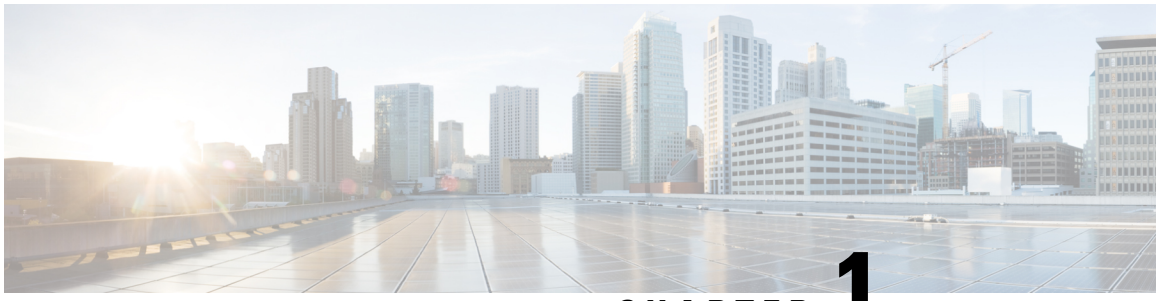
Security Guide for Cisco Unity Connection Release 14

First Published: 2020-11-24

Last Modified: 2020-11-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

IP Communications Required by Cisco Unity Connection

IP Communications Required by Cisco Unity Connection

Service Ports

Table 1: TCP and UDP Ports Used for Inbound Connections to Cisco Unity Connection lists the TCP and UDP ports that are used for inbound connections to the Cisco Unity Connection server, and ports that are used internally by Unity Connection.

Table 1: TCP and UDP Ports Used for Inbound Connections to Cisco Unity Connection

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: 20500, 20501, 20502, 19003, 1935	Open only between servers in a Unity Connection cluster. Port 1935 is blocked and is for internal use only.	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	Servers in a Unity Connection cluster must be able to connect to each other on these ports.
TCP: **21000–21512**	Open	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	IP phones must be able to connect to this range of ports on the Unity Connection server for some phone client applications.

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: **5000**	Open	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	Opened for port-status monitoring read-only connections. Monitoring must be configured in Connection Administration before any data can be seen on this port (Monitoring is off by default). Administration workstations connect to this port.
TCP and UDP ports allocated by administrator for SIP traffic. Possible ports are **5060–5199**	Open	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	Unity Connection SIP Control Traffic handled by conversation manager. SIP devices must be able to connect to these ports.
TCP: 20055	Open only between servers in a Unity Connection cluster	CuLicSvr/Unity Connection License Server	culic	Restricted to localhost only (no remote connections to this service are needed).
TCP: 1502, 1503 (“ciscounity_tcp” in /etc/services)	Open only between servers in a Unity Connection cluster	unityoninit/Unity Connection DB	root	Servers in a Unity Connection cluster must be able to connect to each other on these database ports. For external access to the database, use CuDBProxy.
TCP: **143, 993, 7993, 8143, 8993**	Open	CuImapSvr/Unity Connection IMAP Server	cuimapsvr	Client workstations must be able to connect to ports 143 and 993 for IMAP inbox access, and IMAP over SSL inbox access.

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: **25, 8025**	Open	CuSmtpSvr/Unity Connection SMTP Server	cusmtpsvr	Servers delivering SMTP to Unity Connection port 25, such as other servers in a UC Digital Network.
TCP: 4904	Blocked; internal use only	SWIsvcMon (Nuance SpeechWorks Service Monitor)	openspeech	Restricted to localhost only (no remote connections to this service are needed).
TCP: 4900:4904	Blocked; internal use only	OSServer/Unity Connection Voice Recognizer	openspeech	Restricted to localhost only (no remote connections to this service are needed).
UDP: **16384–21511**	Open	CuMixer/Unity Connection Mixer	cumixer	VoIP devices (phones and gateways) must be able to send traffic to these UDP ports to deliver inbound audio streams.
UDP: 7774–7900	Blocked; internal use only	CuMixer/ Speech recognition RTP	cumixer	Restricted to localhost only (no remote connections to this service are needed).
TCP: 22000 UDP: 22000	Open only between servers in a Unity Connection cluster	CuSrm/ Unity Connection Server Role Manager	cusrm	Cluster SRM RPC. Servers in a Unity Connection cluster must be able to connect to each other on these ports.

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: 22001 UDP: 22001	Open only between servers in a Unity Connection cluster	CuSrm/ Unity Connection Server Role Manager	cusrm	Cluster SRM heartbeat. Heartbeat event traffic is not encrypted but is MAC secured. Servers in a Unity Connection cluster must be able to connect to each other on these ports.
TCP: **20532**	Open	CuDbProxy/ Unity Connection Database Proxy	cudbproxy	If this service is enabled it allows administrative read/write database connections for off-box clients. For example, some of the ciscounitytools.com tools use this port. Administrative workstations would connect to this port.
TCP: **22**	Open	Sshd	root	Firewall must be open for TCP 22 connections for remote CLI access and serving SFTP in a Unity Connection cluster. Administrative workstations must be able to connect to a Unity Connection server on this port. Servers in a Unity Connection cluster must be able to connect to each other on this port.
UDP: **161**	Open	Snmpd Platform SNMP Service	root	—

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
UDP: **500**	Open	Raccoon ipsec isakmp (key management) service	root	Using ipsec is optional, and off by default. If the service is enabled, servers in a Unity Connection cluster must be able to connect to each other on this port.
TCP: **8500** UDP: **8500**	Open	clm/cluster management service	root	The cluster manager service is part of the Voice Operating System. Servers in a Unity Connection cluster must be able to connect to each other on these ports.
UDP: **123**	Open	Ntpd Network Time Service	ntp	Network time service is enabled to keep time synchronized between servers in a Unity Connection cluster. The publisher server can use either the operating system time on the publisher server or the time on a separate NTP server for time synchronization. Subscriber servers always use the publisher server for time synchronization. Servers in a Unity Connection cluster must be able to connect to each other on this port.

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: 5007	Blocked; internal use only.	Tomcat/Cisco Tomcat (SOAP Service)	tomcat	Servers in a Unity Connection cluster must be able to connect to each other on these ports.
TCP: 1500, 1501	Open only between servers in a Unity Connection cluster	cmoninit/Cisco DB	informix	These database instances contain information for LDAP integrated users, and serviceability data. Servers in a Unity Connection cluster must be able to connect to each other on these ports.
TCP: 1515	Open only between servers in a Unity Connection cluster	dblrpm/Cisco DB Replication Service	root	Servers in a Unity Connection cluster must be able to connect to each other on these ports.
TCP: 8001	Open only between servers in a Unity Connection cluster	dbmon/Cisco DB Change Notification Port	database	Servers in a Unity Connection cluster must be able to connect to each other on these ports.
TCP: 2555, 2556	Open only between servers in a Unity Connection cluster	RisDC/Cisco RIS Data Collector	ccmservice	Servers in a Unity Connection cluster must be able to connect to each other on these ports.
TCP: 1090, 1099	Open only between servers in a Unity Connection cluster	Amc/Cisco AMC Service (Alert Manager Collector)	ccmservice	Performs back-end serviceability data exchanges 1090: AMC RMI Object Port 1099: AMC RMI Registry Port Servers in a Unity Connection cluster must be able to connect to each other on these ports.

