermediate CA certificate in the TCS.

   • Activate the certificate chaining feature Offer ID Certificate Chain.

8. Use IP Office Web Manager or IP Office Manager to save the ID certificate on the relevant IP Office server. See Update Certificates on page 102.

9. Distribution of the root CA certificate to phones, clients and browsers is as per PKI Trust Domain based on Primary or Linux Application Server root CA section above.

10. Verification and enabling steps are as per PKI Trust Domain based on Primary or Linux Application Server root CA section above, with the note that many external CAs provide online verification tools.

11. Once all checks have been carried out, a configuration backup should be taken.

Related links

Implementing IP Office PKI on page 74

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

Procedure

1. The CA on the Primary or Linux Application Server is not used; disable the setting **Platform View** > **Settings** > **General** > **Certificates** > **Renew automatically**.

2. Select an appropriate Certificate Authority that can fulfill 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.

Related links

Implementing IP Office PKI on page 74

Chapter 12: Certificate 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.

Related links

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 Linux Application Server should be used.

Select a Certificate Authority that can fulfill 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](#) on page 179 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 File Formats](#) on page 45 for more information on certificate file formats.

    - See [Creating a CSR using the Linux Server Command Line](#) on page 189.

- If required, can the Certificate Authority provide multi-domain (AKA 'Multi-SAN' or 'Unified Communications') certificates?

- If required, can the Certificate Authority provide a signing CA certificate? The option would be required for Approach 2: PKI Trust domain based on Primary or Linux 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 File Formats](#) on page 45 for more information on certificate file formats.

- What notification/assurance level is required? Providers typically offer a number of levels under various names:

	Description
Intermediate	Also know as **Organization Validation**. The domain and company are validated. Browsers should not raise an error/warning, company information is shown.
Basic	Also known as **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.
Enhanced	Also know as **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?

Related links

[Certificate from External Certificate Authorities](#) on page 78

Obtaining Identity Certificates

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

- The name fields of the certificate are vital for correct interoperation with clients; see [Certificate Name Content](#) on page 49 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 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 File Formats](#) on page 45.

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](#) on page 179.

Related links

[Certificate from External Certificate Authorities](#) on page 78

Chapter 13: Certificate Maintenance

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

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

For identity certificates derived from a CA, replacement is relatively straight forward as the CA (and hence the basic trust relationship) is unchanged: Obtain the relevant replacement before expiry with the same content and replace. If the root or intermediate CA requires changing, the process can be more extensive depending on whether the associated public/private key pair also changes. The IP Office internal CA on the Primary will optionally retain the public/private key pair if the CA certificate is recreated via Web Management (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 IP Office Manager and IP Office Web Manager will display an identity certificate expiry warning, along with the number of days remaining. IP Office raises an alarm – a daily system event in SSA, SNMP, syslog, email – whenever any certificate is within 60 days of expiry.

Related links

Renewing an IP500 V2/Linux Secondary Certificate

If the default self-signed certificate or SCEP is being used, deleting the current or restarting the system 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 IP Office 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 IP Office Web Manager.

Related links

[Certificate Maintenance](#) on page 81

Renewing a Primary/Application Server ID Certificate

If the ID certificate has been created by the internal CA, the setting Web Management Platform option **Platform View** > **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 IP Office Web Manager.

Related links

[Certificate Maintenance](#) on page 81

Renewing a Primary/Application Server CA Certificate

A new one can be created using Web Management option **Platform View** > **Settings** > **General** > **Certificates** > **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](#) on page 167.

Related links

[Certificate Maintenance](#) on page 81

Recovering a 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.

Related links

[Certificate Maintenance](#) on page 81

Certificate 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 IP Office Manager, IP Office 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 IP Office Manager can be configured to accept any certificate. See Securing IP Office Manager on page 119.

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.

Related links

Certificate Maintenance on page 81

Comments on this document?

Part 3: VoIP Security

Chapter 14: 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, 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 signaling 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 signaling 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/ signaling – must be secure for the call to be secure end to end.

Related links

IP Office Platform Media Security

IP Office supports both SRTP and IPsec for VoIP media security.

- IP Office's IPsec feature can be utilized, but it is not recommended as it limited to the IP500 V2 platform and uses a legacy key exchange mechanism (IKEv1).

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

  - IP Office , SIP and SM lines

  - Avaya H.323 extensions: 9608, 9611, 9621, 9641

  - Avaya SIP extensions: 9608, 9611, 9621 and 9641 (in centralized branch deployments), 1100 Series, 1200 Series, B179, E129, H175, J100 Series, K100 Series (Vantage), Scopia XT series

  - 3rd Party SIP extensions that 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 overrides, including encryption and authentication settings. The SRTP operation control has the following values:

Option	Description
Disabled	SRTP is not available
Preferred	Always offer both SRTP and RTP and given a choice, choose SRTP.
Enforced	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**.

Notes

- For calls using Dial Emergency, the **Enforce** setting is ignored if SRTP connection cannot be established.

- Where SIP soft clients connect to IP Office in simultaneous-registration mode (that is, another device is registered for the same user), they do 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

- Each leg of a call is regarded independently by IP Office for SRTP control; the appropriate SRTP Line or Extension setting will determine the support by each leg. Conferencing or recording of calls with SRTP legs by IP Office will retain SRTP wherever possible.

- In order to provide complete call security, the SRTP key exchange also requires to be secured.

Related links

VoIP Security on page 85

VoIP Signaling Security

Securing the signaling 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	Additional configuration is required to enable H.323-TLS.

Table continues…

Link Type	Key Security Mechanism	Notes
	H.323-Annex H	No additional configuration required

This does not secure the complete H.323 signaling channel, just the registration, key exchange and dialed digits. |
| **Avaya SIP extensions** | SIP-TLS | Additional SIP registrar configuration is required to enable SIP-TLS |

For SIP extensions, the relevant LAN's SIP registrar layer 4 protocol setting should be configured to enable the TLS protocol. SIP-TLS requires the administration of certificates; see Certificates and Trust on page 40.

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** > **VoIP Security** > **Strict SIPS** when active, causes IP Office to reject any 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 on page 161.

For information on 9608, 9611, 9621 and 9641 H323 secure phone provisioning, see Secure Provisioning of 9600 Series H.323 Phones on page 171.

For further details, see the relevant client documentation.

Related links

VoIP Security on page 85

Endpoint Provisioning Security

When either media or signaling 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.

For Endpoint support of secure remote provisioning, see IP Office VoIP Endpoint Security on page 161.

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.

Related links

VoIP Security on page 85

SRTP Performance & Capacity

SRTP is more processing intensive than RTP. As a result, when SRTP calls are routed through the IP Office system, the systems concurrent call capacity is reduced. On an IP500 V2 the reduction is 66%, on a Linux-base server the reduction is 50%. Refer to the [Avaya IP Office™ Platform Guidelines: Capacity](#)

These reductions only occur when the media stream terminates or originates on IP Office. For that reason, it is important to use direct media wherever possible.

SRTP direct media only occurs when, in addition to normal direct media requirements, both the external endpoints SRTP capabilities match. If they do not match, the IP Office handles the connection to both endpoints as SRTP non-direct media. This reduces the systems concurrent call capacity by two.

The following recommendations must be followed as a starting point:

- Enable both RTP encryption and authentication. Some endpoints will not negotiate at all if either is off.
- Set RTP encryption/authentications to AES-128/CTR plus SHA-1/80.
- Set RTCP encryption off. Some systems, including Avaya Communication Manager, do not support RTCP encryption.
- If possible, configure all SIP extensions for best effort (capability negotiation or 'cap-neg'). This allows the IP Office settings to dictate SRTP behavior.
    - Note: The auto-generated configuration files that IP Office provides to 1100/1200 Series and B179 phones always indicates to the phones to do best effort, even if the IP Office SRTP configuration is set to **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.
- All direct media settings on.
- Ensure that the default codec selections always include G711.

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

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

Related links

[VoIP Security](#) on page 85

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 on page 153.

Related links

VoIP Security on page 85

Session Border Controllers & IP Office

A Session Border Controller (SBC) is a system component evolved to add security and interoperability between SIP endpoints and call servers like IP Office. In addition to security and interoperability, SBCs like Avaya's Session Border Controller for Enterprise (Avaya SBCE) add further features such as resilience and edge proxy services.

IP Office supports many SBC features; it is important to understand the differences between Avaya SBCE and IP Office when designing a deployment. For the strongest security posture, implementation of the Avaya SBCE is recommended as a best practice.

The following table summarizes the differences between IP Office and Avaya SBCE:

SBC Feature	IP500 V2	IP Office Linux	ASBCE
Security			
Customized hardened OS	–	✓	✓
Deployment within DMZ [1]	–	–	✓
Requires external firewall [2]	✓	✓	✓
Internal firewall[3]	✓	✓	✓
Secure Media[4]	✓	✓	✓
Secure Signaling[5]	✓	✓	✓
TLS server name checks	–	–	✓
Secure Settings files	✓	✓	✓
Denial of Service resistance – ICMP, TCP, SIP	–/✓/✓	✓/✓/✓	✓/✓/✓
Denial of Service resistance – TLS	–	✓	–
Denial of Service resistance – H323	✓	✓	–
Distribute Denial of Service resistance	–	✓	✓
Port scan blocking	–	–	✓
Toll Fraud detection/prevention	✓	✓	–
Time of Day and Day of Week detection filters	–	–	✓

Table continues…

SBC Feature	IP500 V2	IP Office Linux	ASBCE
Brute force login resistance[6]	✓	✓	–
Topology hiding	✓	✓	✓
Message rate limiting	–	✓	✓
SIP protocol scrubbing	✓	✓	✓
H323 protocol scrubbing	✓	✓	–
SIP UA whitelist	–	✓	✓
SIP UA blacklist	–	✓	✓
Configurable IP Address whitelist	✓	✓	✓
Configurable IP Address blacklist	–	–	✓
Dynamic IP Address blacklist	✓	✓	✓
Interoperability			
SIP UDP/TCP/TLS	✓	✓	✓
H323 UDP/TCP/TLS	✓	✓	–
WebRTC	–	✓	✓
Media transcoding	✓	✓	✓
Media anchoring	✓	✓	✓
NAT traversal	✓	✓	✓
Signaling adaptation	✓	✓	✓
IPv4/IPv6 support	✓ /–	✓ /–	✓ / ✓
VLAN support	–	✓	✓
MS Teams certification	–	–	✓
DevConnect support	✓	✓	✓
HTTP Reverse proxy[7]	–	–	✓
Quality, Availability			
Single server HA-resilience	–	✓	✓
Dual server geo-resilience	–	✓	✓
Alternate SIP routing	✓	✓	✓
RTCPMON support	✓	✓	✓
Media connection preservation	✓	✓	✓
RTP QoS events & alarms	✓	✓	–

Notes

1. IP Office does not have sufficient port/service separation for DMZ placement.
2. External firewall should always be used.
3. Limited IP Office Linux firewall.
4. IP Office does not support AES-256 SRTP.

5. IP500 V2 does not support TLS GCM ciphers.

6. IP Office brute force login resistance should be disabled when routing via an SCB. ASBCE Call Walking feature may provide some resistance in certain situations.

7. IP Office Subscription provides HTTP reverse proxy for management only (RSS feature).

Related links

[VoIP Security](#) on page 85

VoIP Security Planning Considerations

Secure media and signaling 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 signaling using IP Office, the following should be reviewed:

- The use of a Session Border Controller. See [Session Border Controllers & IP Office](#) on page 90. If Avaya's SBC for Enterprise is used, the security level on each side of the SBC must match. SRTP or SIP-TLS must be implemented on both side of the SBC.

- The IP Office SRTP feature supports media security natively without license or IP infrastructure requirements, but can add extra interoperation complexity with various endpoints.

- Signaling security (SIP-TLS) must be considered whenever SRTP is used. Signaling security can be considered on its own as a security improvement mechanism.

- Secure phone provisioning (HTTPS) must be considered whenever media or signaling security is considered.

- Signaling security or Secure phone provisioning require the administration and maintenance of an identity certificate and it's root CA certificate on the IP Office and SBC.

- When VoIP endpoint resilience is active with secure signaling or provisioning, the root CA certificate for both home and backup server must be the same.

- 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.

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

- [Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager](#)

- [Administering Centralized Users for an IP Office™ Platform Enterprise Branch](#)

- [Avaya IP Office™ Platform in a Branch Environment Reference Configuration](#)

Related links

Part 4: Securing

Chapter 15: 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.

Related links

Comments on this document?

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 Avaya one-X® Portal for IP Office
- 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

Related links

[Securing the IP Office Platform Solution](#) on page 95

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

Related links

[Securing the IP Office Platform Solution](#) on page 95

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, IP Office 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, IP Office Manager and the system will always attempt to use a secured link for configuration and security settings exchanges.

Related links

[Securing the IP Office Platform Solution](#) on page 95

Change Security Details

About this task

All default passwords must be changed to a unique and 'strong' password. See [Password and PIN Management](#) on page 32 for more information on password strength.

Procedure

1. In IP Office Manager security settings **General** tab:

2. For **Security Administration** account:

   a. Change **Password** to a 'strong' password of 8 or more characters.

   b. Set **Minimum Password Complexity** to **High**.

3. Change service user account 'Administrator' password to a 'strong' password of 8 or more characters.

4. 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 (that is, during customer/ engineering Installation).

5. Change the System, VM Pro and Monitor passwords to 'strong' passwords of 8 or more characters.

Related links

[Securing the IP Office Platform Solution](#) on page 95

Remove Unnecessary Accounts

About this task

All unnecessary administration and IP Office user accounts should be removed or disabled to reduce the likelihood of forgotten default accounts being used for unauthorized access. Any remaining accounts must have their passwords changed. See [User Accounts and Rights of Access](#) on page 26 for more information on the differing account types and locations.

Procedure

1. In IP Office Manager security settings **Service Users** 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 Users**, change password to a strong one of 8 or more characters. If using Server Edition, see [Securing Server Edition Servers](#) on page 109 for alternative Service User administration using IP Office Web Manager.

Comments on this document?

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.

Related links

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(s)	Notes
TFTP Server	IP Office Manager Upgrade Phone Manager DECT R4* LegacyVoicemail 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 IP Office Manager.
TFTP Directory Read	Phone Manager DECT R4* TAPI Install**	Also used for legacy applications: IP DECT*, Analog DECT. * 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.

Table continues…

Application Control	Affected Application(s)	Notes
TAPI	TAPI Link Lite (1st party TAPI) TAPI Link Pro (3rd party TAPI) Avaya Contact Center Select	Enable only when TAPI required; note that TAPI driver installation will fail if the TAPI interface is not active. This setting will affect the ACCS CTI Link; when inactive, any ACCS sessions will require TLS and a trusted certificate from ACCS. This setting will not affect the Avaya one-X® Portal for IP Office CTI Link.
HTTP Directory Read	IP Office Centralized Directory J129*	Enable only when J129 or IP Office Centralized Directory used. Access only via HTTPS. HTTP port 80 must be disable. * When inactive, any J129s operate but without the directory feature
HTTP Directory Write	J129*	Enable only when J129. Access only via HTTPS. HTTP port 80 must be disabled. * When inactive, any J129s operate but without the directory feature

Related links

[Securing the IP Office Platform Solution](#) on page 95

Ensure Minimum Rights of Access

About this task

Restrict Service Users' rights of access to the minimum necessary. See [User Accounts and Rights of Access](#) on page 26 for more information on the differing access levels.