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: **80, 443, 8080, 8443**	Open	tomcat/Cisco Tomcat	tomcat	Both client and administrative workstations need to connect to these ports. Servers in a Unity Connection cluster must be able to connect to each other on these ports for communications that use HTTP-based interactions like REST. **Note** These ports support both the IPv4 and IPv6 addresses. However, the IPv6 address works only when Connection platform is configured in Dual (IPv4/IPv6) mode. Cisco Unity Connection Survivable Remote Site Voicemail SRSV supports these ports for IP communication.

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: 8081, 8444	Open only between servers in HTTPS Networking	tomcat/Cisco Tomcat	tomcat	Servers in HTTPS Networking must be able to connect to each other on these ports for communications. Unity Connection HTTPS Directory Feeder service uses these ports for directory synchronization. **Note** Unity Connection HTTPS Directory Feeder service supports only IPv4 mode.
TCP: 5001-5004, 8005	Blocked; internal use only	tomcat/Cisco Tomcat	tomcat	Internal tomcat service control and axis ports.
TCP: **32768–61000** UDP: **32768–61000**	Open	—	—	Ephemeral port ranges, used by anything with a dynamically allocated client port.
TCP: 7443	Open	jetty/Unity Connection Jetty	jetty	Secure Jabber and Web Inbox notifications **Note** You can enable the port using "utils cuc jetty ssl enable" CLI command.

Ports and Protocols[1]	Operating System Firewall Setting	Executable/Service or Application	Service Account	Comments
TCP: 7080	Open	jetty/Unity Connection Jetty	jetty	*Exchange 2010 only, single inbox only:* Jabber and Web Inbox EWS notifications of changes to Unity Connection voice messages.
UDP: 9291	Open	CuMbxSync/ Unity Connection Mailbox Sync Service	cumbxsync	*Single inbox only:* WebDAV notifications of changes to Unity Connection voice messages.
TCP: 6080	Open	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	Video server must be able to connect to Unity Connection on this port for communications.

[1] Bold port numbers are open for direct connections from off-box clients.

Outbound Connections Made by Unity Connection

Table 2: TCP and UDP Ports Unity Connection Uses to Connect With Other Servers in the Network lists the TCP and UDP ports that Cisco Unity Connection uses to connect with other servers in the network.

Table 2: TCP and UDP Ports Unity Connection Uses to Connect With Other Servers in the Network

Ports and Protocols	Executable	Service Account	Comments
TCP: 2000* (Default SCCP port) Optionally TCP port 2443* if you use SCCP over TLS. * Many devices and applications allow configurable RTP port allocations.	CuCsMgr	cucsmgr	Unity Connection SCCP client connection to Cisco Unified CM when they are integrated using SCCP.

Ports and Protocols	Executable	Service Account	Comments
UDP: 16384–32767* (RTP) * Many devices and applications allow configurable RTP port allocations.	CuMixer	cumixer	Unity Connection outbound audio-stream traffic.
UDP: 69	CuCsMgr	cucsmgr	When you are configuring encrypted SCCP, encrypted SIP, or encrypted media streams, Unity Connection makes a TFTP client connection to Cisco Unified CM to download security certificates.
TCP: 6972	CuCsMgr	cucsmgr	When you are configuring encrypted SIP or encrypted media streams, Unity Connection makes the HTTPS client connection with Cisco Unified CM to download ITL security certificates.
TCP: 53 UDP: 53	any	any	Used by any process that needs to perform DNS name resolution.
TCP: 53, and either 389 or 636	CuMbxSync CuCsMgr tomcat	cumbxsync cucsmgr tomcat	Used when Unity Connection is configured for unified messaging with Exchange and one or more unified messaging services are configured to search for Exchange servers. Unity Connection uses port 389 when you select LDAP for the protocol used to communicate with domain controllers. Unity Connection uses port 636 when you select LDAPS for the protocol used to communicate with domain controllers.

Ports and Protocols	Executable	Service Account	Comments
TCP: 80, 443 (HTTP and HTTPS)	CuMbxSync CuCsMgr tomcat	cumbxsync cucsmgr tomcat	**Note** These ports support both the IPv4 and IPv6 addresses.
TCP: 80, 443, 8080, and 8443 (HTTP and HTTPS)	CuCsMgr tomcat	cucsmgr tomcat	Unity Connection makes HTTP and HTTPS client connections to: • Other Unity Connection servers for Digital Networking automatic joins. • Cisco Unified CM for AXL user synchronization. **Note** These ports support both the IPv4 and IPv6 addresses. **Note** Cisco Unity Connection Survivable Remote Site Voicemail SRSV supports these ports for IP communication.
TCP: 143, 993 (IMAP and IMAP over SSL)	CuCsMgr	cucsmgr	Unity Connection makes IMAP connections to Microsoft Exchange servers to perform text-to-speech conversions of email messages in a Unity Connection user's Exchange mailbox.

Ports and Protocols	Executable	Service Account	Comments
TCP: 25,587 (SMTP)	CuSmtpSvr	cusmtpsvr	Unity Connection makes client connections to SMTP servers and smart hosts, or to other Unity Connection servers for features such as VPIM networking or Unity Connection Digital Networking. **Note** Cisco Unity Connection supports STARTTLS over port 25. With Release 14SU2 and later, STARTTLS is also supported over port 587.
TCP: 21 (FTP)	ftp	root	The installation framework performs FTP connections to download upgrade media when an FTP server is specified.
TCP: 22 (SSH/SFTP)	CiscoDRFMaster sftp	drf root	The Disaster Recovery Framework performs SFTP connections to network backup servers to perform backups and retrieve backups for restoration. The installation framework performs SFTP connections to download upgrade media when an SFTP server is specified.

Ports and Protocols	Executable	Service Account	Comments
UDP: 67 (DHCP/BootP)	dhclient	root	Client connections made for obtaining DHCP addressing. Although DHCP is supported, Cisco highly recommends that you assign static IP addresses to Unity Connection servers.
TCP: 123 UDP: 123 (NTP)	Ntpd	root	Client connections made for NTP clock synchronization.
UDP: 514 TCP: 601	Syslog/Cisco Syslog Server	syslog	Unity Connection server must be able to send audit logs to remote syslog server through these ports

Securing Transport Layer

Unity Connection uses Transport Layer Security(TLS) protocol and Secure Sockets Layer(SSL) protocol for signaling and client server communication. Unity Connection supports TLS 1.0, TLS 1.1 and TLS 1.2 for secure communication across various interfaces of Cisco Unity Connection. TLS 1.2 is the most secure and authenticated protocol for communication.

Depending upon the organization security policies and deployment capabilities, Unity Connection 11.5(1) SU3 and later allows you to configure the minimum TLS version. After configuring the minimum version of TLS, Unity Connection supports the minimum configured version and higher versions of TLS. For example, if you configure TLS 1.1 as a minimum version of TLS, Unity Connection uses TLS 1.1 and higher versions for communication and rejects the request for a TLS version that is lower than the configured value. By default, TLS 1.0 is configured.

Before configuring minimum TLS version, ensure that all the interfaces of Unity Connection must be secured and use configured minimum TLS version or higher version for communication. However, you can configure the minimum TLS version for inbound interfaces of Unity Connection.

Table 3 lists the supported interfaces for which you can configure the minimum TLS version on Unity Connection.

Table 3: Supported Interfaces for secure Communication

Ports	Executable/Service or Application	Service Account	Comments
8443, 443, 8444	• Cisco HAProxy	• haproxy	Both client and administrative workstations must connect to these ports. Servers in a Unity Connection cluster must be able to connect to each other on these ports for communications that use HTTP-based interactions like REST.
7443	jetty/Unity Connection Jetty	jetty	Secure Jabber and Web Inbox notifications. Cisco Unity Connection 14SU3 and later, supports only TLS version 1.2 for secure communication
993	CuImapSvr/Unity Connection IMAP Server	cuimapsvr	Client workstations must be able to connect to port 993 for IMAP over SSL inbox access.
25,587	CuSmtpSvr/Unity Connection SMTP Server	cusmtpsvr	Servers delivering SMTP to Unity Connection port 25 or 587, such as other servers in a UC Digital Network.
5061-5199	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	Unity Connection SIP Control Traffic handled by conversation manager. SIP devices must be able to connect to these ports.
LDAP *(outbound interface)*	CuMbxSync CuCsMgr tomcat	cumbxsync cucsmgr tomcat	Unity Connection uses port 636 when you select LDAPS for the protocol used to communicate with domain controllers.
20536	Cisco HAProxy	haproxy	If this service is enabled it allows administrative secure read/write database connections for off-box clients.

For more information on supported inbound interfaces of Cisco Unity Connection, see "Service Ports" section.

Configuring Minimum TLS Version

To configure the minimum TLS version in Cisco Unity Connection, execute the following CLI command:

- set tls min-version <tls minVersion>

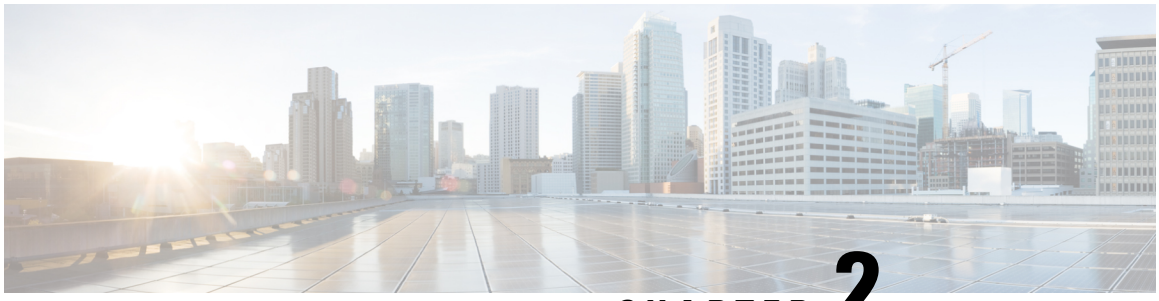
In cluster, you must execute the CLI command on both publisher and subscriber.

In addition to this, you can execute the following CLI command to check the configured value of minimum TLS version on Unity Connection:

- show tls min-version

For detailed information on the CLI, see *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* available at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Caution After configuring minimum TLS version, the Cisco Unity Connection server restart automatically.



CHAPTER 2

Preventing Toll Fraud

Introduction

In this chapter, you would find a description of toll fraud—a potential security issue in any organization. You can also find information that may help you to develop preventive measures, and best practices to avoid toll fraud.

Using Restriction Tables to Help Prevent Toll Fraud

Toll fraud is defined as any toll (long distance) call that is made at the expense of your organization and in violation of its policies. Cisco Unity Connection provides restriction tables that you can use to help guard against toll fraud. Restriction tables control the phone numbers that can be used for transferring calls, for message notification, and for other Unity Connection functions. Each class of service has several restriction tables associated with it, and you can add more as needed. By default, restriction tables are configured for basic toll fraud restrictions for a dial plan with a trunk access code of 9. Restriction tables should be adjusted for your specific dial plan and international dialing prefixes.

Best Practices:

To prevent toll fraud by users, administrators, and even outside callers who have improperly gained access to a Cisco Unity Connection mailbox, implement the following changes:

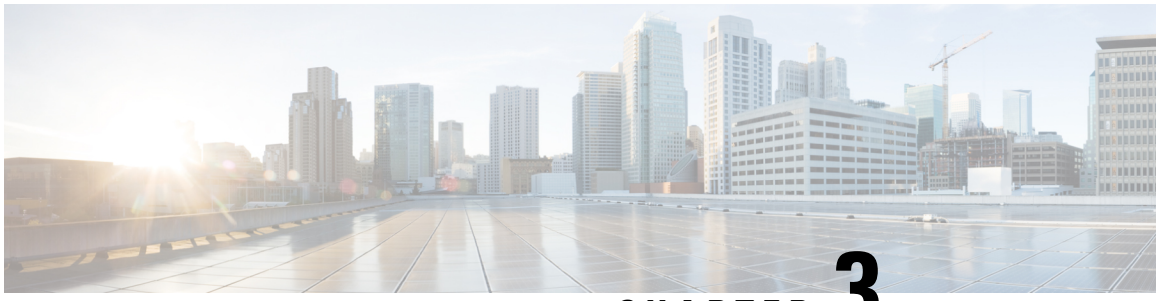
- Set up all restriction tables to block calls to the international operator. When this is done, a person cannot dial out to or configure call transfers from an extension to the international operator (for example, a trunk access code of 9 followed by 00 to dial the international operator) for placing international calls.
- If Unity Connection is integrated with two phone systems, add restriction table patterns to match applicable trunk access codes for both phone system integrations. For example, if the trunk access code for one of the phone system integrations is 99 and you want to restrict the call pattern 900, you would also restrict the pattern 99900. When patterns that include the trunk access codes are restricted, attempts to bypass the restriction table by first accessing either trunk and then dialing the international operator is blocked.
- For those in your organization who do not need to access international numbers to do their work, set up restriction tables to block all calls to international numbers. This prevents a person who has access to a

Unity Connection mailbox that is associated with the restriction table from configuring call transfers or fax delivery from that extension to an international number.

- Set up restriction tables to permit calls only to specific domestic long distance area codes or to prohibit calls to long distance area codes. This prevents a person who has access to a Unity Connection mailbox that is associated with the restriction table from configuring call transfers or fax delivery from that extension to a long distance number.
- Restrict the numbers that can be used for system transfers—a feature that allows callers to dial a number and then transfer to another number that they specify. For example, set up the applicable restriction tables to allow callers to transfer to a lobby or conference room phone, but not to the international operator or to a long distance phone number.

Restricting Collect Calling Options

We recommend that you work with your telecommunications provider to restrict the collect calling option on your incoming phone lines, if appropriate.



CHAPTER 3

Cisco Unity Connection- Restricted and Unrestricted Version

Cisco Unity Connection - Restricted and Unrestricted Version

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws.

Cisco Unity Connection provides two versions of the Connection software - restricted and unrestricted that address import requirements for some countries related to encryption of user data. Restricted version of the Cisco Unity Connection allows you to enable the encryption on the product to use the below given security modules whereas in Unrestricted version, you are not allowed to use the security modules

Functionality	Restricted Version of Connection	Unrestricted Version of Connection
SSL for IMAP connections used to access voice messages	Allowed	Disallowed
Secure SCCP, SIP, and SRTP for call signaling and media	Allowed	Disallowed
Communications among networked Connection servers or clusters (over secure MIME)	Allowed	Disallowed
SSL for Comet notification (Jetty SSL command)	Allowed	Disallowed

Caution With restricted and unrestricted versions of Connection software available, download software or order a DVD. Upgrading a restricted version to an unrestricted version is supported, but future upgrades are then limited to unrestricted versions. Upgrading an unrestricted version to a restricted version is not supported.