Procedure

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(s)	Service Security Level	Notes
Configuration	IP Office Manager, Configuration Web Service (DevConnect)	**Secure, Medium**	Should always be enabled
Security Administration	IP Office Manager	**Secure, Medium**	Should always be enabled
System Status Application Interface	SSA	**Secure, Medium**	Disable if SSA not present
Enhanced TSPI	Avaya one-X® Portal for IP Office	**Secure, Medium**	Disable if Avaya one-X® Portal for IP Office not present
HTTP	H323 Phones Embedded File Manager (HTTP only), IP Office Softphone SysMonitor Voicemail Pro (HTTPS only) IP Office Line	–	Controls the IP Office HTTP server. Disable if not required. If just HTTPS required, set to Secure, Medium. If HTTP must be enabled, set the **System** > **System** > **Avaya HTTP Clients Only** setting active to reject all non-Avaya clients.
Web Services	IP Office Web Manager	**Secure, Medium**	Disable if Web Management or System Manager (SMGR) not used
External	Voicemail Pro, Avaya one-X® Portal for IP Office, 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.

Related links

[Securing the IP Office Platform Solution](#) on page 95

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 IP Office 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:

	Settings
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.
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 on page 32 for more information.

Related links

Securing the IP Office Platform Solution on page 95

Update Certificates

Procedure

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

2. If required, administer a new platform identity certificate:

   a. The new identity certificate should be in a `'p12'` or `'pfx'` file.

   b. Ideally, all certificates used to sign the new identity certificate should be in the same file.

   c. If the signing certificates are in separate files, use IP Office Manager security **System** > **Certificates** > **Trusted Certificate Store** > **Add** to upload each one.

   d. Activate the IP Office Manager security setting **System** > **Certificates** > **Identity Certificate** > **Offer ID Certificate Chain**.

   e. Use IP Office Manager security setting **System** > **Certificates** > **Identity Certificate** > **Set** to upload the identity certificate file.

   f. The identity certificate will be automatically propagated to all TLS/HTTPS interfaces of the server, any signing certificates will be placed in the Trusted Certificate Store (TCS).

   g. If a separate telephony identity certificate is required, it should be administered using IP Office Manager security settings.

   h. The 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 IP Office Manager or IP Office Web Manager's File Manager.

3. Any default certificates to be trusted by IP Office should be added to the `system/primary/certificates/tcs/add` directory. See [Default Trusted Certificates](#) on page 141 for more information and how to create the certificate files.

4. If there is a change to the server's LAN IP address, SIP domain or FQDN, the Identity certificate will require regeneration. An IP500 V2, Secondary or Linux Expansion Server will always require manual regeneration. A Primary or Linux Application Server will be automatic if the IP Office Web Manager menu **Platform View** > **Settings** > **General** > **Certificates** > **Renew automatically** setting is active (default).

5. After ensuring that all other IP Office components' identity certificates are correctly configured, set the received certificate check levels using the settings:

   • **System** > **Certificates** > **Received Certificate Checks (Management Interfaces)**

   • **System** > **Certificates** > **Received Certificate Checks (Telephony Endpoints)**

Related links

[Securing the IP Office Platform Solution](#) on page 95

Securing Telephony Users & Extensions

About this task

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

Procedure

1. All unused users should be deleted – except NoUser.

2. The following auto-create settings must be disabled when not required:

   - **LAN1/LAN2** > **VoIP** > **H323 Gatekeeper** > **Auto-create Extn**
   - **LAN1/LAN2** > **VoIP** > **H323 Gatekeeper** > **Auto-create User**
   - **LAN1/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 these settings are automatically deactivated 24 hours after being set to avoid inadvertent exposure.

4. If no H.323 extensions are supported, the **System** > **LAN1/2** > **VoIP** > **H.323 Gatekeeper Enabled** must be 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 **System** > **LAN1/2** > **VoIP** > **H.323 Gatekeeper** > **H.323 Remote Extn Enabled** 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 **System** > **LAN1/2** > **VoIP** > **SIP Registrar Enabled** 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 **System** > **LAN1/2** > **VoIP** > **SIP Registrar** > **SIP Remote Extn Enabled** 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 Test**. For more information, see Password and PIN Management on page 32.

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 must be followed.

11. All SIP extensions' **Extension** > **Extn** > **Force Authorization** 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** > **User Portal** interface features enabled, all others disabled:

15. If different from the system-wide setting, change the **Extn** > **VoIP** > **Media Security** setting. See VoIP Security on page 85.

16. 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. To force settings file provision to be HTTPS, change the security settings **Services** > **HTTP** setting, see Ensure Minimum Rights of Access on page 100. This will additionally require certificate administration, see Certificates and Trust on page 40.

Related links

Securing the IP Office Platform Solution on page 95

Hardening for Remote Workers

About this task

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.

Procedure

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.

   • **LAN1/2** > **VoIP** > **Port Number Range** > **Maximum**
   • **LAN1/2** > **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 on page 85. 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 on page 40.

5. SRTP for media security should be considered, see VoIP Security on page 85.

6. If any H323 Gatekeeper or SIP registrar is exposed directly or indirectly to an unsecure network, all remote worker's **Extension** > **Extn** > **Phone Password** must be set. The code

Comments on this document?

must not be a sequence, repeated digits, or same as the extension number. It must not be less than 9 digits, preferably 13 digits.

7. Each H323 or SIP 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. The steps of Securing Telephony Users & Extensions must be followed.

9. The steps of Preventing Unwanted Calls must be followed.

10. A Session Border Controller (SBC) must be considered for enhanced SIP remote worker security – the Avaya SBC for Enterprise (ABSCE) is a solution specifically tailored for IP Office SIP remote workers and SIP trunks. For more information, refer to Deploying Remote IP Office SIP Phones with an ASBCE.

    • If an SBC or SIP Application Level Gateway (ALG) is deployed, some of the IP Office security measures must be moved from the IP Office to the SBC/ALG; the IP Office source IP address blacklisting should be disabled with the No User Source Number 'B_DISABLE_SIP_IPADDR'. The SBC/ALG black/white listing must be activated to compensate.

Related links

Securing the IP Office Platform Solution on page 95

Securing Trunks/Lines

About this task

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

Procedure

1. If using SIP trunks, IP Office must be connected externally via a properly configured Firewall; see Limiting IP Network Exposure on page 128 for more information. IP Office must never be connected directly.

2. Unless SIP trunks are configured for a particular LAN interface, the **System** > **LAN1/2** > **VoIP** > **SIP Trunks 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.

- • If an SBC or SIP Application Level Gateway (ALG) is deployed, some of the IP Office security measures must be moved from the IP Office to the SBC/ALG; the IP Office source IP address blacklisting should be disabled with the No User Source Number 'B_DISABLE_SIP_IPADDR'. The SBC/ALG black/white listing must be activated to compensate.

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** > **Allow Analog Trunk to Trunk Connect**.

6. Other changes to restrict calls are contained in Preventing Unwanted Calls.

7. IP Office Lines (SCN trunks) may be secured using the **Line** > **Line** > **Transport Type** of **WebSocket Client** or **WebSocket 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 on page 40 for more information.

8. For Server Edition deployments, Secure IP Office Lines should always be used.

Related links

Securing the IP Office Platform Solution on page 95

Securing 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 signaling security.

For more information, see Certificates and Trust on page 40. This should be reviewed prior to enabling any IP Office VoIP media security.

Related links

Securing the IP Office Platform Solution on page 95

Securing CTI Interfaces

Procedure

1. If not required, disable TAPI Link Lite/Pro (1st /3rd party TAPI) as per Disable Unused Services/Interfaces.

2. To secure the link between ACCS 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 ACCS.

3. Administer ACCS with an identity certificate. See the relevant ACCS documentation.

4. Administer the IP Office Trusted Certificate Store (TCS) with the root CA certificate of the ACCS.

Related links

[Securing the IP Office Platform Solution](#) on page 95

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 Avaya one-X® Portal for IP Office 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 unauthorized access

- Any backup/restore mechanism itself should be secure; IP Office, Voicemail Pro and Avaya one-X® Portal for IP Office support secure backup/restore options such as HTTPS and SFTP

- Access to call recordings which are held as files on servers such as Voicemail Pro 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 organization.

Related links

[Securing the IP Office Platform Solution](#) on page 95

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 IP Office 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 on page 121and Securing SysMonitor on page 122.

SNMP should not be used as this is not secure.

- Enabling security on these interfaces will increase the software processing of the IP Office and will be unsuitable for instances where high traffic is expected. In this instance local monitoring via unsecured interfaces or external secure solution are required. See Limiting IP Network Exposure on page 128.

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

Related links

Securing the IP Office Platform Solution on page 95

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.

Related links

Securing the IP Office Platform Solution on page 95

Securing Server Edition Servers

Procedure

1. It is important to understand the information and recommendations of Certificates and Trust 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 Avaya one-X® Portal for IP Office, 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 settings **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 IP Office Web Manager Security Manager Service Users | Synchronize Service User and System Password.

5. Apply a password policy to the Web Control application using IP Office Web Manager menu **Platform View** > **Settings** > **System Settings** > **Password Rules** settings.

6. Enable the setting IP Office Web Manager menu **Platform View** > **Settings** > **System Settings** > **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 IP Office Web Manager setting **Platform View** > **Settings** > **System Settings** > **Enable HTTP file store for backup/restore**. 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 IP Office Web Manager setting **Platform View** > **Settings** > **System Settings** > **Firewall Settings**.

   • Note: The firewall support on Server Edition does not replace the need for an external firewall. For further information see [Limiting IP Network Exposure](#) on page 128.

9. Disable any unused unsecure TCP or UDP ports using IP Office Web Manager setting **Platform View** > **Settings** > **System Settings** > **Firewall Settings** settings. 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 View** > **Settings** > **System Settings** > **Firewall Settings** > **Enable Filtering** 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 server's **Platform View** > **Settings** > **General** tab.

12. If not required, remove the syslog client on the Secondary and each Expansion System using the IP Office Manager setting **System** > **System Events** > **Alarms** > **Syslog**.

    • Removing the syslog destination will stop audit trail and security events being sent to the Primary Server.

13. If not required, disable the Enhanced Access Security Gateway (EASG) support using the IP Office Web Manager setting **Platform View** > **Settings** > **General** > **EASG Settings** > **Status**.

14. If required, administer a new server identity certificate using IP Office Web Manager:

    a. The new identity certificate should be in a 'p12' or 'pfx' file.

    b. Set **Platform View** > **Settings** > **General** > **Certificates** > **Renew automatically**.

     c. Ideally, all certificates used to sign the new identity certificate should be in the same file.

     d. If the signing certificates are in separate files, use **Certificates** > **Add** to upload each one.

     e. Set **Certificates** > **Offer ID Certificate Chain** active.

     f. Use **Certificates** > **Offer ID Certificate Chain** > **Set** to upload the identity certificate file.

     g. The identity certificate will be automatically propagated to all TLS/HTTPS interfaces of the server, any signing certificates will be placed in the Trusted Certificate Store (TCS). For more information, see [Certificates and Trust](#) on page 40 on page 33.

15. Follow [Securing the IP Office Platform Solution](#) on page 95.

     a. If Voicemail Pro is installed, follow [Securing Voicemail Pro](#) on page 123.

     b. If Avaya one-X® Portal for IP Office is installed, follow [Securing Avaya one-X Portal for IP Office](#) on page 125.

     c. Any applications not used should be disabled using the **Platform View** > **System** > **Services** > **Automatically Start**. Note that IP Office and Management Services should never be disabled.

16. Do not activate the server's Intelligent Platform Management Interface (IPMI) – this effectively grants physical access to the server.

Related links

[Securing the IP Office Platform Solution](#) on page 95

Securing Linux Application Server

About this task

The Linux Application Server runs 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.

Procedure

1. It is important to understand the information and recommendations of Certificates and Trust 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 Avaya one-X® Portal for IP Office, Voicemail Pro and Web Control (the local Linux administration web interface).

3. Apply a password policy to the Web Control application using IP Office Web Manager menu **Platform View** > **Settings** > **System Settings** > **Password Rules** settings.

4. Enable the setting IP Office Web Manager menu **Platform View** > **Settings** > **System Settings** > **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.

5. Use IP Office Manager to load the security settings of the IP Office Shell Server that co-resides on the Linux Application Server at the same IP address.

6. Follow Securing the IP Office Platform Solution on page 95.

7. Disable the HTTP backup/restore server using IP Office Web Manager setting **Platform View** > **Settings** > **System Settings** > **Enable HTTP file store for backup/restore**. An HTTPS backup/restore server is always active for this purpose.

8. Disable any unused unsecure ports/protocols using **Platform View** > **Settings** > **System Settings** > **Firewall Settings**. This will apply filtering to all LAN 1 and LAN 2 traffic, regardless of source or destination.

   • The firewall support on the Linux Application Server do not replace the needs for an external firewall. For further information see Limiting IP Network Exposure on page 128.

9. If not required, disable the Enhanced Access Security Gateway (EASG) support using the IP Office Web Manager setting **Platform View** > **Settings** > **General** > **EASG 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 Linux Application Server, the **Platform View** > **General** > **Certificates** > **Identity Certificates** settings can be used. For more information, see Certificates and Trust on page 40.

11. If required, administer a new server identity certificate on the IP Office Shell Server using the IP Office Manager **Certificates** > **Offer ID Certificate Chain** > **Set**; this identity certificate will be automatically propagated to all TLS/HTTPS interfaces of the server.

12. If Voicemail Pro is installed, follow Securing Voicemail Pro on page 123.

13. If Avaya one-X® Portal for IP Office is installed, follow Securing Avaya one-X® Portal for IP Office.

14. Any applications not used should be disabled using the **Platform View** > **System** > **Services** > **Automatically Start**. Note that IP Office and Management Services should never be disabled.

15. Do not activate the server's Intelligent Platform Management Interface (IPMI) – this effectively grants physical access to the server.

Related links

Securing the IP Office Platform Solution on page 95

Chapter 16: 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:

Related links

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 dialed 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.

Related links

User Based Barring

There are several potential methods for achieving different routing/barring rules for Users.

One effective method that minimizes the per-user config, and can be part of user rights templates, centralizes 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
XXXXXXXXXXN	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 and so on. Short codes can be added for areas where 7 digit local dialing is still available if required, also it might be useful to create Short Codes to trap local Area Codes that have been dialed with a leading 1, also Freephone dialing.

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
XXXXXXXXXXN	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 dialing matching a simple "1N;" short code. The barring for *67 and *82 is repeated.

The Unrestricted ARS short codes will be:

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

This is totally unrestricted, in real operation it is unlikely that there will be totally unrestricted out-dialing.

The Default system short code for dialing is Unchanged:

Add specific User Short Codes for users who are allowed greater dialing 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 ARS tab in Administering Avaya IP Office™ Platform with Manager.

Related links

Protecting Phones

In some environments, one of the risks is not from the phones users, but from other people having physical access to the phones when unattended. There are several mechanisms you can use to protect the phone when the user is away from their desk:

Feature	Description
Phone Lock	Phones can be locked using the Lock feature on the phone Features menu. Locking the phone also locks the Features menu. The 9500, 9600 and J100 Series phones have an option to specify an inactivity timer after which the phone locks itself.
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 user's 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 **User** > **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 uncontrolled 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.

Related links

Making Calls from Protected Phones

Once phones have outbound dialing 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 Dialing has been correctly defined.

Related links

Preventing Unwanted Calls on page 113

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**.

Related links

Preventing Unwanted Calls on page 113

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 judgment made to decide if the benefit is worth the risk of unauthorized access.

Related links

Preventing Unwanted Calls on page 113

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. The call will be zero duration, zero ring time, with the word 'Barred' in the 2nd party info field.