In Unity Connection, by default the encryption is disabled for the Restricted version of the product in Evaluation Mode. Hence you are not allowed to use the above security modules with Restricted version of Unity Connection until the product is registered with Cisco Smart Software Manager (CSSM) or Cisco Smart Software Manager satellite using a token that allows Export-Controlled Functionality. The behavior of Restricted version of Unity Connection in Evaluation Mode is similar to the behavior of Unrestricted version of Unity Connection.

When you are upgrading Cisco Unity Connection from any earlier releases to 12.0(1) and later, you get the following behavior of encryption on Cisco Unity Connection:

Upgrade Path	Cluster Mode before Upgrade	License Status before Upgrade	License Status after Upgrade	Action
Pre-12.0(1) to 12.0(1)	Secure	Demo or PLM Licensed	Evaluation Mode	Cisco Unity Connection continues to run in secure mode. If the product is not registered with CSSM or satellite through Export Controlled Functionality enabled token before Evaluation Period Expired, system will generate an alarm on RTMT after Evaluation Period Expired.

Caution After deregistration, if any of the following services - "Connection Conversation Manager" or "Connection IMAP Server" is restarted, you will not be able to use security modules. For example IMAP in case IMAP Server restart and SCCP/SIP/SRTP in case Connection Conversation Manager in Cisco Unity Connection.

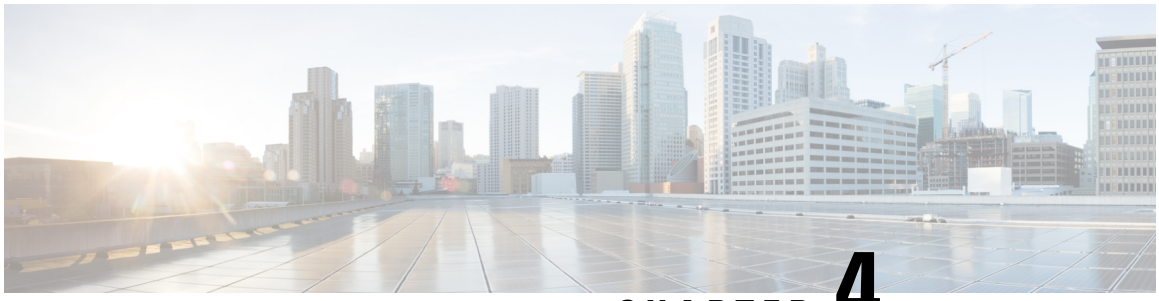
Note Upgrade from 12.0(1) to 12.0(1) and later will have the existing encryption status of the system after upgrade.

For more information on how to register the product with CSSM or satellite, see "Managing Licenses" chapter of *Install, Upgrade and Maintenance Guide for Cisco Unity Connection 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html.

To enable or disable the encryption on Cisco Unity Connection Restricted version, a CLI command "utils cuc encryption <enable/disable>" can be used.

Note In case of upgrade, you must execute the CLI after successfully completed the switch version.

For more information on the CLI, see the Command Line Interface Reference Guide for Cisco Unified Solutions for the latest release, available at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html



CHAPTER 4

Securing the Connection between Cisco Unity Connection, Cisco Unified Communications Manager, and IP Phones

Securing the Connection between Cisco Unity Connection, Cisco Unified Communications Manager, and IP Phones

Introduction

In this chapter, you would find descriptions of potential security issues related to connections between Cisco Unity Connection, Cisco Unified Communications Manager, and IP phones; information on any actions you need to take; recommendations that helps you make decisions; discussion of the ramifications of the decisions you make; and best practices.

Security Issues for Connections between Unity Connection, Cisco Unified Communications Manager, and IP Phones

A potential point of vulnerability for a Cisco Unity Connection system is the connection between Unity Connection voice messaging ports (for an SCCP integration) or port groups (for a SIP integration), Cisco Unified Communications Manager, and the IP phones.

Possible threats include:

- Man-in-the-middle attacks (when the information flow between Cisco Unified CM and Unity Connection is observed and modified)
- Network traffic sniffing (when software is used to capture phone conversations and signaling information that flow between Cisco Unified CM, Unity Connection, and IP phones that are managed by Cisco Unified CM)
- Modification of call signaling between Unity Connection and Cisco Unified CM

- Modification of the media stream between Unity Connection and the endpoint (for example, an IP phone or a gateway)
- Identity theft of Unity Connection (when a non-Unity Connection device presents itself to Cisco Unified CM as a Unity Connection server)
- Identity theft of the Cisco Unified CM server (when a non-Cisco Unified CM server presents itself to Unity Connection as a Cisco Unified CM server)

Cisco Unified Communications Manager Security Features for Unity Connection Voice Messaging Ports

Cisco Unified CM can secure the connection with Unity Connection against the threats listed in the Security Issues for Connections between Unity Connection, Cisco Unified Communications Manager, and IP Phones. The Cisco Unified CM security features that Unity Connection can take advantage of are described in Table 4: Cisco Unified CM Security Features Used by Cisco Unity Connection.

Table 4: Cisco Unified CM Security Features Used by Cisco Unity Connection

Security Feature	Description
Signaling authentication	The process that uses the Transport Layer Security (TLS) protocol to validate that no tampering has occurred to signaling packets during transmission. Signaling authentication relies on the creation of the Cisco Certificate Trust List (CTL) file. This feature protects against: • Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and Unity Connection. • Modification of the call signalling. • Identity theft of the Unity Connection server. • Identity theft of the Cisco Unified CM server.

Security Feature	Description
Device authentication	The process that validates the identity of the device and ensures that the entity is what it claims to be. This process occurs between Cisco Unified CM and either Unity Connection voice messaging ports (for an SCCP integration) or Unity Connection port groups (for a SIP integration) when each device accepts the certificate of the other device. When the certificates are accepted, a secure connection between the devices is established. Device authentication relies on the creation of the Cisco Certificate Trust List (CTL) file. This feature protects against: • Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and Unity Connection. • Modification of the media stream. • Identity theft of the Unity Connection server. • Identity theft of the Cisco Unified CM server.
Signaling encryption	The process that uses cryptographic methods to protect (through encryption) the confidentiality of all SCCP or SIP signaling messages that are sent between Unity Connection and Cisco Unified CM. Signaling encryption ensures that the information that pertains to the parties, DTMF digits that are entered by the parties, call status, media encryption keys, and so on are protected against unintended or unauthorized access. This feature protects against: • Man-in-the-middle attacks that observe the information flow between Cisco Unified CM and Unity Connection. • Network traffic sniffing that observes the signaling information flow between Cisco Unified CM and Unity Connection.

Security Feature	Description
Media encryption	The process whereby the confidentiality of the media occurs through the use of cryptographic procedures. This process uses Secure Real Time Protocol (SRTP) as defined in IETF RFC 3711, and ensures that only the intended recipient can interpret the media streams between Unity Connection and the endpoint (for example, a phone or gateway). Support includes audio streams only. Media encryption includes creating a Media Player key pair for the devices, delivering the keys to Unity Connection and the endpoint, and securing the delivery of the keys while the keys are in transport. Unity Connection and the endpoint use the keys to encrypt and decrypt the media stream. This feature protects against: • Man-in-the-middle attacks that listen to the media stream between Cisco Unified CM and Unity Connection. • Network traffic sniffing that eavesdrops on phone conversations that flow between Cisco Unified CM, Unity Connection, and IP phones that are managed by Cisco Unified CM.

Authentication and signaling encryption serve as the minimum requirements for media encryption; that is, if the devices do not support signaling encryption and authentication, media encryption cannot occur.