Related links

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.

Related links

Chapter 17: Securing IP Office Applications

To help secure IP Office applications, use the following recommendations:

Related links

Securing IP Office Manager

Procedure

1. Apply the following configuration settings in IP Office Manager using the **File** > **Preferences** > **Security** tab to ensures more secure IP Office communications and help keep configuration data away from unauthorized users:

Configuration	Parameter Settings
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 Checks** 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](#) on page 40 and [Windows Certificate Management](#) on page 149.

4. If mutual certificate authentication is required (that is, the IP Office configuration or security administration service will request a certificate from IP Office Manager) the **File** > **Preferences** > **Security** > **Certificate offered to IP Office** needs to be set with an identity certificate. 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** to be different to the **Binary Directory**. 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.

Related links

[Securing IP Office Applications](#) on page 119

Securing IP Office Web Manager/Web Control

About this task

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

Procedure

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](#) on page 40.

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

Related links

[Securing IP Office Applications](#) on page 119

Securing Web Licence Manager

About this task

Web License Manager (WebLM) administrative accounts 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.

Procedure

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 on page 32).

3. For subsequent password management, go to the WebLM 'Manage Users' page. Any unused administrator accounts must be deleted.

   • Note: WebLM does not support referred authentication; local user accounts are used at all times.

4. Any browser used for web-based management should have the CA certificate/ID certificate of the IP Office installed in the relevant trusted certificate store. It is possible in some browsers to provide temporary or permanent exceptions, but this should be avoided. For more information about certificates and browser support, see Certificates and Trust on page 40.

5. If the application is not used, it should be disabled using the **Platform View** > **System** > **Services** > **Automatically Start** setting.

Related links

Securing IP Office Applications on page 119

Securing System Status Application

About this task

System Status Application 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.

Procedure

1. To prevent the use of the unsecure connection, the IP Office Manager security setting **Services** > **System Status Application Interface** > **Service Security Level** should be set to **Secure, Low** or **Secure, Medium**.

   • Note: The use of SSA with a TLS connection limits 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 Application** > **Read all configuration** and **Rights Groups** > **System Status Application** > **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.

Related links

Securing SysMonitor

About this task

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

Procedure

1. A Service User account should be used rather than the legacy Monitor Password, the IP Office Manager security using the setting **System** > **Unsecured Interfaces** > **Use Service User Credentials**. For default accounts that can use SysMonitor in this way, see Default Administrative Users and Rights Groups on page 27.

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 IP Office 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](#) on page 40.

4. To ensure only HTTPS is used, the IP Office 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,IP Office SoftConsole, Voicemail Pro and Avaya one-X® Portal for IP Office.

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.

Related links

[Securing IP Office Applications](#) on page 119

Securing Voicemail Pro

Procedure

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.

   • For Server Edition and Linux Application Server, all authentication is referred to the 'local' IP Office – the default administration account is only used under failure conditions. For Linux Application Server, the local IP Office is a management instance running on the server itself. See [User Accounts and Rights of Access](#) on page 26 for more information.

2. Using the Voicemail Pro client, configure the password using **Preferences** > **General** > **Voicemail Password**. This password must match the password entered in the IP Office Manager setting **Security** > **System** > **Unsecured Interfaces** > **Voicemail Password**. The password must be 31-characters.

   • For new systems, a suitable 31-character password is automatically generated and used on the first connection between the IP Office and Voicemail Pro services.

   • Existing systems upgraded to IP Office R11.1 FP1 can continue to use their existing shorter password but are forced to a 31-character password on any change.

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.

   • Disabling the mailbox will also disable IMAP, MAPI, email and Web Voicemail integrations for that user

5. All mailboxes must be protected by a **Voicemail Code**, except when connecting from trusted extensions (by the use of the **User** > **Source Numbers**). The recommended minimum is 4 digits for internal use, 9 when the mailbox can be accessed externally.

6. The mailbox **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 IP Office Manager setting **System** > **Voicemail** > **Voicemail Code Complexity**.

   • Note: If IP Office voicemail TUI is used, the users are not forced to set a new **Voicemail Code** on initial mailbox access.

7. To prevent Toll fraud via the outdialing feature, it can be disabled on the IP Office configuration **System** > **Voicemail** tab in IP Office Manager. Where outcalling is required, call barring steps must be used, see [Preventing Unwanted Calls](#) on page 113.

8. To prevent Toll fraud via call flows, all call flows must have adequate protection against dialing unauthorized numbers. Where external calling is required, call barring steps must be used. See [Preventing Unwanted Calls](#) on page 113

9. Where a phone is in an uncontrolled area, the default Trusted Source Number for Voicemail access should be removed, so that all IP Office voicemail access requires entering the **Voicemail 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, authentication should be used. TLS is always enforced.

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

14. If the application is not used, it should be disabled using the Web Control Settings **Platform View** > **System** > **Services** > **Automatically Start** setting.

Related links

[Securing IP Office Applications](#) on page 119

Securing Embedded Voicemail

Procedure

1. Only users and groups that are entitled to use voicemail should have their mailbox activated.

2. All mailboxes must be protected by a **Voicemail Code**, except when connecting from trusted extensions (by the use of the **User** > **Source Numbers**). The recommended minimum is 4 digits for internal use, 9 when the mailbox can be accessed externally.

3. The mailbox **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 IP Office Manager setting **System** > **Voicemail** > **Voicemail Code Complexity**.

   • Note: If IP Office voicemail TUI is used, the users are not forced to set a new **Voicemail Code** on initial mailbox access.

4. Where a phone is in an uncontrolled area, the default Trusted Source Number for Voicemail access should be removed, so that all IP Office Voicemail access requires entering the **Voicemail Code**, even from the user's home extension.

Related links

Securing IP Office Applications on page 119

Securing Avaya one-X® Portal for IP Office

Procedure

1. Log in to the default Avaya one-X® Portal for IP Office Administrator account and change the password to a strong password of 8 or more characters.

   • This account is used by Avaya one-X® Portal for IP Office if IP Office referred authentication service is not available, see User Accounts and Rights of Access on page 26 for more information.

2. For subsequent password management, go to the Avaya one-X® Portal for IP Office **Configuration** > **User** page. Any unused administrator accounts must be deleted.

3. On the Avaya one-X® Portal for IP Office 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 `EnhTcpaService`.

4. If Avaya one-X® Portal for IP Office clients are to be used externally, follow Hardening for Remote Worker Operation.

5. If external Avaya one-X® Portal for IP Office clients are configured to support VoIP calls, follow Limiting IP Network Exposure.

6. Avaya one-X® Portal for IP Office 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 on a Linux-based server, see [Update Certificates](#) on page 102.

8. 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 Avaya one-X® Portal for IP Office AFA page **Configuration** > **Edit** page.

9. If the host server operating system is Microsoft Windows, consult the relevant Microsoft OS security guidelines at https://technet.microsoft.com/en-us/library/windows-server-security.aspx. For more general information, see https://technet.microsoft.com/en-us/security/default.aspx

10. The Openfire console should not normally be enabled. If in exceptional circumstances, it is enabled under the direction of Avaya, then it must be disabled as soon as possible afterwards. The command to disable is at: http://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/oneXportaladmin/diabling_openfire_admin_consol.htm

11. If the application is not used, it should be disabled using the **Platform View** > **System** > **Services** > **Automatically Start** setting.

Related links

[Securing IP Office Applications](#) on page 119

Securing WebRTC Gateway

Procedure

If the application is not used, it should be disabled using the **Platform View** > **System** > **Services** > **Automatically Start** setting.

Related links

[Securing IP Office Applications](#) on page 119

Securing Media Manager

Procedure

1. If the application is not used, it should be disabled using the **Platform View** > **System** > **Services** > **Automatically Start** setting.

2. If SMTP emails are used for alarms and events, in IP Office Web Manager select **Applications** > **Media Manager** > **Configuration** > **Secured Connection**.

3. If connectors to external archiving are used, select **Encrypt Recording** in the connector settings unless the archive location complies with local data protection and privacy requirements.

Related links

[Securing IP Office Applications](#) on page 119

Securing Avaya Contact Center Applications

Procedure

1. Whenever Avaya Contact Center Select (ACCS) is deployed with IP Office, the CTI link between IP Office and the application should be secured, see [Securing CTI Interfaces](#) on page 108.

2. Refer to the relevant application documentation for all other security aspects: *Avaya Contact Center Select Solution Description*

Related links

[Securing IP Office Applications](#) on page 119

Chapter 18: 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 (for example, 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 IP Office 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 DCHP settings modified to prevent re-occurrence.

Related links

Firewalls

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.

Related links

[Limiting IP Network Exposure](#) on page 128

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.

- If an SBC or SIP Application Level Gateway (ALG) is deployed, some of the IP Office security measures must be moved from the IP Office to the SBC/ALG; the IP Office source IP address blacklisting should be disabled with the No User Source Number 'B_DISABLE_SIP_IPADDR'. The SBC/ALG black/white listing must be activated to compensate.

Related links

[Limiting IP Network Exposure](#) on page 128

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 Avaya 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.

Related links

[Limiting IP Network Exposure](#) on page 128

Part 5: Monitoring

Chapter 19: 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.
- 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

Related links

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:

- 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, that is, 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 (for example, 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 at https://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/general/port_matrix/index.htm.

Port	Protocol	Use	Possible Test Tool/Notes
22	TCP	SSH	SSH, port scanner. Linux servers only
69	UDP	TFTP	Port scanner. A TFTP RRQ of 'nasystem/who_is' can be used
80	TCP	HTTP	Browser, port scanner. `http://[ IP Address]` can be used
143	TCP	IMAP	Port scanner. Voicemail Pro only
161	UDP	SNMP	SNMP test tool, port scanner
411	TCP	HTTP	Port scanner
443	TCP	HTTPS	Browser, port scanner. `https://[ IP Address]` can be used
993	TCP	IMAP-TLS	Port scanner. Voicemail Pro only
1300	TCP	H323-TLS	Port scanner
1720	TCP	H323	Port scanner.
5060	UDP	SIP	Port scanner.
5061	TCP	SIP	Port scanner.
5443	TCP	HTTPS	Port scanner. Linux servers only
7070	TCP	HTTPS	Browser, port scanner. Linux servers only. `https://[IP Address]:7070` can be used

Table continues…

Port	Protocol	Use	Possible Test Tool/Notes
7071	TCP	HTTPS	Browser, port scanner. Linux servers only. `https://[IP Address]:7071` can be used
8000	TCP	HTTP	Port scanner. Linux servers only
8069	TCP	HTTP	Port scanner. Avaya one-X® Portal for IP Office only
8080	TCP	HTTP	Browser, port scanner. `https://[IP Address]:8080/onexportal-admin.html` can be used
8086	TCP	HTTP	Port scanner. Avaya one-X® Portal for IP Office only
8411	TCP	HTTPS	Port scanner.
8443	TCP	HTTPS	Port scanner.
9443	TCP	HTTPS	Port scanner. Avaya one-X® Portal for IP Office only
50791	TCP		Voicemail Pro Client, port scanner
50792	UDP		Port scanner.
50793	TCP		Port scanner. IP500 V2 only
50794	UDP + TCP	SysMonitor	SysMonitor, port scanner.
50796	TCP	TLS	Port scanner.
50804	TCP		IP Office Manager, port scanner.
50805	TCP	TLS	IP Office Manager, port scanner.
50808	TCP		SSA, port scanner.
50809	TCP	TLS	SSA, port scanner.
50812	TCP		IP Office Manager, port scanner.
50813	TCP	TLS	IP Office Manager, port scanner.
50814	TCP		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	IP Office Web Manager IP Office Manager	All servers, includingIP500 V2.
Administrator	Voicemail Pro	Voicemail Pro client	Voicemail Pro only.
Administrator	Avaya one-X® Portal for IP Office	Browser	Avaya one-X® Portal for IP Office 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 on page 98 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 Authorization** setting has not been disabled.

- Check the special IP Office user 'NoUser' **Source Numbers** field; any unexpected entries should be clarified with support personnel. NoUser source numbers are sometimes used to enable specific features or behavior.

- Check that the padlock symbol is displayed on the bottom right of the screen, indicating a secure connection to IP Office.

- Use IP Office Manager to load the security settings and review all warnings; none should be present.

- Again, check that the padlock symbol is displayed on the bottom right of the screen, indicating a secure connection to IP Office.

- Log on to Avaya one-X® Portal for IP Office administration page, if a warning is displayed 'Change Administrator Default Password' the administrator account is at default.

- If login to Web Control, Avaya one-X® Portal for IP Office 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, authorization 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.

Related links

[Monitoring the IP Office Platform](#) on page 131

IP Office Reporting

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 IP Office System Status](#).

  - 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 System Status Application and IP Office Manager. Note that user/phone based changes are not currently captured. For more information see:

  - "Control Unit Audit" in [Using IP Office System Status](#).

  - **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](#).

Related links

[Monitoring the IP Office Platform](#) on page 131

Voicemail Pro Reporting

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, refer to [Administering IP Office 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.

Related links

[Monitoring the IP Office Platform](#) on page 131

Avaya one-X® Portal for IP Office Reporting

The following events and logging features are available for Avaya one-X® Portal for IP Office 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.

• Avaya one-X® Portal for IP Office client login failures are reported via the IP Office failed login alarms, see [IP Office Reporting](#) on page 135.

Related links

[Monitoring the IP Office Platform](#) on page 131

Linux-Based Server Reporting

Linux-based IP Office 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 **Platform View** > **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 **Platform View** > **Logs** > **Syslog Event Viewer** and **Platform View** > **Settings** > **General** > **Syslog**.

Related links

[Monitoring the IP Office Platform](#) on page 131

Other Components Reporting

• 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.

Related links

[Monitoring the IP Office Platform](#) on page 131

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](#) on page 139.

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

Related links

[Monitoring the IP Office Platform](#) on page 131

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](#) on page 139 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.

Related links

[Monitoring the IP Office Platform](#) on page 131

Part 6: Appendices

Chapter 20: Avaya Product Security Support

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

- Manages Avaya product vulnerabilities and threats.
- Maintains information posted at https://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

Before contacting Avaya on a security matter, please consult the Product Security Support Flow, which can be found at https://downloads.avaya.com/css/P8/documents/100161515. There is a link this document on the Avaya security support site at https://support.avaya.com/security.

When a security vulnerability is identified, the PSST determines susceptibility of Avaya products to those vulnerabilities and follows a process according to the Avaya's Product Security Vulnerability Response Policy, defined at https://downloads.avaya.com/css/P8/documents/100045520. Depending on the category of risk, the PSST creates an Avaya Security Advisory to notify customers of the vulnerability.

Related links

[Accessing Avaya Security Advisories](#) on page 139
[Interpreting an Avaya Security Advisory](#) on page 140

Accessing Avaya Security Advisories

Avaya Security Advisories are posted on the Security Support web site at https://support.avaya.com/security. Customers can register at Avaya Support web site to receive email notifications of Avaya security advisories.

Related links

[Avaya Product Security Support](#) on page 139

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 Avaya's Product Security Vulnerability Response Policy at https://downloads.avaya.com/css/P8/documents/100045520.

Related links

Chapter 21: Default Trusted Certificates

IP Office does not trust all certificate authorities by default.