Cisco Unified CM security (authentication and encryption) only protects calls to Unity Connection. Messages recorded on the message store are not protected by the Cisco Unified CM authentication and encryption features but can be protected by the Unity Connection private secure messaging feature. For details on the Unity Connection secure messaging feature, see the Handling Messages Marked Private or Secure.

Self-encrypting drive

Cisco Unity Connection also supports self-encrypting drives (SED). This is also called Full Disk Encryption (FDE). FDE is a cryptographic method that is used to encrypt all the data that is available on the hard drive. The data include files, operating system and software programs. The hardware available on the disk encrypts all the incoming data and decrypts all the outgoing data. When the drive is locked, an encryption key is created and stored internally. All data that is stored on this drive is encrypted using that key and stored in the encrypted form. The FDE comprises a key ID and a security key.

For more information, see https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/2-0/b_Cisco_UCS_C-series_GUI_Configuration_Guide_201/b_Cisco_UCS_C-series_GUI_Configuration_Guide_201_chapter_010011.html#concept_E8C37FA4A71F4C8F8E1B9B94305AD844.

Security Mode Settings for Cisco Unified Communications Manager and Unity Connection

Cisco Unified Communications Manager and Cisco Unity Connection have the security mode options shown in Table 5: Security Mode Options for voice messaging ports (for SCCP integrations) or port groups (for SIP integrations).

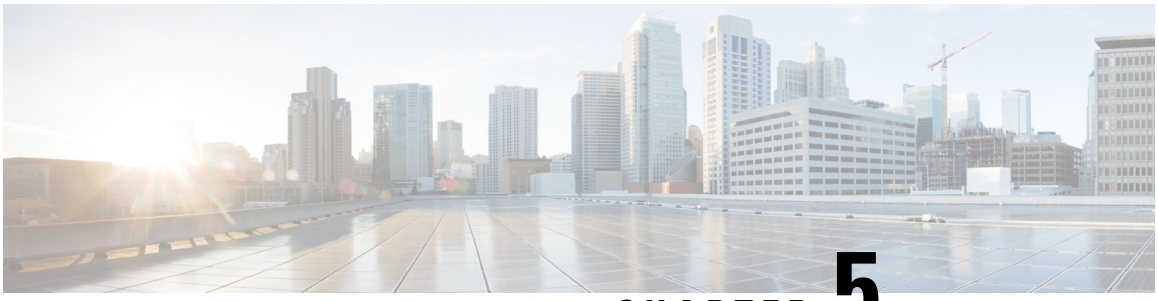
Caution The Cluster Security Mode setting for Unity Connection voice messaging ports (for SCCP integrations) or port groups (for SIP integrations) must match the security mode setting for the Cisco Unified CM ports. Otherwise, Cisco Unified CM authentication and encryption fails.

Table 5: Security Mode Options

Setting	Effect
Non-secure	The integrity and privacy of call-signaling messages are not ensured because call-signaling messages are sent as clear (unencrypted) text connected to Cisco Unified CM through a non-authenticated port rather than an authenticated TLS port. In addition, the media stream cannot be encrypted.
Authenticated	The integrity of call-signaling messages are ensured because they are connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages are not ensured because they are sent as clear (unencrypted) text. In addition, the media stream is not encrypted.
Encrypted	The integrity and privacy of call-signaling messages are ensured because they are connected to Cisco Unified CM through an authenticated TLS port, and the call-signaling messages are encrypted. In addition, the media stream can be encrypted. Both end points must be registered in encrypted mode for the media stream to be encrypted. However, when one end point is set for non-secure or authenticated mode and the other end point is set for encrypted mode, the media stream are not encrypted. Also, if an intervening device (such as a transcoder or gateway) is not enabled for encryption, the media stream is not encrypted.

Best Practices for Securing the Connection between Unity Connection, Cisco Unified Communications Manager, and IP Phones

If you want to enable authentication and encryption for the voice messaging ports on both Cisco Unity Connection and Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager SCCP Integration Guide for Unity Connection Release 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/integration/cucm_sccp/b_14cucintcucmskinny.html



CHAPTER 5

Securing Administration and Services Accounts

Securing Administration and Services Accounts

Introduction

In this chapter, you would find descriptions of potential security issues related to securing accounts; information on any actions you need to take; recommendations that help you make decisions; ramifications of the decisions you make; and in many cases, best practices.

Understanding Cisco Unity Connection Administration Accounts

A Cisco Unity Connection server has two types of administration accounts. Table 6: Administration Accounts on a Unity Connection Server summarizes the purposes for and the differences between the two types of accounts.

Table 6: Administration Accounts on a Unity Connection Server

	Operating System Administration Account	Application Administration Account
The account is used to access	• Cisco Unified Operating System Administration • Disaster Recovery System • Command line interface	• Cisco Unity Connection Administration • Cisco Unified Serviceability • Cisco Unity Connection Serviceability • Real-Time Monitoring Tool
The first account is created	During installation, when you specify the Administrator ID and password	During installation, when you specify the application user name and password

	Operating System Administration Account	Application Administration Account
How to change the account name	Not supported	Using Cisco Unity Connection Administration. **Caution** Do not change the account name using the **utils reset_ui_administrator_name** command, or Unity Connection does not function properly.
How to change the account password	Using the **set password** CLI command	• Using Cisco Unity Connection Administration • Using the **utils cuc reset password** CLI command **Caution** Do not change the account nam using the **utils reset_ui_administrator_passw** command, or Unity Connection not function properly.
How to create additional accounts	Using the **set account** CLI command	Using Cisco Unity Connection Administration **Caution** Do not create additional accounts using the **set account** command, or Unity Connection does not function properly.
How to delete accounts other than the first account	Using the **delete account** CLI command	Using Cisco Unity Connection Administration **Caution** Do not delete accounts using the **delete account** command, or Unity Connection does not function properly.
How to list administrator accounts	Using the **show account** CLI command.	Using Cisco Unity Connection Administration
Can be integrated with an LDAP user account	No	Yes

Best Practices for Accounts Used to Access Cisco Unity Connection Administration

Cisco Unity Connection Administration is a web application that you use to do most administrative tasks. An administrative account can be used to access Connection Administration to define how Cisco Unity Connection works for individual users (or for a group of users), to set system schedules, to set call management options, and to make changes to other important data, all depending on the roles to which the administrative account is assigned. If your site is comprised of multiple Unity Connection servers, an account that is used to access Connection Administration on one server may be able to authenticate and gain access to Connection Administration on the other networked servers as well. To secure access to Connection Administration, consider the following best practices.

Best Practice: Limit the Use of the Application Administration Account

Until you create a Unity Connection user account specifically for the purpose of administering Unity Connection, you sign in to Cisco Unity Connection Administration using the credentials that are associated with the default administrator account. The default administrator account is created during the installation of Unity Connection with the application user username and password you specify during installation. The default administrator account is automatically assigned to the system administrator role, which offers full system access rights to Connection Administration. This means that not only can the administration account access all pages in Connection Administration, but it also has read, edit, create, delete and execute privileges for all Connection Administration pages. For this reason, you should limit the use of this highly privileged account to only one or to very few individuals.

As an alternative to the default administrator account, you can create additional administrative accounts that are assigned to roles that have fewer privileges based on what is appropriate to the administrative tasks that each person performs.

Note Make sure you do not use the following application usernames as this generate an error:

- CCMSysUser
- WDSysUser
- CCMQRTSysUser
- IPMASysUser
- WDSecureSysUser
- CCMQRTSecureSysUser
- IPMASecureSysUser
- TabSyncSysUser
- CUCService

Best Practice: Use Roles to Provide Different Levels of Access to Cisco Unity Connection Administration

When modifying role assignments to secure access to Cisco Unity Connection Administration, consider the following best practices:

- Do not modify the role assignment of the default administrator account. Instead, create additional administrative user accounts that offer the appropriate levels of access to Connection Administration. For example, you may want to assign an administrative user account to the User Administrator role, which allows the administrator to manage user account settings and access all user administration functions. Or you may want to assign an administrative user account to the Help Desk Administrator role, which allows the administrator to reset user passwords and PINs, unlock user accounts, and view user setting pages.
- Create additional administrative user templates that are assigned to roles that provide varying levels of access. By default, the Administrator user template is assigned to the System Administrator role. Any administrative user accounts that are created from the Administrator user template is assigned to the System Administrator role, which gives administrators full access to all Unity Connection administrative functions. Use this Administrator template sparingly to create accounts for administrative users.
- By default, the Voicemail User Template is not assigned to any roles, and should not be assigned to any administrative roles. Instead, use this template to create accounts for end users with mailboxes. (The only role that should be assigned to an end user with a mailbox is the Greeting Administrator role; with this role, the only "administrative" function is to have access to the Cisco Unity Greetings Administrator, which allows users to manage the recorded greetings for call handlers by phone.)

Best Practice: Use Different Accounts to Access a Voice Mailbox and Cisco Unity Connection Administration

We recommend that Cisco Unity Connection administrators do not use the same account to access Cisco Unity Connection Administration that they use to sign in to the Cisco Personal Communications Assistant (PCA) or the phone interface.

Securing Unified Messaging Services Accounts

When you configure unified messaging for Cisco Unity Connection 14, you create one or more Active Directory accounts that Unity Connection uses to communicate with Exchange. Like any Active Directory account that has the right to access Exchange mailboxes, this account allows anyone who knows the account name and password to read mail and listen to voice messages, and to send and delete messages. The account does not have broad rights in Exchange, so you could not use it to restart an Exchange server, for example.

To secure the account, we recommend that you give the account a long password (20 or more characters) that includes upper- and lower-case characters, numbers, and special characters. The password is encrypted with AES 128-bit encryption and stored in the Unity Connection database. The database is accessible only with root access, and root access is available only with assistance from Cisco TAC.

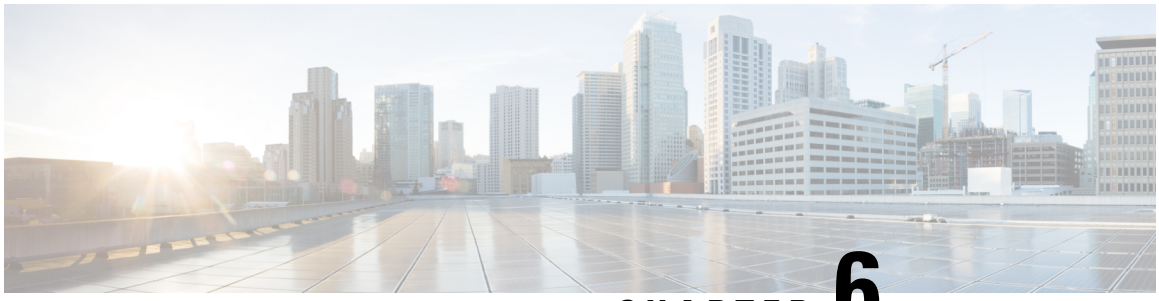
Do not disable the account, or Unity Connection cannot use it to access Exchange mailboxes.

Ensuring File Integrity

Unity Connection provides enhanced security by allowing the administrator to ensure the integrity of the files that can be downloaded from various interfaces, such as Cisco Unity Connection Administration and Cisco Unity Connection Serviceability of Cisco Unity Connection. To verify the file integrity, Unity Connection offers the SHA-512 checksum value for all download files. For example, the SHA-512 checksum value for Cisco Unified Real-Time Monitoring Tool plugin appears in the **Description** field of the Search Plugin page.

For ensuring the integrity of the file, administrator can download the file and generate the checksum for the file by using any external tool available online. Now, compare the displayed checksum with the checksum of

the downloaded file. If both the checksums of the file are same, it means there is no error in the download file.



CHAPTER 6

FIPS Compliance in Cisco Unity Connection

FIPS Compliance in Cisco Unity Connection

Introduction

FIPS, or Federal Information Processing Standard, is a U.S. and Canadian government certification standard that defines requirements that cryptographic modules must follow.

Caution FIPS mode is only supported on releases that have been through FIPS compliance. Be warned that FIPS mode should be disabled before you upgrade to a non-FIPS compliance version of Cisco Unity Connection.

For information about which releases are FIPS compliant and to view their certifications, see the FIPS 140 document at link : https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html

Certain versions of Unity Connection are FIPS 140-2 compliant, in accordance with the U.S. National Institute of Standards (NIST). They can operate in FIPS mode, level 1 compliance.

FIPS mode uses the following FIPS 140-2 level 1 validated cryptographic modules:

- CiscoSSL 1.1.1n.7.2.390 with FIPS Module CiscoSSL FOM 7.2a
- CiscoSSH -1.9.29
- RSA CryptoJ 6_2_3
- BC FIPS -1.0.2.3.jar

- BCTLS FIPS - 1.0.12.3.jar
- BCPKIX FIPS -1.0.5.jar
- Libreswan -3.25-9
- NSS -3.67

Note For more information on Unity Connection upgrades, see Upgrade Types section of the "Upgrading Cisco Unity Connection" chapter of the *Install, Upgrade and Maintenance Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html.

Running CLI Commands for FIPS

To enable the FIPS feature in Cisco Unity Connection, you use the utils fips enable CLI command. In addition to this, the following CLI commands are also available:

- utils fips disable- Use to disable the FIPS feature.
- utils fips status- Use to check the status of FIPS compliance.

For more information on the utils fips <option> CLI commands, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html.

Caution After enabling or disabling the FIPS mode, the Cisco Unity Connection server restart automatically.

Caution If the Cisco Unity Connection server is in a cluster, do not change the FIPS settings on any other node until the FIPS operation on the current node is complete and the system is back up and running.

Note Before enabling the FIPS mode on the Unity Connection server, ensure that the security password length is minimum of 14 characters. In case of upgrading Unity Connection, password needs to be updated if the prior version was FIPS enabled.

All the new certificates are signed using SHA-256 hashing algorithm in FIPS mode. When you generate a self-signed certificate or Certificate Signing Request, you can choose only SHA-256 as the hashing algorithm.

Regenerating Certificates for FIPS

Regenerating Root Certificates

Cisco Unity Connection servers with pre-existing telephony integrations must have the root certificate manually regenerated after enabling or disabling the FIPS mode. If the telephony integration uses an Authenticated or Encrypted Security mode, the regenerated root certificate must be re-uploaded to any corresponding Cisco Unified Communications Manager servers. For fresh installations, regenerating the root certificate can be avoided by enabling FIPS mode before adding the telephony integration.

Note In case of clusters, perform the following steps on all nodes.

1. Sign in to Cisco Unity Connection Administration.
2. Select Telephony Integrations> Security> Root Certificate.
3. On the View Root Certificate page, click Generate New.
4. If the telephony integration uses an Authenticated or Encrypted Security mode, continue with steps 5-10, otherwise skip to step 12.
5. On the View Root Certificate page, right-click the Right-click to Save the Root Certificate as a File link.
6. Select Save As to browse to the location to save the Cisco Unity Connection root certificate as a.pem file.