Related links

Default Trusted Certificates

There are a number of certificates that are trusted by IP Office and are present on initial default and security settings reset:

Name	Duration/Thumbnail	Usage
Symantec Class 3 Secure Server CA - G4	30 October 2023 23:59:59 ff67367c5cd4de 4ae18bcce1d70fdabd7c8 66135	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.
Entrust Certification Authority - L1K	Start (yymmddhhmmss): 20151005191356Z End (yymmddhhmmss): 20301205194356Z	Required for Apple Push Notification Support and Avaya Spaces SSO

Table continues…

Default Trusted Certificates

Name	Duration/Thumbnail	Usage
GTS Root R1	Start (yymmddhhmmss): 20160622000000Z End (yymmddhhmmss): 20360622000000Z	Required for Apple Push Notification Support and Avaya Spaces SSO
GTS Root R2	Start (yymmddhhmmss): 20160622000000Z End (yymmddhhmmss): 20360622000000Z	Required for Apple Push Notification Support and Avaya Spaces SSO
GlobalSign Root CA - R2	Start (yymmddhhmmss): 20061215080000Z End (yymmddhhmmss): 20211215080000Z	Required for Apple Push Notification Support and Avaya Spaces SSO
ISRG Root X1	Start (yymmddhhmmss): 20150604110438Z End (yymmddhhmmss): 20350604110438Z	Required to trust certificates issued by Let's Encrypt, used by IP Office Containerized and Subscription systems.
DigiCert Global Root CA	Start (yymmddhhmmss): 20061110000000Z End (yymmddhhmmss): 20311110000000Z	Required for Apple Push Notification Support and Avaya Spaces SSO
DigiCert SHA2 Secure Server CA	Start (yymmddhhmmss): 20130308120000Z End (yymmddhhmmss): 20230308120000Z	Required for Apple Push Notification Support and Avaya Spaces SSO
Let's Encrypt Authority X3	Start (yymmddhhmmss): 20160317164046Z End (yymmddhhmmss): 20210317164046Z	Required to trust certificates issued by Let's Encrypt, used by IP Office Containerised

Related links

Symantec Class 3 Secure Server CA - G4 in PEM format

```
-----BEGIN CERTIFICATE-----
MIIFODCCBCCgAwIBAgIQUT+5dDhwtzRAQY0wkwaZ/zANBgkqhkiG9w0BAQsFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJp
U2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxW
ZXJpU2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0
aG9yaXR5IC0gRzUwHhcNMTMxMDMxMDAwMDAwWhcNMjMxMDMwMjM1OTU5WjB+MQsw
CQYDVQQGEwJVUzEdMBsGA1UEChMUU3ltYW50ZWMgQ29ycG9yYXRpb24xHzAdBgNV
```

```
BAsTFlN5bWFudGVjIFRydXN0IE5ldHdvcmsxLzAtBgNVBAMTJlN5bWFudGVjIENs
YXNzIDMgU2VjdXJlIFNlcnZlciBDQSAtIEc0MIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAstgFyhx0LbUXVjnFSlIJluhL2AzxaJ+aQihiw6UwU35VEYJb
A3oNL+F5BMm0lncZgQGUWfm893qZJ4Itt4PdWid/sgN6nFMl6UgfRk/InSn4vnlW
9vf92Tpo2otLgjNBEsPIPMzWlnqEIRoiBAMnF4scaGGTDw5RgDMdtLXO637QYqzu
s3sBdO9pNevK1T2p7peYyo2qRA4lmUoVlqTObQJUHypqJuIGOmNIrLRM0XWTUP8T
L9ba4cYY9Z/JJV3zADreJk20KQnNDz0jbxZKgRb78oMQw7jW2FUyPfG9D72MUpVK
Fpd6UiFjdS8W+cRmvvW1Cdj/JwDNRHxvSz+w9wIDAQABo4IBYzCCAV8wEgYDVR0T
AQH/BAgwBgEB/wIBADAwBgNVHR8EKTAnMCWgI6Ahhh9odHRwOi8vczEuc3ltY2Iu
Y29tL3BjYTMtZzUuY3JsMA4GA1UdDwEB/wQEAwIBBjAvBggrBgEFBQcBAQQjMCEw
HwYIKwYBBQUHMAGGE2h0dHA6Ly9zMi5zeW1jYi5jb20wawYDVR0gBGQwYjBgBgpg
hkgBhvhFAQc2MFIwLJgYIKwYBBQUHAgEWGmh0dHA6Ly93d3cuc3ltYXV0aC5jb20v
Y3BzMCgGCCsGAQUFBwICMBwaGmh0dHA6Ly93d3cuc3ltYXV0aC5jb20vcnBhMCkg
A1UdEQQiMCCkHjAcMRowGAYDVQQDExFTeW1hbnRlY1BLSS0xLTUzNDAdBgNVHQ4E
FgQUX2DPYZBV34RDFIpgKrL1evRDGO8wHwYDVR0jBBgwFoAUf9Nlp8Ld7LvwMAnz
Qzn6Aq8zMTMwDQYJKoZIhvcNAQELBQADggEBAF6UVkndjil19cE2UbYD49qecxny
H1mrWH5sJgUs+oHXXCMXIiw3k/eG7IXmsKP9H+IyqEVv4dn7ua/ScKAyQmW/hP4W
Ko8/xabWo5N9Q+l0IZE1KPRj6S7t9/Vcf0uatSDpCr3gRRAMFJSaXaXjS5HoJJtG
QGX0InLNmfiIEfXzf+YzguaoxX7+0AjiJVgIcWjmzaLmFN5OUiQt/eV5E1PnXi8t
TRttQBVSK/eHiXgSgW7ZTaoteNTCLD0IX4eRnh8OsN4wUmSGiaqdZpwOdgyA8nTY
Kvi4Os7X1g8RvmurFPW9QaAiY4nxug9vKWNmLT+sjHLF+8fk1A/yO0+MKcc=
-----END CERTIFICATE-----
```

Related links

[Default Trusted Certificates](#) on page 141

Entrust Certification Authority - L1K in PEM format

```
-----BEGIN CERTIFICATE-----
MIIFDjCCA/agAwIBAgIMDulMwwAAAABR03eFMA0GCSqGSIb3DQEBCwUAMIG+MQsw
CQYDVQQGEwJVUzEWMBQGA1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2Vl
IHd3dy5lbnRydXN0Lm5ldC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMDkg
RW50cnVzdCwgSW5jLiAtIGZvciBhdXRob3JpemVkIHVzZSBvbmx5MTIwMAYDVQQD
EylFbnRydXN0IEFjdb3Qg2VydGlmaWNhdGlvbiBBdXRob3JpdHkgLSBHMjAeFw0x
NTEwMDUxOTEzNTTaFw0zMDEyMDUxOTQzNTTaMIG6MQswCQYDVQQGEwJVUzEWMBQG
A1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2VlIHd3dy5lbnRydXN0Lm5l
dC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMTIgRW50cnVzdCwgSW5jLiAt
IGZvciBhdXRob3JpemVkIHVzZSBvbmx5MS4wLAYDVQQDEyVFbnRydXN0IENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5IC0gTDFLMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA2j+W0E25L0Tn2zlem1DuXKVh2kFnUwmqAJqOV38pa9vH4SEkqjrQ
jUcj0u1yFvCRIdJdt7hLqIOPt5EyaM/OJZMssn2XyP7BtBe6CZ4DkJN7fEmDImiK
m95HwzGYei59QAvS7z7Tsoyqj0ip/wDoKVgG97aTWpRzJiatWA7lQrjV6nN5ZGhT
JbiEz5R6rgZFDKNrTdDGvuoYpDbwkrK6HIiPOlJ/915tgxyd8B/lw9bdpXiSPbBt
LOrJz5RBGXFEaLpHPATpXbo+8DX3Fbae8i4VHj9HyMg4p3NFXU2wO7GOFyk36t0F
ASK7lDYqjVs1/lMZLwhGwSqzGmIdTivZGwIDAQABo4IBDDCCAQgwDgYDVR0PAQH/
BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwMwYIKwYBBQUHAQEEJzAlMCMGCCsG
AQUFBzABhhdodHRwOi8vb2NzcC5lbnRydXN0Lm5ldDAwBgNVHR8EKTAnMCWgI6Ah
hh9odHRwOi8vY3JsLmVudHJ1c3QubmV0L2cyY2EuY3JsMDsGA1UdIAQ0MDIwMAYE
VR0gADAoMCYGCCsGAQUFBwIBFhpodHRwOi8vd3d3LmVudHJ1c3QubmV0L3JwYTAd
BgNVHQ4EFgQUGqJwdN28Uz/Pe9T3zX+nYMYKTL8wHwYDVR0jBBgwFoAUanImetAe
733nO2lR1GyNn5ASZqswDQYJKoZIhvcNAQELBQADggEBADnVjpiDYcgsY9NcwHRkw
y/YJrMxp1cncN0HyMg/vdMNY9ngnCTQIlZIv19+4o/0OgemknNM/TWgrFTEKFcxS
BJPok1DD2bHi4Wi3Ogl08TRYCj93mEC45mj/XeTIRsXsgdfJghhcg85x2Ly/rJkC
k9uUmITSnKa1/ly78EqvIazCP0kkZ9Yujs+szGQVGHLlbHfTUqi53Y2sAEo1GdRv
c6N172tkw+CNgxKhiucOhk3YtCAbvmqljEtoZuMrx1gL+1YQ1JH7HdMxWBCMRON1
exCdtTix9qrKgWRs6PLigVWXUX/hwidQosk8WwBD9lu51aX8/wdQQGcHsFXwt35u
Lcw=
-----END CERTIFICATE-----
```

Default Trusted Certificates

Related links

[Default Trusted Certificates](#) on page 141

GTS Root R1 in PEM format

```
-----BEGIN CERTIFICATE-----
MIIFWjCCA0KgAwIBAgIQbkepxUtHDA3sM9CJuRz04TANBgkqhkiG9w0BAQwFADBH
MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
QzEUMBIGA1UEAxMLR1RTIFJvb3QgUjEwHhcNMTYwNjIyMDAwMDAwWhcNMzYwNjIy
MDAwMDAwWjBHMQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNl
cnZpY2VzIExMQzEUMBIGA1UEAxMLR1RTIFJvb3QgUjEwggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQC2EQKLHuOhd5s73L+UPreVp0A8of2C+X0yBoJx9vaM
f/vo27xqLpeXo4xL+Sv2sfnOhB2x+cWX3u+58qPpvBKJXqeqUqv4IyfLpLGcY9vX
mX7wCl7raKb0xlpHDU0QM+NOsROjyBhsS+z8CZDfnWQpJSMHobTSPS5g4M/SCYe7
zUjwTcLCeoiKu7rPWRnWr4+wB7CeMfGCwcDfLqZtbBkOtdh+JhpFAz2weaSUKK0P
fyblqAj+lug8aJRT7oM6iCsVlgmy4HqMLnXWnOunVmSPlk9orj2XwoSPwLxAwAtc
vfaHszVsrBhQf4TgTM2S0yDpM7xSma8ytSmzJSq0SPly4cpk9+aCEI3oncKKiPo4
Zor8Y/kB+Xj9e1x3+naH+uzfsQ55lVe0vSbv1gHR6xYKu44LtcXFilWr06zqkUsp
zBmkMiVOKvFlRNACzqrOSbTqn3yDsEB750Orp2yjj32JgfpMpf/VjsPOS+C12LOO
Rc92wO1AK/1TD7Cn1TsNsYqiA94xrcx36m97PtbfkSIS5r762DL8EGMUUXLeXdYW
k70paDPvOmbsB4om3xPXV2V4J95eSRQAogB/mqghtqmxlbCluQ0WEdrHbEg8QOB+
DVrNVjzRlwW5y0vtOUucxD/SVRNuJLDWcfr0wbrM7Rv1/oFB2ACYPTrIrnqYNxgF
lQIDAQABo0IwQDAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zAdBgNV
HQ4EFgQU5K8rJnEaK0gnhS9SZizv8IkTcT4wDQYJKoZIhvcNAQEMBQADggIBADiW
Cu49tJYeX++dnAsznyvgyv3SjgofQXSlfKqE1OXyHuY3UjKcC9FhHb8owbZEKTV1
d5iyfNm9dKyKaOOpMQkpAWBz40d8U6iQSifvS9efk+eCNs6aaAyC58/UEBZvXw6Z
XPYfcX3v73svfuo21pdwCxXu11xWajOl40k4DLh9+42FpLFZXvRq4d2h9mREruZR
gyFmxhE+885H7pwoHyXa/6xmld01D1zvICxi/ZG6qcz8WpyTgYMpl0p8WnK0OdC3
d8t5/Wk6kjftbjhlRn7pYL15iJdfOBL07q9bgsiG1eGZbYwE8na6SfZu6W0eX6Dv
J4J2QPim01hcDyxC2kLGe4g0x8HYRZvBPsVhHdljUEn2NIVq4BjFbkerQUIpm/ZG
DdIx02OYI5NaAIFItO/Nis3Jz5nu2Z6qNuFoS3FJFDYoOj0dzpqPJeaAcWErtXvM
+SUWgeExX6GjfhaknBZqlxi9dnKlC54dNuYvoS++cJEPqOba+MSSQGwlfnuzCdyy
F62ARPBopY+Udf90WuioAnwMCeKpSwughQtiue+hMZL77/ZRBIls6Kl0obsXs7X9
SQ98POyDGCBDTtWTurQ0sR8WNh8M5mQ5Fkzc4P4dyKliPUDqysU0ArSuiYgzNdws
E3PYJ/HQcu51OyLemGhmW/HGY0dVHLqlCFF1pkgl
-----END CERTIFICATE-----
```

Related links

[Default Trusted Certificates](#) on page 141

GTS Root R2 in PEM format

```
-----BEGIN CERTIFICATE-----
MIIFWjCCA0KgAwIBAgIQbkepxlqz5yDFMJo/aFLybzANBgkqhkiG9w0BAQwFADBH
MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
QzEUMBIGA1UEAxMLR1RTIFJvb3QgUjIwHhcNMTYwNjIyMDAwMDAwWhcNMzYwNjIy
MDAwMDAwWjBHMQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNl
cnZpY2VzIExMQzEUMBIGA1UEAxMLR1RTIFJvb3QgUjIwggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQDO3v2m++zsFDQ8BwZabFn3GTXd98GdVarTzTukk3Lv
CvptnfbwhYBboUhSnznFt+4orO/LdmgUud+tAWyZH8QiHZ/+cnfgLFuv5AS/T3Kg
GjSY6Dlo7JUle3ah5mm5hRm9iYz+re026nO8/4Piy33B0s5Ks40FnotJk9/BW9Bu
XvAuMC6C/Pq8tBcKSOWIm8Wba96wyrQD8Nr0kLhlZPdcTK3ofmZemde4wj7I0BOd
re7kRXuJVfeKH2JShBKzwkCX44ofR5GmdFrS+LFjKBC4swm4VndAoiaYecb+3yXu
PuWgf9RhD1FLPD+M2uFwdNjCaKH5wQzpoeJ/u1U8dgbuak7MkogwTZq9TwtImoS1
```

mKPV+3PBV2HdKFZ1E66HjucMUQkQdYhMvI35ezzUIkgfKtzra7tEscszcTJGr61K
8YzodDqs5xoic4DSMPclQsciOzsSrZYuxsN2B6ogtzVJV+mSSeh2FnIxZyuWfoqj
x5RWIr9qS34BIbIjMt/kmkRtWVtd9QCgHJvGeJeNkP+byKq0rxFROV7Z+2et1VsR
nTKaG73VululycslaVNVJ1zgyjbLiGH7HrfQy+4W+9OmTN6SpdTi3/UGVN4unUu0
kzCqgc7dGtxRcw1PcOnlthYhGXmy5okLdWTK1au8CcEYof/UVKGFPP0UJAOyh9Ok
twIDAQABo0IwQDAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zAdBgNV
HQ4EFgQUu//KjiOfT5nK2+JopqUVJxce2Q4wDQYJKoZIhvcNAQEMBQADggIBALZp
8KZ3/p7uC4Gt4cCpx/k1HUCCq+YEtN/L9x0Pg/B+E02NjO7jMyLDOfxA325BS0JT
vhaI8dI4XsRomRyYUpOM52jtG2pzegVATX9lO9ZY8c6DR2Dj/5epnGB3GFW1fgiT
z9D2PGcDFWEJ+YF59exTpJ/JjwGLc8R3dtyDovUMSRqodt6Sm2T4syzFJ9MHwAiA
pJiS4wGWAqoC7o87xdFtCjMwc3i5T1QWvwsHoaRc5svJXISPD+AVdyx+Jn7axEvb
pxZ3B7DNdehyQtaVhJ2Gg/LkkM0JR9SLA3DaWsYDQvTtN6LwG1BUSw7YhN4ZKJmB
R64JGz9I0cNv4rBgF/XuIwKl2gBbbZCr7qLpGzvpx0QnRY5rn/WkhLx3+WuXrD5R
RaIRpsyF7gpo8j5QOHokYh4XIDdtak23CZvJ/KRY9bb7nE4Yu5UC56GtmwfuNmsk
0jmGwZODUNKBRqhfYlcsu2xkiAhu7xNUX90txGdj08+JN7+dIPT7eoOboB6BAFDC
5AwiWVIQ7UNWhwD4FFKnHYuTjKJNRn8nxnGbJN7k2oaLDX5rIMHAnuFl2GqjpuiF
izoHCBy69Y9Vmhh1fuXsgWbRIXOhNUQLgD1bnF5vKheW0YMjiGZt5obicDIvUiLn
yOd/xCxgXS/Dr55FBcOEArf9LAhST4Ldo/DUhgkC
-----END CERTIFICATE-----