Note The certificate must be saved as a file with the extension.pem rather than.htm, else Cisco Unified CM will not recognize the certificate.

7. Copy the Cisco Unity Connection root certificate to all Cisco Unified CM servers by performing the following substeps:
   a. On the Cisco Unified CM server, sign in to Cisco Unified Operating System Administration.
   b. Select the Certificate Management option from the Security menu.
   c. Select Upload Certificate/Certificate Chain on the Certificate List page.
   d. On the Upload Certificate/Certificate Chain page, select the CallManager-trust option from the Certificate Name drop-down.
   e. Enter Cisco Unity Connection Root Certificate in the Root Certificate field.
   f. Click Browse in the Upload File field to locate and select the Cisco Unity Connection root certificate that was saved in Step 5.
   g. Click Upload File.
   h. Click Close.
8. On the Cisco Unified CM server, sign in to Cisco Unified Serviceability.
9. Select Service Management from the Tools menu.
10. On the Control Center - Feature Services page, restart the Cisco CallManager service.
11. Repeat steps 5-10 on all remaining Cisco Unified CM servers in the Cisco Unified CM cluster.
12. Restart the Unity Connection Conversation Manager Service by following these steps:

a. Sign in to Cisco Unity Connection Serviceability.
b. Select Service Management from the Tools menu.
c. Select Stop for the Unity Connection Conversation Manager service in the Critical Services section.
d. When the Status area displays a message that the Unity Connection Conversation Manager service is successfully stopped, select Start for the service.

13. New and pre-existing telephony integration ports are now correctly registered with Cisco Unified CM.

FIPS is supported for both SCCP and SIP integrations between Cisco Unified Communications Manager and Cisco Unity Connection.

For more information on managing certificates, see the "Manage Certificates and Certificate Trust Lists" section in the "Security" chapter of the *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14cucosagx.html

Regenerating Tomcat Certificates

Unity Connection supports only RSA key based Tomcat certificates to configure secure calls using SIP Integration.This allows the use of self signed as well as third-party CA signed certificate for SIP secure call. Cisco Unity Connection servers with pre-existing telephony integrations must have the Tomcat certificate manually regenerated after enabling or disabling the FIPS mode. If the telephony integration uses an Authenticated or Encrypted Security mode, the regenerated tomcat certificate must be re-uploaded to any corresponding Cisco Unified Communications Manager servers. For fresh installations, regenerating the tomcat certificate can be avoided by enabling FIPS mode before adding the telephony integration.

To learn how to regenerate certificates, see section Settings for RSA Key Based certificates of chapter "Setting Up a Cisco Unified Communications Manager SIP Trunk Integration" in *Cisco Unified Communications Manager SIP Integration Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/integration/cucm_sip/b_14cucintcucmsip.html.

Note Verify that the value entered in **X.509 Subject Name** field on SIP Trunk Security Profile Configuration page of Cisco Unified Communication Manager is the FQDN of the Unity Connection server.

Configuring Additional Settings When Using FIPS Mode

In order to maintain FIPS compliance, additional configurations are mandatory for the following features:

- Networking: Intrasite, Intersite, VPIM
- Unified Messaging: Unified Messaging Services.

Configure Networking When Using FIPS Mode

Networking from Cisco Unity Connection to another server must be secured by an IPsec policy. This includes intersite links, intrasite links, and VPIM locations. The remote server is responsible for assuring its own FIPS compliance.

Note Secure Messages are not sent in a FIPS compliant manner unless an IPsec Policy is configured.

Configure Unified Messaging When Using FIPS Mode

Unified Messaging Services require the following configuration:

- Configure IPsec policy between Cisco Unity Connection and Microsoft Exchange.
- Set the Web-Based Authentication Mode setting to Basic on the Edit Unified Messaging Service page in Unity Connection Administration. NTLM web authentication mode is not supported in FIPS mode.

Caution The IPsec policy between servers is required to protect the plain text nature of Basic web authentication.

Configure IPsec Policies Using FIPS Mode

For information on setting up IPsec policies, see the "IPSec Management" section in the "Security" chapter of the *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14cucosagx.html.

For information on the impact of IPsec policies with Unity Connection, see "Upgrading Cisco Unity Connection" chapter of *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html.

Unsupported Features When Using FIPS Mode

The following Cisco Unity Connection features are not supported when FIPS mode is enabled:

- SpeechView Transcription Service.
- SIP Digest Authentication (configured for SIP Telephony Integrations).
- SIP NTLM Authentication (configured for SIP Telephony Integration).
- Video Messaging.

Configuring Voicemail PIN For Touchtone Conversation Users To Sign-In

Enabling FIPS in Cisco Unity Connection prevents a touchtone conversation user from signing in to play or send voice messages or to change user settings if both of the following options are true:

- The user was created in Cisco Unity 5.x or earlier, and migrated to Connection.
- The Unity Connection user still has a voicemail PIN that was assigned in Cisco Unity 5.x or earlier.

A touchtone conversation user signs in by entering an ID (usually the user's extension) and a voicemail PIN. The ID and PIN are assigned when the user is created. Either an administrator or the user can change the PIN.

To prevent administrators from accessing PINs in Connection Administration, PINs are hashed. In Cisco Unity 5.x and earlier, Cisco Unity hashed the PIN by using an MD5 hashing algorithm, which is not FIPS compliant. In Cisco Unity 7.x and later, and in Unity Connection, the PIN is hashed by using an SHA-1 algorithm, which is much harder to decrypt and is FIPS compliant.

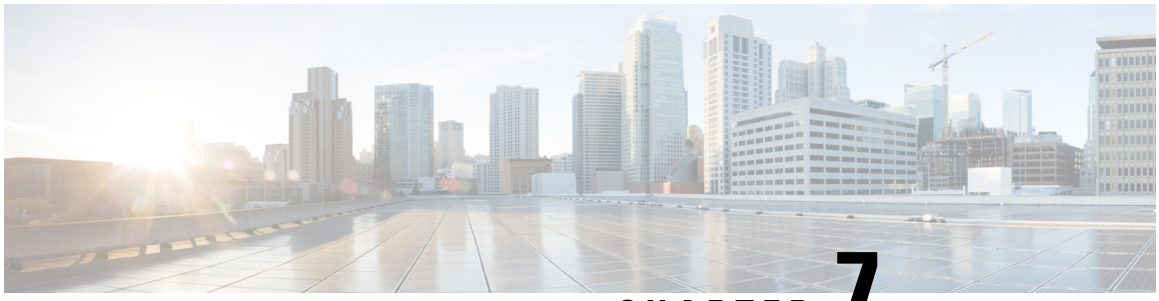
Hashing All Voicemail PIN with SHA-1 Algorithm in Unity Connection

When FIPS is enabled, Cisco Unity Connection no longer checks the database to determine whether the user's voicemail PIN was hashed with MD5 or SHA-1 algorithm. Unity Connection hashes all the voicemail PINs with SHA-1 and compares it with the hashed PIN in the Unity Connection database. The user is not allowed to sign in if the MD5 hashed voicemail PIN entered by user does not match with the SHA-1 hashed voicemail PIN in the database.