Related links

GlobalSign Root CA - R2 in PEM format

-----BEGIN CERTIFICATE-----
MIIDujCCAqKgAwIBAgILBAAAAAABD4Ym5g0wDQYJKoZIhvcNAQEFBQAwTDEgMB4G
A1UECxMXR2xvYmFsU2lnbiBSb290IENBIC0gUjIxEzARBgNVBAoTCkdsb2JhbFNp
Z24xEzARBgNVBAMTCkdsb2JhbFNpZ24wHhcNMDYxMjE1MDgwMDAwWhcNMjExMjE1
MDgwMDAwWjBMMSAwHgYDVQQLExdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSMjETMBEG
A1UEChMKR2xvYmFsU2lnbjETMBEGA1UEAxMKR2xvYmFsU2lnbjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAKbPJA6+Lm8omUVCxKs+IVSbC9N/hHD6ErPL
v4dfxn+G07IwXNb9rfF73OX4YJYJkhD10FPe+3t+c4isUoh7SqbKSaZeqKeMWhG8
eoLrvozps6yWJQeXSpkqBy+0Hne/ig+1AnwblrjFuTosvNYSuetZfeLQBoZfXklq
tTleiDTsvHgMCJiEbKjNS7SgfQx5TfC4LcshytVsW33hoCmEofnTlEnLJGKRILzd
C9XZzPnqJworc5HGnRusyMvo4KD0L5CLTfuwNhv2GXqF4G3yYROIXJ/gkwpRl4pa
zq+r1feqCapgvdzZX99yqWATXgAByUr6P6TqBwMhAo6CygPCm48CAwEAAaOBnDCB
mTAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUm+IH
V2ccHsBqBt5ZtJot39wZhi4wNgYDVR0fBC8wLTAroCmgJ4YlaHR0cDovL2NybC5n
bG9iYWxzaWduLm5ldC9yb290LXIyLmNybDAfBgNVHSMEGDAWgBSb4gdXZxwewGoG
3lm0mi3f3BmGLjANBgkqhkiG9w0BAQUFAAOCAQEAmYFThxxol4aR7OBKuEQLq4Gs
J0/WwbgcQ3izDJr86iw8bmEbTUsp9Z8FHSbBuOmDAGJFtqkIk7mpM0sYmsL4h4hO
291xNBrBVNpGP+DTKqttVCL1OmLNIG+6KYnX3ZHu01yiPqFbQfXf5WRDLenVOavS
ot+3i9DAgBkcRcAtjOj4LaR0VknFBbVPFd5uRHg5h6h+u/N5GJG79G+dwfCMNYxd
AfvDbbnvRG15RjF+Cv6pgsH/76tuIMRQyV+dTZsXjAzlAcmgQWpzU/qlULRuJQ/7
TBj0/VLZjmmx6BEP3ojY+x1J96relc8geMJgEtslQIxq/H5COEBkEveegeGTLg==
-----END CERTIFICATE-----

Related links

ISRG Root X1 in PEM format

```
-----BEGIN CERTIFICATE-----
MIIFazCCA1OgAwIBAgIRAIIQz7DSQONZRGPgu2OCiwAwDQYJKoZIhvcNAQELBQAw
TzELMAkGA1UEBhMCVVMxKTAnBgNVBAoTIEludGVybmV0IFNlY3VyaXR5IFJlc2Vh
cmNoIEdyb3VwMRUwEwYDVQQDEwxJU1JHIFJvb3QgWDEwHhcNMTUwNjA0MTEwNDM4
WhcNMzUwNjA0MTEwNDM4WjBPMQswCQYDVQQGEwJVUzEpMCcGA1UEChMgSW50ZXJu
ZXQgU2VjdXJpdHkgUmVzZWFyY2ggR3JvdXAxFTATBgNVBAMTDElTUkcgUm9vdCBY
MTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAK3oJHP0FDfzm54rVygc
h77ct984kIxuPOZXoHj3dcKi/vVqbvYATyjb3miGbESTtrFj/RQSa78f0uoxmyF+
0TM8ukj13Xnfs7j/EvEhmkvBioZxaUpmZmyPfjxwv60pIgbz5MDmgK7iS4+3mX6U
A5/TR5d8mUgjU+g4rk8Kb4Mu0UlXjIB0ttov0DiNewNwIRt18jA8+o+u3dpjq+sW
T8KOEUt+zwvo/7V3LvSye0rgTBIlDHCNAymg4VMk7BPZ7hm/ELNKjD+Jo2FR3qyH
B5T0Y3HsLuJvW5iB4YlcNHlsdu87kGJ55tukmi8mxdAQ4Q7e2RCOFvu396j3x+UC
B5iPNgiV5+I3lg02dZ77DnKxHZu8A/lJBdiB3QW0KtZB6awBdpUKD9jf1b0SHzUv
KBds0pjBqAlkd25HN7rOrFleaJ1/ctaJxQZBKT5ZPt0m9STJEadao0xAH0ahmbWn
OlFuhjuefXKnEgV4We0+UXgVCwOPjdAvBbI+e0ocS3MFEvzG6uBQE3xDk3SzynTn
jh8BCNAw1FtxNrQHusEwMFxIt4I7mKZ9YIqioymCzLq9gwQbooMDQaHWBfEbwrbw
qHyGO0aoSCqI3Haadr8faqU9GY/rOPNk3sgrDQoo//fb4hVC1CLQJ13hef4Y53CI
rU7m2Ys6xt0nUW7/vGT1M0NPAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIBBjAPBgNV
HRMBAf8EBTADAQH/MB0GA1UdDgQWBBR5tFnme7bl5AFzgAiIyBpY9umbbjANBgkq
hkiG9w0BAQsFAAOCAgEAVR9YqbyyqFDQDLHYGmkgJykIrGF1XIpu+ILlaS/V9lZL
ubhzEFnTIZd+50xx+7LSYK05qAvqFyFWhfFQDlnrzuBZ6brJFe+GnY+EgPbk6ZGQ
3BebYhtF8GaV0nxvwuo77x/Py9auJ/GpsMiu/X1+mvoiBOv/2X/qkSsisRcOj/KK
NFtY2PwByVS5uCbMiogziUwthDyC3+6WVwwW6LLv3xLfHTjuCvjHIInNzktHCgKQ5
ORAzI4JMPJ+GslWYHb4phowim57iaztXOoJwTdwJx4nLCgdNbOhdjsnvzqvHu7Ur
TkXWStAmzOVyyghqpZXjFaH3pO3JLF+l+/+sKAIuvtd7u+Nxe5AW0wdeRlN8NwdC
jNPELpzVmbUq4JUagEiuTDkHzsxHpFKVK7q4+63SM1N95R1NbdWhscdCb+ZAJzVc
oyi3B43njTOQ5yOf+1CceWxG1bQVs5Zufps Mljq4Ui0/1lvh+wjChP4kqKOJ2qxq
4RgqsahDYVvTH9w7jXbyLeiNdd8XM2w9U/t7y0Ff/9yi0GE44Za4rF2LN9d11TPA
mRGunUHBcnWEvgJBQl9nJEiU0Zsnvgc/ubhPgXRR4Xq37Z0j4r7g1SgEEzwxA57d
emyPxgcYxn/eR44/KJ4EBs+lVDR3veyJm+kXQ99b21/+jh5Xos1AnX5iItreGCc=
-----END CERTIFICATE-----
```

Related links

DigiCert Global Root CA in PEM format

```
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsB
CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97
nh6Vfe63SKMI2tavegw5BmV/Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt
43C/dxC//AH2hdmoRBBYMql1GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P
T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4
gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO
BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR
TLtm8KPiGxvDl7I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw
DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr
hMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg
06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF
PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls
```

```
YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk
CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=
-----END CERTIFICATE-----
```

Related links

[Default Trusted Certificates](#) on page 141

DigiCert SHA2 Secure Server CA in PEM format

```
-----BEGIN CERTIFICATE-----
MIIElDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xMzAzMDgxMjAwMDBaFw0yMzAzMDgxMjAwMDBaME0xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxJzAlBgNVBAMTHkRpZ2lDZXJ0IFNIQTIg
U2VjdXJlIFNlcnZlciBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANyuWJBNwcQwFZA1W248ghX1LFy949v/cUP6ZCWA1O4Yok3wZtAKc24RmDYXZK83
nf36QYSvx6+M/hpzTc8zl5CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXUu3R0bd
KpPDkC55gIDvEwRqFDu1m5K+wgdlTvza/P96rtxcflUxDOg5B6TXvi/TC2rSsd9f
/ld0Uzs1gN2ujkSYs58O09rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARFdRdNzGX
kujNVA075ME/OV4uuPNcfhCOhkEAjUVmR7ChZc6gqikJTvOX6+guqw9ypzAO+sf0
/RR3w6RbKFfCs/mC/bdFWJsCAwEAAaOCAVowggFWMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDgYDVR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY
aHR0cDovL29jc3AuZGlnaWNlcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGMWh0dHA6
Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwN6A1
oDOGMWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD
QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v
d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh
xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB
CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqipl
5TlPHoOlblyYoiQm5vuh7ZPHLgLGTUq/sELfeNqzqPlt/yGFUzZgTHbO7Djc1lGA
8MXW5dRNJ2Srm8c+cftIl7gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC
2iDJ6m6K7hQGrn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit
c+LJMto4JQtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0
j6tJLp07kzQoH3jOlOrHvdPJbRzeXDLz
-----END CERTIFICATE-----
```

Related links

[Default Trusted Certificates](#) on page 141

Let's Encrypt Authority X3 in PEM format

```
-----BEGIN CERTIFICATE-----
MIIEkjCCA3qgAwIBAgIQCgFBQgAAAVOFc2oLheynCDANBgkqhkiG9w0BAQsFADA/
MSQwIgYDVQQKExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMT
DkRTVCBSb290IENBIFgzMB4XDTE2MDMxNzE2NDA0NloXDTIxMDMxNzE2NDA0Nlow
SjELMAkGA1UEBhMCVVMxFjAUBgNVBAoTDUxldCdzIEVuY3J5cHQxIzAhBgNVBAMT
GkxldCdzIEVuY3J5cHQgQXV0aG9yaXR5IFgzMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAnNMM8FrlLke3cl03g7NoYzDq1zUmGSXhvb418XCSL7e4S0EF
q6meNQhY7LEqxGiHC6PjdeTm86dicbp5gWAf15Gan/PQeGdxyGkOlZHP/uaZ6WA8
SMx+yk13EiSdRxta67nsHjcAHJyse6cF6s5K671B5TaYucv9bTyWaN8jKkKQDIZ0
Z8h/pZq4UmEUEz9l6YKHy9v6Dlb2honzhT+Xhq+w3Brvaw2VFn3EK6BlspkENnWA
a6xK8xuQSXgvopZPKiAlKQTGdMDQMc2PMTiVFrqoM7hD8bEfwzB/onkxEz0tNvjj
/PIzark5McWvxI0NHWQWM6r6hCm21AvA2H3DkwIDAQABo4IBfTCCAXkwEgYDVR0T
```

```
AQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAYYwfwYIKwYBBQUHAQEEczBxMDIG
CCsGAQUFBzABhiZodHRwOi8vaXNyZy50cnVzdGdlbC9jc3AuaWRlbnRydXN0LmNv
bTA7BggrBgEFBQcwAoYvaHR0cDovL2FwcHMuaWRlbnRydXN0LmNvbS9yb290cy9k
c3Ryb290Y2F4My5wN2MwHwYDVR0jBBgwFoAUxKexpHsscfrb4UuQdf/EFWCFiRAw
VAYDVR0gBE0wSzAIBgZngQwBAgEwPwYLKwYBBAGC3xMBAQEwMDAuBggrBgEFBQcC
ARYiaHR0cDovL2Nwcy5yb290LXgxLmxldHNlbmNyeXB0Lm9yZZA8BgNVHR8ENTAz
MDGgL6AthitodHRwOi8vY3JsLmlkZW50cnVzdC5jb20vRFNUUk9PVENBWDNDUkwu
Y3JsMB0GA1UdDgQWBBSoSmpjBH3duubRObemRWXv86jsoTANBgkqhkiG9w0BAQsF
AAOCAQEA3TPXEfNjWDjdGBX7CVW+dla5cEilaUcne8IkCJLxWh9KEik3JHRRHGJo
uM2VcGfl96S8TihRzZvoroed6ti6WqEBmtzw3Wodatg+VyOeph4EYpr/1wXKtx8/
wApIvJSwtmVi4MFU5aMqrSDE6ea73Mj2tcMyo5jMd6jmeWUHK8so/joWUoHOUgwu
X4Po1QYz+3dszkDqMp4fklxBwXRsW10KXzPMTZ+sOPAveyxindmjkW8lGy+QsRlG
PfZ+G6Z6h7mjem0Y+iWlkYcV4PIWL1iwBi8saCbGS5jN2p8M+X+Q7UNKEkROb3N6
KOqkqm57TH2H3eDJAkSnh6/DNFu0Qg==
-----END CERTIFICATE-----
```

Related links

[Default Trusted Certificates](#) on page 141

Removing a Default Trusted Certificate

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

1. 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.

2. One .pem, file per certificate

3. Using the IP Office or IP Office Web Manager File Manager feature, copy the file to the `system/primary/certificates/tcs/delete` directory

4. 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](#) on page 40 for more information on certificate file formats.

Related links

[Default Trusted Certificates](#) on page 141

Chapter 22: 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
- Google Chrome Browser
- Safari Browser
- Microsoft Edge

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 1.8 uses its own internal certificate store

⚠️ **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.

Related links

Windows Certificate Store Organization

By default, certificates are stored in the following structure:
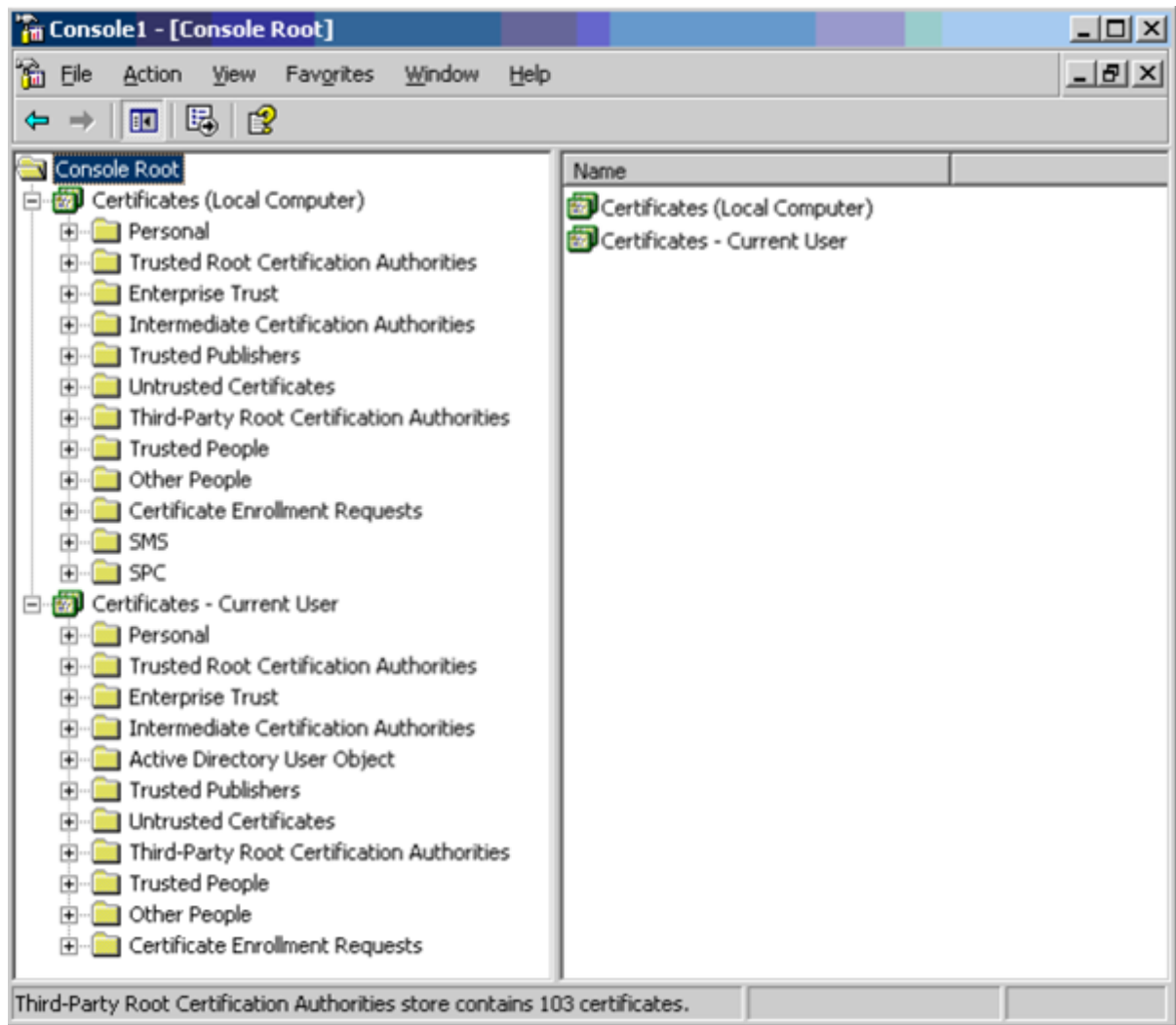
Each of the sub folders has differing usage. The `Certificates - Current User` area changes with the currently logged-in windows user. The `Certificate (Local Computer)` area does not change with the currently logged-in windows user.

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

Local Computer Folder	Usage
Personal > **Certificates**	Folder searched by IP Office Manager and some Web Browsers 1st 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 IP Office**.
	Folder accessed whenever '`Local Machine`' certificate store used for Security Settings.
	Folder searched by IP Office Manager for matching certificate when certificate received from the system, and **File** > **Preferences** > **Security** > **Manager Certificate Checks** = **Medium** or **High**.
Trusted Root Certification Authorities > **Certificates**	Folder searched by IP Office 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**.
	Folder searched by some browsers and other applications for matching root CA certificate when a certificate received from IP Office.

Current User Folder	Usage
Personal > **Certificates**	Folder searched by IP Office 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 IP Office**.
	Folder accessed whenever '`Current User`' certificate store is used for Security Settings.
	Folder searched by IP Office Manager for matching certificate when certificate received from IP Office, and **File** > **Preferences** > **Security** > **Manager Certificate Checks** = **Medium** or **High**.
Trusted Root Certification Authorities > **Certificates**	Folder searched by IP Office Manager for matching parent certificates when non-self-signed certificate received from the system, and **File** > **Preferences** > **Security** > **Manager Certificate Checks** = **Medium** or **High**.
	This folder is not used by non-Microsoft applications such as Chrome or Safari browsers – the corresponding `Local Computer` folder is used.
Other People > **Certificates**	Folder searched by IP Office Manager for matching parent certificates when non-self-signed certificate received from the system, and **File** > **Preferences** > **Security** > **Manager Certificate Checks** = **Medium** or **High**.
	This folder is not used by non-Microsoft applications such as Chrome or Safari browsers – the corresponding `Local Computer` folder is used.

Related links

Certificate Store Import

In order to use certificates – either for security settings or IP Office 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 IP Office 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 IP Office Manager, the Personal folder should be used, and the associated private key saved as well.

Related links

[Windows Certificate Management](#) on page 149

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 (that is, 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 (that is, 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.

Related links

[Windows Certificate Management](#) on page 149

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

Related links

[Windows Certificate Management](#) on page 149

Chapter 23: SRTP Troubleshooting

This section provides notes for SRTP troubleshooting.

Related links

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 the **Show SRTP** button to display further details on SRTP sessions.

Related links

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 System Status Application/ 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 IP Office 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** > **Media Security** setting to **Enforce** or **Disabled**.

- Some phones do not support RTCP (SRTCP); verify operation with SRTCP disabled.

Related links

SRTP Troubleshooting on page 153

Comments on this document?

Chapter 24: 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.
- For VoIP endpoints, also see IP Office VoIP Endpoint Security on page 161.
- Unless stated otherwise, in the scenarios below IP Office is the server

Related links

IP Office Interface Certificate Support: IP Office

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

Link	Protocol	Certificate Support	ID Certificate Offered	Trust Checks	Check Controls
SIP Line	SIP-TLS	✓	Telephony	Both	✓ [1]
SM Line	SIP-TLS	✓	Telephony	Both	✓ [1]
SIP Extension	SIP-TLS	✓	Telephony	Client	✗
H323 Extension – Signaling	H323-TLS	✓	Management	Client	n/a
H323 Extension – Provisioning	HTTPS	✓	Management	Both	✓ [2]

Table continues…

Link	Protocol	Certificate Support	ID Certificate Offered	Trust Checks	Check Controls
DECT R4 Provisioning	HTTPS	✓	Management	Both	✓ [2]
D100 Provisioning	HTTP	–	–	–	n/a
IP Office Line (WebSocket)	HTTPS	✓	Management	Both	✓ [3]
IP Office Manager - Security	TLS	✓	Management	Both	✓ [4]
IP Office Manager - Configuration	TLS	✓	Management	Both	✓ [5]
IP Office SoftConsole	HTTPS	✓	Management	IPO	✓ [2]
System Status Application	TLS	✓	Management	IPO	✗
IP Office Web Manager (Single instance management over port 8443)	HTTPS	✓	Management	Both	✓
IP Office Web Manager (Server Edition management over port 7070)	HTTPS	✓	Management	Client	✗
System Directory Central external directory feature	HTTPS	✓	Management	Both	✓ [2]
Avaya one-X® Portal for IP Office CTI	TCP	–	–	–	–
ACCS CTI	TLS	✓	Management	Server	✓ [7]
Avaya one-X® Portal for IP Office Directory	HTTPS	✓	Management	Server	✓ [2]
Voicemail Pro	HTTPS	✓	Management	Server	✓ [2]
SysMonitor	HTTPS	✓	Management	Server	✓ [2]
Backup/Restore client	HTTPS	✓	Management	Client	✓ [6]

Notes

[n] indicates the grouping for the certificate check controls on the IP Office server component. See Certificate Check Controls on page 52 for more details.

1. Manager Security: **System** > **Certificates** > **Received Certificate Checks (Telephony Endpoints)**. Any setting other than **None** will request a client certificate

2. Manager Security: **System** > **Services** > **HTTP** > **Service Security Level** and **System** > **Certificates** > **Received Certificate Checks (Management Interfaces)**.

3. 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

4. Manager Security: **System** > **Services** > **Security Administration** > **Service Security Level** and **System** > **Certificates** > **Received Certificate Checks (Management Interfaces)**.

5. Manager Security: **System** > **Services** > **Configuration** > **Service Security Level** and **System** > **Certificates** > **Received Certificate Checks (Management Interfaces)**.

6. Manager Security: **System** > **Certificates** > **Received Certificate Checks (Management Interfaces)**. IP Office HTTP clients will check the server certificate against the TCS for a setting of **Medium** or **High**.

7. Manager Security: **System** > **Unsecured Interfaces** > **TAPI** = unchecked. IP Office will check the ACCS server certificate against the TCS as per a setting of **Medium**.

Definitions

Column	Description
ID Certificate Offered	Type of ID certificate presented: • **Telephony** – Telephony or Management (configurable). • **Management** – Management certificate.
Trust Checks	Support and direction of certificate trust checks: • **Both** – Mutual certificate checks can be enabled. • **Server** – Only the server can check certificates. • **Client** – Only the client can check certificates.

Related links

[IP Office Interface Certificate Support](#) on page 155

IP Office Interface Certificate Support: Voicemail Pro

The following table provides an overview of certificate support for the IP Office platform Voicemail Pro interface.

Link	Protocol	Certificate Support	ID Certificate Offered	Trust Checks	Check Controls
Avaya one-X® Portal for IP Office message status	TCP	–	–	–	–
Avaya one-X® Portal for IP Office VM play	HTTPS	✓	Management	–	✕
Exchange WS client	HTTPS	✓	Management	Server	–
SFTP Client Exporting voicemail and recording data	SSHv2	✓	–	–	–

Comments on this document?

Definitions

Column	Description
ID Certificate Offered	Type of ID certificate presented: • **Telephony** – Telephony or Management (configurable). • **Management** – Management certificate.
Trust Checks	Support and direction of certificate trust checks: • **Both** – Mutual certificate checks can be enabled. • **Server** – Only the server can check certificates. • **Client** – Only the client can check certificates.

Related links

IP Office Interface Certificate Support: Avaya one-X® Portal for IP Office

The following table provides an overview of certificate support for the IP Office platform Avaya one-X® Portal for IP Office interface.

Link	Protocol	Certificate Support	ID Certificate Offered	Trust Checks	Check Controls
Avaya one-X® Portal for IP Office Browser/ Call Assistant	HTTPS	✓	Management[4]	Client	✗
Outlook, SalesForce, Lync Plugin	HTTPS	✓	Management[4]	Client	✗

Definitions

Column	Description
ID Certificate Offered	Type of ID certificate presented: • **Telephony** – Telephony or Management (configurable). • **Management** – Management certificate.
Trust Checks	Support and direction of certificate trust checks: • **Both** – Mutual certificate checks can be enabled. • **Server** – Only the server can check certificates. • **Client** – Only the client can check certificates.

Related links

IP Office Interface Certificate Support: Linux Server

The following table provides an overview of certificate support for the IP Office platform Linux server interface.

Link	Protocol	Certificate Support	ID Certificate Offered	Trust Checks	Check Controls
Backup/Restore server	HTTPS	✓	Management	Client	✕
Web Control	HTTPS	✓	Management	Client	✕
SSH Server	SSHv2	✓	–	–	–
SFTP Server	SSHv2	✓	–	–	–

Definitions

Column	Description
ID Certificate Offered	Type of ID certificate presented: • **Telephony** – Telephony or Management (configurable). • **Management** – Management certificate.
Trust Checks	Support and direction of certificate trust checks: • **Both** – Mutual certificate checks can be enabled. • **Server** – Only the server can check certificates. • **Client** – Only the client can check certificates.

Related links

IP Office Interface Certificate Support: WebLM Server

The following table provides an overview of certificate support for the IP Office platform WebLM server interface.

Link	Protocol	Certificate Support	ID Certificate Offered	Trust Checks	Check Controls
Web Admin (WebLM is the server)	HTTPS	✓	Management	Client	✕

Definitions

Column	Description
ID Certificate Offered	Type of ID certificate presented: • **Telephony** – Telephony or Management (configurable). • **Management** – Management certificate.
Trust Checks	Support and direction of certificate trust checks: • **Both** – Mutual certificate checks can be enabled. • **Server** – Only the server can check certificates. • **Client** – Only the client can check certificates.

Related links

Chapter 25: IP Office VoIP Endpoint Security

The following tables summarizes various security aspects for Avaya endpoints when used with IP Office.

- You must also consult the relevant endpoint or server documentation, as supported features can vary between firmware releases.

Related links

Avaya SIP Endpoint Security Options

The following table summarizes various security aspects for Avaya SIP endpoints when used with IP Office.

- You must also consult the relevant endpoint or server documentation, as supported features can vary between firmware releases.

Endpoint	Secure Media	Secure Signaling	Secure Remote Settings[1]	Auto Generated Settings	SIPS Support
9600 Series[2]	✓ [5]	✓	✓	✗	✓
1100/1200 Series[4]	✓ [5]	✓	✓	✓	✗
B179[6]	✓	✓	✓	✓	✓
H175	✓ [5]	✓	✓	✓	✓
J129[4]	✓	✓	✓	✓	✓
J100 Series	✓	✓	✓	✓	✓
K155, K165, K175 (Vantage)	✓	✓	✓	✓	✓
Scopia XT series	✓	✓	–	✗	✓ [3]

Table continues…

Endpoint	Secure Media	Secure Signaling	Secure Remote Settings[1]	Auto Generated Settings	SIPS Support
D100 SIP DECT	✗	✗	✗	✓	✗
Workplace	✓	✓	✓	✓	✓

Notes:

1. Remote phones can securely remotely download their settings and configuration, typically using HTTPS.

2. IP Office supports SIP 9608, 9611, 9621 and 9641 phones only as centralized users in a branch deployment.

3. SIPS always active when Secure Signaling selected.

4. 1100/1200 Series and J129 phones do not support FQDNs and so cannot use certificates provided by public Certificate Authorities.

5. Direct media is disabled when SRTP is enabled.

6. The B179 phone does not support secure RTCP (SRTCP).

Related links

IP Office SIP Endpoint Certificate Operation

The following tables summarizes various certificate aspects for Avaya SIP endpoints when used with IP Office.

- You must also consult the relevant endpoint or server documentation, as supported features can vary between firmware releases.

- IP Office does not support wildcard certificates for use with Avaya SIP clients. That includes Avaya Workplace Client, Avaya Vantage™ or J100 Series endpoints.

SIP Endpoint	Validate Server Certificate	Offer ID Certificate[2]	SAN Required?[3]
9608, 9611, 9621, 9641[1]	✓	✓	✗
1100/1200 Series[4]	✓	✓	✓ [A]
B179	✓	✓	✗
H175	✓	✓	✓ [B]
J129[4]	✓	✓	✓ [C]
J100 Series	✓	✓	✓ [D]
K155, K165, K175 (Vantage)	✓	✓	✓ [D]

Table continues…

SIP Endpoint	Validate Server Certificate	Offer ID Certificate[2]	SAN Required?[3]
Scopia XT series	✓	✓	✓ [D]
D100 SIP DECT	✕	✕	✕
Workplace	✓	✓	✓ [D]

IP Office Subject Alt Name Requirements

SAN	SIP Endpoint	Subject Alt Name Content
A.	• **1100/1200 Series**[4]	• **IP.1:** LAN 1 IP address.[5] • **IP.2:** LAN2 IP address.[5] • **IP.3:** Public IP Address if remote.[5]
B.	• **H175**	• **DNS:** SIP Domain Name
C.	• **J129**[4]	• **IP.1:** LAN 1 IP address.[5] • **IP.2:** LAN2 IP address.[5] • **IP.3:** Public IP Address if remote.[5] • **URI.1:** 'sip':SIP FQDN • **DNS:** SIP Domain
D.	• **J100 Series** (ex J129) • **9608, 9611, 9621 and 9641** • **K155, K165, K175 (Vantage)** • **Scopia XT series** • **Workplace**	• **DNS.1:** FQDN of IP Office. • **IP.1:** LAN 1 IP address.[5] • **IP.2:** LAN2 IP address.[5] • **IP.3:** Public IP Address if remote.[5]

Notes:

1. Remote phones can securely remotely download their settings and configuration, typically using HTTPS.

2. IP Office does not request certificates from SIP clients for SIP-TLS sessions. It can request a certificate for HTTPS transfers according to the Mutual Authentication setting; see Certificate Check Controls on page 52.

3. Indicates whether the endpoint requires **Subject Alternative Name** support within the identity certificate received from the IP Office. Typically, when using DNS, VoIP endpoints require only the FQDN of the IP Office in the SAN and no IP Address. Public Certificate Authorities do not support IP addresses and private domain names.

4. 1100/1200 Series and J129 phones do not support FQDNs and so cannot use certificates provided by public Certificate Authorities.

5. Avaya does not recommend using IP address entries in certificates.

6. If using VoIP resilience with secure signaling or provisioning, the root CA certificate for both servers must be the same.

7. If IP address entries are required for devices with Public CAs, you can use an `FQDN_IP_MAP` setting to map IP addresses to FQDNs. If using an auto-generated

46xxsettings.txt file, you can add the FQDN_IP_MAP entry to a 46xxspecials.txt file. For example, to map an IP addresses to an FQDN for just 9608, 9611, 9621 and 9641 phones:

```
IF $MODEL4 SEQ 9608 GOTO 96X1SETTINGS
IF $MODEL4 SEQ 9611 GOTO 96X1SETTINGS
IF $MODEL4 SEQ 9621 GOTO 96X1SETTINGS
IF $MODEL4 SEQ 9641 GOTO 96X1SETTINGS
GOTO END
# 96X1SETTINGS
SET FQDN_IP_MAP "ipol.ca.avaya.com=10.136.100.70,ipol2.ca.avaya.com=10.136.100.74"
# END
```

Related links

[IP Office VoIP Endpoint Security](#) on page 161

Avaya H.323 Endpoint Security Options

The following table summarizes various security aspects for Avaya H.323 endpoints when used with IP Office.

- You must also consult the relevant endpoint or server documentation, as supported features can vary between firmware releases.

Endpoint	Secure Media	Secure Signaling	Secure Remote Settings[1]	Auto-Generated Settings	SIPS Support
9600 Series	✓	✓ or partial[2]	✓	✓ [5]	–
1600 Series	✕	✕	✕	✓	–
DECT R4	✕	✕	✓	✓	–
IP Office[3]	✓	✓	✓	–	–
Voicemail Pro[4]	✕	✕	✓	–	–

Notes:

1. Remote phones can securely remotely download their settings and configuration, typically using HTTPS.

2. When H323-TLS is not used, signaling is not fully secured, but registration, SRTP Key exchange and dialed digits are.

3. IP Office line with WebSocket and security active.

4. Linking Voicemail Pro and the host IP Office if external.

5. The IP Office root CA certificate can be provisioned to the phone automatically by IP Office using the auto-generated settings file.

Related links

[IP Office VoIP Endpoint Security](#) on page 161

Avaya H.323 Endpoint Certificate Operation

The following tables summarizes various certificate aspects for Avaya H.323 endpoints when used with IP Office.

- You must also consult the relevant endpoint or server documentation, as supported features can vary between firmware releases.

H.323 Endpoint	Validate Server Certificate	Offer ID Certificate[3]	SAN Required?[4]
9600 Series	✓	✓	✓ [D]
1600 Series	✓	✓	✗
DECT R4	✓	✓	✗
IP Office[1]	✓	✓	✗
Voicemail Pro[2]	✗	✗	✗

IP Office Subject Alt Name Requirements

SAN	H.323 Endpoint	Subject Alt Name Content
A.	• **9600 Series1**	• **DNS.1:** FQDN of IP Office. • **IP.1:** LAN 1 IP address.[5] • **IP.2:** LAN2 IP address.[5] • **IP.3:** Public IP Address if remote.[5]

Notes:

1. IP Office line with WebSocket and security active.

2. Linking Voicemail Pro and the host IP Office if external.

3. IP Office does not request certificates from SIP clients for SIP-TLS sessions. It can request a certificate for HTTPS transfers according to the Mutual Authentication setting; see Certificate Check Controls on page 52.

4. Indicates whether the endpoint requires **Subject Alternative Name** support within the identity certificate received from the IP Office. Typically, when using DNS, VoIP endpoints require only the FQDN of the IP Office in the SAN and no IP Address. Public Certificate Authorities do not support IP addresses and private domain names.

5. Avaya does not recommend using IP address entries in certificates.

6. If using VoIP resilience with secure signaling or provisioning, the root CA certificate for both servers must be the same.

7. If IP address entries are required for devices with Public CAs, you can use an `FQDN_IP_MAP` setting to map IP addresses to FQDNs. If using an auto-generated `46xxsettings.txt` file, you can add the `FQDN_IP_MAP` entry to a `46xxspecials.txt` file. For example, to map an IP addresses to an FQDN for just 9608, 9611, 9621 and 9641 phones:

```
IF $MODEL4 SEQ 9608 GOTO 96X1SETTINGS
IF $MODEL4 SEQ 9611 GOTO 96X1SETTINGS
IF $MODEL4 SEQ 9621 GOTO 96X1SETTINGS
```

```
IF $MODEL4 SEQ 9641 GOTO 96X1SETTINGS
GOTO END
# 96X1SETTINGS
SET FQDN_IP_MAP "ipol.ca.avaya.com=10.136.100.70,ipol2.ca.avaya.com=10.136.100.74"
# END
```

Related links

IP Office VoIP Endpoint Security on page 161

Chapter 26: Using the IP Office Certificate Authority

The Certificate Authority (CA) feature of the Linux 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 IP Office Web Manager setting **Platform View** > **Settings** > **General** > **Certificates**.

Related links

Generating the CA Server's Own Identity Certificate

By default, the Primary or Linux 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. This is controlled by the Web Management setting **Platform View** > **Settings** > **General** > **Certificates** > **Identity Certificates** > **Renew automatically**.

To manually create an identity certificate for the CA server:

1. Uncheck the setting **Platform View** > **Settings** > **General** > **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 on page 49 for more information.

3. Enter the subject alternative names if the default offered is not acceptable. 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:203.0.113.30, 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 to all interfaces during which service loss will occur.

Related links

[Using the IP Office Certificate Authority](#) on page 167

Generating Identity Certificates for Other Devices

To manually create an identity certificate for another device:

1. Check the setting **Platform View** > **Settings** > **General** > **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](#) on page 49 for more information.

5. Enter any subject alternative names.

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 Update Certificates on page 102 and Implementing IP Office PKI on page 74 for more information.

Related links

Using the IP Office Certificate Authority on page 167

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 View** > **Settings** > **General** > **Certificates** > **CA Certificate** > **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 View** > **Settings** > **General** > **Certificates** > **CA Certificate** > **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.

Related links

Using the IP Office Certificate Authority on page 167

Renewing/Replacing the Signing Certificate

To create a new signing certificate:

1. Select **Platform View** > **Settings** > **General** > **Certificates** > **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 View** > **Settings** > **General** > **Certificates** > **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 View** > **Settings** > **General** > **Certificates** > **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 View** > **Settings** > **General** > **Certificates** > **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 View** > **Settings** > **General** > **Certificates** > **CA Certificate** > **Import**.

Related links

[Using the IP Office Certificate Authority](#) on page 167

Chapter 27: Secure Provisioning of 9600 Series H.323 Phones

You can configure 9608, 9611, 9621 and 9641 H.323 endpoints with or without staging.

- The manual staging process is the most secure.
- The automated process is less secure.

In the automated process, the phone does not authenticate the server with the initial HTTPS connection. If the initial phone connection to HTTPS is hijacked to an attacker's file server, the fraudulent file server can become trusted by the phone. In deployments with stronger security requirements where this risk is not acceptable, the phones must be manually staged in a controlled environment.

Related links

Manual Staging Process

Prepare the file server at the staging center. It can be an IP Office acting as the file server or another HTTP file server.

1. Put the phones upgrade file and firmware files on the file server.
2. Put the certificate of the root CA that signed the cloud IP Office identity certificate on the file server. Or the root CA that signed the top intermediate CA in the certificate chain of the IP Office identity certificate.
3. Edit the phones settings file per customer to contain the following settings, and put it on the staging file server:
   a. `NVTLSSRVR`, `NVHTTPSRVR` and `NVMCIPADD` - all three settings should specify the DNS name (FQDN) of the cloud IP Office instance. This FQDN will be resolved by DNS to the public IP address of the cloud IP Office instance. Note that the cloud IP Office instance for each customer will have a different FQDN and public IP address, hence the settings file has to be edited for staging phones for each customer.
      - As an alternative to the above, the HTTPS Sever IP Address, HTTP Sever IP Address and Call Server IP Address can be manually configured on each phone using the CRAFT UI. But since programming phones manually via CRAFT UI can

be very time consuming, the preferred method is setting the parameters using the staging settings file per the bullet above.

    b. `SET TRUSTCERTS <filename of root CA certificate>`

    c. `SET TLSSRVRVERIFYID 1` - When set to 1, the phone will verify the server identity in TLS connections, which is recommended for security. The phone will verify that the DNS name of the TLS server (as set in NVTLSSRVR) matches the `Common Name` or `subjectAltName` in the server certificate.

4. Connect the phone to the staging center network, and provide it with the staging file server IP address, from DHCP or from the phone UI.

5. The phone will contact the staging file server using HTTP and will download the upgrade and settings files, the trusted root CA certificate, and the firmware files if needed.

6. After staging, ship the phone to the customer site.

7. The phone is connected to the LAN at the customer site and powered up.

8. The phone contacts the cloud IP Office via HTTPS over TLS, using the `NVTLSSRVR` IP address it previously got from the staging settings file, and using port 411 (phone's default value of `TLSPORT`). The port 411 has to be open in the cloud firewall and in the IP Office. An authenticated TLS connection will be established, as the phone will verify the identity certificate (or identity certificate chain) that the cloud IP Office offers in the TLS connection, by checking it against the trusted root CA cert that the phone got during staging.

9. The phone will get the `96x1Hupgrade.txt` file and the auto-generated `46xxsettings.txt` file from the cloud IP Office through the HTTPS/TLS connection. The phone will also get the language files from the cloud IP Office through HTTPS.

10. The auto-generated `46xxsettings.txt` will specify `HTTPPORT 8411`. The port number 8411 has to be open in the cloud firewall, whereas port 80 is usually closed.

11. This is based on an enhancement on the IP Office. Port 8411 is hard-coded on the Linux IP Office and is open for restricted HTTP access allowing only Avaya IP phones to get only firmware files.

12. IP Office includes the setting HTTPPORT 8411 in the auto-generated 46xxsettings.txt file sent to a phone if and only if the request for the settings file came in HTTPS (not HTTP) and IP Office determines that the phone is connecting from the Internet. IP Office makes this determination if the source IP address of the request is not an RFC 1918 private address and not in the customer's private network as can optionally be specified in NUSN "PRIVATE_ADDR".

13. If new phone firmware is available on the cloud IP Office, as indicated in the upgrade file, the phone will get it from the cloud IP Office via HTTP on port 8411 as specified by the HTTPPORT in the auto-generated 46xxsettings.txt.

Related links

[Secure Provisioning of 9600 Series H.323 Phones](#) on page 171

Automated Process

1. Make sure the Root CA certificate used to sign the IP Office identity certificate, is installed in the IP Office Trusted Certificate Store:

   - If the trust policy selected for the IP Office uses a well-known public CA, download the PEM-encoded root CA certificate from the CA's web site and install it in the IP Office Trusted Certificate Store using IP Office Manager security settings **System** > **Certificates** > **Trusted Certificate Store** > **Add**.

   - If the trust policy selected for the IP Office uses its own internal CA, then the root CA certificate will already be in the IP Office Trusted Certificate Store.

2. Make sure that the IP Office identity certificate includes a Subject Alternative Name field containing the public IP address of the IP Office.

   - This is needed for the phones to be able to verify the server identity, when the phones are configured to connect to the IP Office's public IP address. It is not needed when the phones are configured through staging to connect to the IP Office's FQDN.

   - If IP Office is using an identity certificate generated by its own internal CA, then you need to generate a new identity certificate with the public IP address in Subject Alternative Name. Caution: Re-generate only the identity certificate and do not unnecessarily re-generate the root CA certificate, which can be disruptive (see Changing an IP Office Root CA Certificate on page 173).

3. Configure the following parameters on each phone through the phone CRAFT menu: **HTTPS Server IP Address**, **HTTP Server IP Address** and **Call Server IP Address**. All three parameters have to be set to the IP address of the IP Office.

4. The phone is restarted and contacts the IP Office from which it automatically obtains and installs the Root CA certificate of the IP Office.

Related links

Changing an IP Office Root CA Certificate

⚠ **Caution:**

   - Changing the root CA that signed the IP Office identity certificate can lock out installed phones that have previously been provisioned to trust only the old root CA. Avoid doing this unnecessarily. If an identity certificate signed by an external CA is going to be installed in the IP Office, this should be done before installing the phones.

If it is necessary to change the root CA after installing the phones, this has to be done with caution and will require some administrative effort

From Release 11.1, the following process can be used:

1. Ensure phones are registered to IP Office.

2. Enable the manager admin setting Automatic Phone Provisioning

3. Administer the new Root CA certificate on IP Office using Manager

4. IP Office will attempt to reboot the phones. Any phones busy on a call will be rebooted as soon as they are idle.

5. IP Office will wait for all phones to re-register, then activate the new Root CA

Prior to Release 11.1, some manual steps are required:

1. Obtain the current root CA and the new root CA file in the PEM format.

2. Perform a preparation step before changing the IP Office identity certificate; place a manually-edited settings file on the IP Office with `TRUSTCERTS` specifying both the current root CA and the new root CA file

3. Place both CA files on the SD card/disk in the system/primary directory. For IP Office Linux this will be the `opt/ipoffice/system/primary` directory

4. Reset all the phones which can be done remotely via SSA.

5. The phones will successfully connect to the IP Office, will get the new settings file and will get and install the new trusted root CA.

6. Change the IP Office identity certificate and remove the manually-edited settings file.

7. Next time the phones connect they will trust the new identity certificate.

Alternative manual on-site option:

1. Clear the phone configuration using CRAFT reset

2. Repeat the configuration of the server address on each phone.

Related links

[Secure Provisioning of 9600 Series H.323 Phones](#) on page 171

Chapter 28: Application/Client Security Dependencies

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

Applications

Component	Interface Control	Login Account	Certificate User	Notes
IP Office Manager	- Configuration (secure) - Security Administration (secure) - Program Code	Service User	✓ Management	Program Code used for IP Office Manager upgrade of IP500 V2 only.
Web Management	- Web Services	Service User	✓ Management	–
Web Control	- External	Service User	✓ Management	–
Voicemail Pro	- HTTP (secure)	Voicemail password	✓ Management	–
Avaya one-X® Portal for IP Office	- EnhTSPI - HTTP directory read - HTTP directory write	Service User	✗	–
System Status Application	- System Status Application	Service User	✓ Management	–
IP Office SoftConsole	- HTTP	IP Office User	✓ Management	–
SysMonitor	- HTTP - DevLink	Service User or Monitor password	✓ Management	Uses service user password when **System > Unsecured Interfaces > Use Service User Credentials** enabled.

Table continues…

Comments on this document?

Component	Interface Control	Login Account	Certificate User	Notes
TAPI	- TAPI	System password	✗	TAPI installer requires IP Office TAPI service enabled
DevLink	- DevLink	Monitor password	✗	DevLink installer requires IP Office DevLink service enabled (?)
DECT R4 Master base station	- HTTP (secure) - TFTP directory read	Service User	✓ Management	See DECT R4 extension below
ACCS		Internal to ACCS	–	See ACCS documentation
WebLM	Disable service	Internal to WebLM	–	See WebLM documentation

Lines

Component	Interface Control	Login Account	Certificate User	Notes
IP Office Line	- HTTP	IP Office Line password	✓ Management	–
SIP Line	Remove SIP line	SIP Line	✓ Management ✓ Telephony	–
Analog/Digital	Remove line	No	✗	Analog/ Digital lines cannot be removed

UC Clients

Component	Interface Control	Login Account	Certificate User	Notes
WebRTC	WebRTC service SIP Registrar	IP Office User	✓ Management	–

Extensions

Component	Interface Control	Login Account	Certificate User	Notes
DECT R4	IP DECT Line	IP Office User SARI/ PARK	✗	Auto-create DECT extension
H.323	H323 Registrar	IP Office User or Extension password	✓ Management	Auto-create H323 extension TLS only can be enabled
SIP	SIP Registrar	IP Office User	✓ Management	Auto-create SIP extension

Table continues…

Component	Interface Control	Login Account	Certificate User	Notes
Analog/Digital	No	IP Office User	✕	Analog/ Digital extensions cannot be removed

Chapter 29: Supported Ciphers

For IP Office R11.1.3 and higher, the following ciphers are supported.

Set	Ciphers
Set A	Note: This set is not supported on IP500 V2 systems. • `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` • `TLS_DHE_RSA_WITH_AES_256_GCM_SHA384` • `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256` • `TLS_DHE_RSA_WITH_AES_128_GCM_SHA256` • `TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384` • `TLS_RSA_WITH_AES_256_GCM_SHA384` • `TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256` • `TLS_RSA_WITH_AES_128_GCM_SHA256`
Set B	This set is included for backwards compatibility. • `TLS_DHE_RSA_WITH_AES_256_CBC_SHA` • `TLS_DHE_RSA_WITH_AES_128_CBC_SHA` • `TLS_DHE_RSA_WITH_AES_256_CBC_SHA256` • `TLS_DHE_RSA_WITH_AES_128_CBC_SHA256` • `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA` • `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA` • `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` • `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256`

- When the IP Office is acting as a TLS server, the **H.323 Security Level** and **SIP Security Level** setting operate as follows:
  - If set to **Medium**, the IP Office supports cipher sets A and B.
  - If set to **High**, the IP Office supports cipher set A.
- When the IP Office is acting as a TLS client:
  - The IP Office supports cipher sets A and B.
  - SysMonitor and System Status Application supports cipher sets A and B.

Part 7: Certificate Signing Requests

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 all cases the server used will retain the private key and therefore must be secured.

For the 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.

Related links

Converting Certificate Files

The intermediate .crt file can be in PEM or DER format; it is PEM format if viewable using a text editor. See Certificate File Naming and File Formats on page 45 for more information.

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
```

You will be asked for an encryption key for the resultant PKCS#12 file.

To convert PEM certificate and private key to PKCS#12:

```
openssl pkcs12 -export -in certificate.pem -inkey privateKey.pem -
certificate.pfx
```

You will be asked for an encryption key for the resultant PKCS#12 file. You may also be asked for the private key password.

Related links

Chapter 30: Creating a CSR using Microsoft MMC Certificates Snap-in

Use the following processes.

Related links

Create the CSR (MMC)

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.

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.

1. All steps must be carefully followed to avoid errors.

2. Further information on the snap-in and certificate operations can be found at: https://technet.microsoft.com/en-us/library/cc771157.aspx

3. Ensure all naming information has been identified (Common name, Alternate subject names, organization details and so on).

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

5. To open the Microsoft Management Console (MMC):

    a. Click **Start**.

    b. In the **Search** box, type `mmc`.

    c. Click `mmc.exe`.

6. Click **File** > **Add/Remove Snap-in** .

7. Click **Certificates** > **Add** > **OK**.

8. Select **Computer Account** and click **Next**.

9. Select **Local Computer** and click **Finish** then **OK**.

10. Expand **Certificates (Local Computer)**.

11. Right-click **Personal**, then click **Select All Tasks** > **Advanced Operations** > **Create Custom Request**.

12. Click **Next**.

13. Select **Proceed without enrollment policy** and click **Next**.

14. Select **(No Template) Legacy Key**.

15. Select **PKCS #10** and click **Next**.

16. In the **Certificate Information** section, click arrow button next to **Details** and click **Properties**.

17. On the **General** tab, type the domain name of the certificate in the **Friendly Name** field.

18. 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. For example, US
State	State or Province name	Do not abbreviate
Locality	Locality name	For example, City
Organization	Organization name	For example, Company Name
Organization Unit	Section/Department name	For example, IT
Common Name	FQDN of server	For example, www.example.com
Email	Contact email address	For example, contact@example.com

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

20. 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**.
URL	URI SAN entry	For example: sip:example.com
IP address (v4)	IP SAN entry	For example: 192.168.0.42 IP address entries are not recommended.

21. On the **Extension** tab, select **Key usage**.

22. Select **Non repudiation**, **Digital signature**, **Key encipherment**, and **Data encipherment**, clicking **Add** after entering each option.

23. Unselect **Make these key usages critical**.

24. On the **Extension** tab, select **Extended Key Usage**.

25. Select **Server Authentication** and **Client Authentication**, clicking **Add** after entering each option.

26. Unselect **Make the Extended Key Usage** critical.

27. On the **Private Key** tab, select **Cryptographic Service Provider**, select **Microsoft Strong Cryptographic Provider (Encryption)** only.

28. On the **Private Key** tab, select **Key type**, select **Exchange**.

29. On the **Private Key** tab, select **Key options** > **Key size** and set the value to 2048.

30. Select **Make Private Key Exportable**. Note: This step is important.

31. If presented, select **Select Hash Algorithm**, select **Hash Algorithm** and set the value to sha256.

32. Review all entries; check the **Key options** > **Key size** is still set to the value to 2048.

33. Click **OK** then **Next**.

34. Enter the filename (for example, `yourdomain`) and location to save the CSR to. Ensure **Base 64** is selected. Click **Finish**.

35. Open the CSR file `yourdomain.req` in a text editor and copy all of the text, including the start and end lines.

36. Go to the CA and follow instruction to paste the full CSR into the SSL enrollment 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. Do not use **SHA-1**.

Related links

Creating a CSR using Microsoft MMC Certificates Snap-in on page 181

Download and Import the Signed Identity Certificate (MMC)

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 File Formats on page 45 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.

Related links

[Creating a CSR using Microsoft MMC Certificates Snap-in](#) on page 181

Export the Signed Identity Certificate (MMC)

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 (for example, 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 using IP Office or IP Office Web Manager. See the relevant documentation and Implementing IP Office PKI on page 74 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.

Related links

Creating a CSR using Microsoft MMC Certificates Snap-in on page 181

Chapter 31: Creating a CSR using the OpenSSL Package

Use the following processes.

Related links

Create the CSR (OpenSSL)

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 and so on).

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 (for example, City)
organizationName = Organization Name (for example, Company)
organizationalUnitName = Organizational Unit Name (for example, Section/
Department)
commonName = Common Name (for example, www.example.com)
emailAddress = Email Address (for example, 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 = 203.0.113.30
IP.2 = 203.0.113.40
URI.1 = sip:example.com
URI.2 = 203.0.113.30
URI.3 = sip: 203.0.113.30
```

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 (for example, 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.

Related links

Creating a CSR using the OpenSSL Package on page 186

Download and Combine the Signed Identity Certificate (OpenSSL)

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'`, enter the password used to secure the private key file when creating the CSR.

8. When prompted `'Enter Export Password'`, a strong password should be used to secure the output PKCS#12 file. This password is 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 using IP Office or IP Office Web Manager. See the relevant documentation and Implementing IP Office PKI on page 74 for more information.

12. The example.key, example.p12, root and intermediate certificate files should be retained and used for recovery purposes.

    • Note: A password is always required to open the PKCS#12 and key file.

Related links

Creating a CSR using the OpenSSL Package on page 186

Chapter 32: Creating a CSR using the Linux Server Command Line

Use the following processes.

Related links

Create the CSR (Linux CLI)

All steps must be carefully followed to avoid errors.

1. Log in on the IPOL machine through the SSH service as Administrator, enter the certificates menu under the admin tab

2. Here the user can begin to create the CSR filling the SN and SAN parameters.

3. With the help of the `csr_subjectName` command the user should specify the following parameters: Country/State/Locality/Organization/OrganizationUnit/CommonName/Email as defined in the CSR parameters table above at the subject name fields.

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

5. If the CSR is for a multi-domain/SAN certificate, the user has the possibility to add entries in the SAN fields with the help of the `csr_subjectAltName` (add) command. The valid values are DNS (DNS SAN entry), IP (IPv4 SAN entry), URI (URI SAN entry). We can specify multiple values for every entry, numbering them as per ex: DNS.1=test1csr.com, DNS.2=test2csr.com.

6. When all the parameters of the CSR have been filled the user should check the CSR generation configuration with the help of the `csr_view_parameters` command. The command will display the current configuration for the CSR. The user should see something similar on the console display:

```
[ req ]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
[ req_distinguished_name ]
C=US
ST=Tennessee
L=Nashville
```

```
O=CSRsTest
OU=CSRsTestDep
CN=testcsr.com
emailAddress=admin@testcsr.com
[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyAgreement, dataEncipherment,
keyEncipherment
subjectAltName = @alt_names
subjectKeyIdentifier = hash
[ alt_names ]
DNS.1=testcsr.com
IP.1=192.168.42.1
URI.1=sip:testcsr.com
```

7. The user should then issue the generate_csr command which will generate the CSR, it will store the private key of the CSR in a location only accessible by root and it will display the generated CSR in the console.

8. The user should copy the from the console the generated CSR (that is view as text starting with the `-----BEGIN CERTIFICATE REQUEST-----` string and it ends with the `-----END CERTIFICATE REQUEST-----` string.

9. The CSR can be pasted in a text file and can be signed at a public CA or a private one resulting in a signed certificate based on a CSR generated on the IPOL machine.

Related links

[Creating a CSR using the Linux Server Command Line](#) on page 189

Download and Combine the Signed Identity Certificate (Linux CLI)

1. After approval and generation, receive/download the certificate file(s) from the CA.

2. The user can import a signed certificate in CLI under the admin/certificates menu with the help of the import_certid command. This command does not need any arguments. After invocation the CLI awaits the input of a signed certificate beginning with the string `-----BEGIN CERTIFICATE-----` and ending with the string `-----END CERTIFICATE-----`. The certificate should be in pem format (text).

3. If the certificate is valid (the certificate text is valid and also the certificate Is based on a CSR generated on the same ipol machine) the ipol machine will import the certificate into ipoffice application.

4. Upon successful operation an Operation Successful will be reported to the user.

5. The user will be able to read and set the certificate distribution flag through the `read_distribution_flag` and `set_distribution_flag` (on/off) so the certificate will remain the default one only for the ipoffice application (distribution flag off) or it will be distributed for all the applications on the machine (distribution flag on).

Related links

[Creating a CSR using the Linux Server Command Line](#) on page 189

Part 8: Further Help

Chapter 33: Additional Help and Documentation

The following pages provide sources for additional help.

Related links

Additional Manuals and User Guides

The [Avaya Documentation Center](#) website contains user guides and manuals for Avaya products including IP Office.

- For a listing of the current IP Office manuals and user guides, look at the [Avaya IP Office™ Platform Manuals and User Guides](#) document.

- The [Avaya IP Office Knowledgebase](#) and [Avaya Support](#) websites also provide access to the IP Office technical manuals and users guides.

  - Note that where possible these sites redirect users to the version of the document hosted by the [Avaya Documentation Center](#).

For other types of documents and other resources, visit the various Avaya websites (see [Additional IP Office resources](#) on page 193).

Related links

Getting Help

Avaya sells IP Office through accredited business partners. Those business partners provide direct support to their customers and can escalate issues to Avaya when necessary.

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner. See Finding an Avaya Business Partner on page 193.

Related links

Additional Help and Documentation on page 192

Finding an Avaya Business Partner

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner.

Procedure

1. Using a browser, go to the Avaya Website at https://www.avaya.com

2. Select **Partners** and then **Find a Partner**.

3. Enter your location information.

4. For IP Office business partners, using the **Filter**, select **Small/Medium Business**.

Related links

Additional Help and Documentation on page 192

Additional IP Office resources

In addition to the documentation website (see Additional Manuals and User Guides on page 192), there are a range of website that provide information about Avaya products and services including IP Office.

- Avaya Website (https://www.avaya.com)

  This is the official Avaya website. The front page also provides access to individual Avaya websites for different regions and countries.

- **Avaya Sales & Partner Portal** *(https://sales.avaya.com)*

  This is the official website for all Avaya business partners. The site requires registration for a user name and password. Once accessed, you can customize the portal to show specific products and information type that you want to see.

- **Avaya IP Office Knowledgebase** *(https://ipofficekb.avaya.com)*

  This site provides access to an online, regularly updated version of IP Office user guides and technical manual.

- **Avaya Support** *(https://support.avaya.com)*

This site provide access to Avaya product software, documentation and other services for Avaya product installers and maintainers.

  - **Avaya Support Forums** *(https://support.avaya.com/forums/index.php)*

    This site provides forums for discussing product issues.

• **International Avaya User Group** *(https://www.iuag.org)*

  This is the organization for Avaya customers. It provides discussion groups and forums.

• **Avaya DevConnect** *(https://www.devconnectprogram.com/)*

  This site provides details on APIs and SDKs for Avaya products, including IP Office. The site also provides application notes for third-party non-Avaya products that interoperate with IP Office using those APIs and SDKs.

• **Avaya Learning** *(https://www.avaya-learning.com/)*

  This site provides access to training courses and accreditation programs for Avaya products.

Related links

Training

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

• Avaya Certified Sales Specialist (APSS)

• Avaya Implementation Professional Specialist (AIPS)

• Avaya Certified Support Specialist (ACSS)

Credential maps are available on the Avaya Learning website.

Related links

Index

T

U

V

W