FIPS Mode Restrictions

Feature	Restrictions
SNMP v3	FIPS mode does not support SNMP v3 with MD5 or DES. If you have SNMP v3 configured while FIPS mode is enabled, you must configure **SHA** as the Authentication Protocol and **AES128** as the Privacy Protocol.
SFTP Server	By Default, the JSCH library was using ssh-rsa for SFTP connection but the FIPS mode doesn't support ssh-rsa. Due to a recent update of CentOS, the JSCH library supports both ssh-rsa (SHA1withRSA) or rsa-sha2-256 (SHA256withRSA) depending on the FIPS value after modifications. That is, **Note** • FIPS mode only supports rsa-sha2-256. • Non-FIPS mode supports both ssh-rsa and rsa-sha2-256. The rsa-sha2-256 (SHA256WithRSA) support is available only from OpenSSH 6.8 version onwards. In FIPS mode, only the SFTP servers running with OpenSSH 6.8 version onwards supports the rsa-sha2-256 (SHA256WithRSA).

Feature	Restrictions
SSH Host Key Algorithms	Deprecated Algorithm: • **ssh-rsa** (SHAlwithRSA) New Supported Algorithm: • **rsa-sha2-256** • **rsa-sha2-512** **Note** Before upgrading, we recommend you to refer the Upgrade Types section of the "Upgrading Cisco Unity Connection" chapter of the *Install, Upgrade and Maintenance Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html.
IPSec Policy	Certificate based IPSec Policy will not work when moving from Non-FIPS to FIPS or vice-versa. Perform the following when you move from Non-FIPS mode to FIPS or vice-versa. If you have a certificate based IPSec policy and its in enabled state then: **1.** Disable the IPSec policy before moving to FIPS or vice versa. **2.** Re-certify the certificate and exchange the new certificate after moving to FIPS mode or vice versa. **3.** Enable IPSec policy.



CHAPTER 7

Enhanced Security Mode in Cisco Unity Connection

Enhanced Security Mode in Cisco Unity Connection

Overview

When Unity Connection is enabled to operate in EnhancedSecurityMode, the system implements a set of strict security and risk management controls that secure the system deployment.

The EnhancedSecurityMode includes the following features:

- **Stringent Password Requirements:** A strict credential policy is implemented for new user passwords and for existing passwords when they are modified. See the Credential Policy, on page 42section.
- **Remote Audit Logging:** All audit logs and event syslogs are saved locally as well as to a remote syslog server.

  See the Remote Audit Logging, on page 42section.
- **System logging:** All system events, such as CLI logins and incorrect password attempts are logged and saved.
- **Limit log-on:** The maximum number of concurrent sessions for an interface can be configured. Any new session beyond the configured maximum limit gets disconnected. In EnhancedSecurityMode, the default value of Maximum Concurrent Sessions for **Telephony Interface (Per User)** is 2 and of **Maximum Concurrent Sessions for IMAP Interface (Per User)** is 5. For more information, see Passwords, PINs, and Authentication Rule Management chapter.
- **Disable Inactive Users:** The number of days for user inactivity timeout can be configured. If a user does not login to the voicemail account for the configured numbers of days, the account is disabled and further access is denied.

  In EnhancedSecurityMode , the default value of **User Inactivity Timeout (in Days)** is 90. For more information, see Passwords, PINs, and Authentication Rule Management

Role Based Access

In EnhancedSecurityMode , a new privilege "Super Custom Administrator" is added to the privilege list on the Custom Roles page. With the help of the "Super Custom Administrator" privilege, a system administrator can create two levels of administrator hierarchies in the system.

Credential Policy

Once the EnhancedSecurityMode is enabled, a stringent credential policy for new passwords and password changes can be implemented for platform administrator. This policy enforces the following default requirements for passwords:

- Credential Length should be between 14 to 127 characters.
- Password should contain at least 1 lowercase, 1 uppercase, 1 digit and 1 special character.
- Stored Number of Previous Credentials are 24, any of the previous 24 passwords cannot be reused.
- Credential Expires After minimum limit of 1 day and maximum limit is 60 days.
- Minimum Number of Character Changes between Successive Credentials must be at least 4.

After enabling the EnhancedSecurityMode , the administrator can use the Authentication Rules to modify any of the password requirements to enforce stringent password policy for all password changes. For information on credential policies, see the "Passwords, PINs, and Authentication Rule Management " chapter.

Remote Audit Logging

To comply with the security requirements, you must configure remote audit logging in Unity Connection.

In EnhancedSecurityMode , the system uses TCP as the default protocol to send audit events and alarms to the remote syslog server. Unlike UDP, which is used while the system is in normal operating mode, TCP contains mechanisms to guarantee delivery of all packets. However, if you prefer, you can reconfigure the system to use UDP while in this mode.

If a transfer failure occurs, the TCPRemoteSyslogDeliveryFailed alarm and alert are triggered to notify administrator about the TCP transfer failure. A throttling mechanism ensures that not more than one alarm and one alert are sent per hour. This ensures that administrator is not flooded with identical alarms and alerts. Administrator can use the local audit logs as a backup while communications are reestablished.

Prerequisites for Enhanced Security Mode

- FIPS 140-2 Mode Setup: FIPS mode must be enabled before you enable the Enhanced Security Mode . If FIPS mode is not already enabled, you will be prompted to enable FIPS mode when you attempt to enable EnhancedSecurityMode .
- Set up a remote syslog server and configure IPSec between Unity Connection and the remote server, including the gateways in between.
- Set up smart host and configure IPSec between Unity Connection and exchange where exchange acts as a smart host, including the gateways in between. For information on setting up IPsec configuration, see the "IPSEC Management" section in the "Security" chapter of the *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 14* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14cucosagx.html.

- Before enabling the Enhanced Security Mode on the Unity Connection server, ensure that the security password length is minimum of 14 characters. In case of upgrading Unity Connection, password needs to be updated if the prior version was EnhancedSecurityMode enabled.

Configuration Task Flow in EnhancedSecurityMode

Step 1 Enable the EnhancedSecurityMode in Unity Connection. See the Configuring the EnhancedSecurityMode, on page 43 section.

Step 2 Confirm that the system credential policy meets the security guidelines. See the Configuring Credential Policy, on page 43section.

Step 3 Configure Audit Framework for the mode.

Set up the audit logging framework for Unity Connection, which includes setting up remote syslog servers for all audit logs and alarms. See the Configuring Audit Framework, on page 44section.

Configuring the EnhancedSecurityMode

Use the following procedure to enable or disable the **EnhancedSecurityMode**. However, FIPS mode must be enabled before enabling the **EnhancedSecurityMode**.

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils EnhancedSecurityModestatus** command to confirm whether the status of the mode status is set to enabled or disabled.

Step 3 Run the following command to enable the **EnhancedSecurityMode** if the mode is disabled:

```
utils EnhancedSecurityMode enable
```

Similarly, you can run the **utils EnhancedSecurityMode disable** command to disable the mode.

Step 4 Repeat this procedure for all nodes of Cisco Unity Connection.

Configuring Credential Policy

Use the following procedure to update the system credential policies.

Step 1 Log in to Cisco Unity Connection Administration.

Step 2 Select **Authentication Rules** > **Edit Authentication Rule**.

Step 3 Update the authentication rules as per your requirement.

Step 4 Click **Save**.

For information on credential policies, see the "Passwords, PINs, and Authentication Rule Management" chapter.

Configuring Audit Framework

Complete the following tasks to set up audit requirements for the **EnhancedSecurityMode** in Unity Connection.

Step 1 Configure Remote Audit Log.

Set up your audit log configuration for remote audit logging.

Step 2 Configure Remote Audit Log Transfer Protocol.

(Optional) When the **EnhancedSecurityMode** is enabled, by default, the system uses TCP as the transfer protocol for remote audit logs. You can use this procedure to reconfigure the system to use UDP.

Step 3 In RTMT, set up the email server for email alerts.

Step 4 Set up the email notification for the TCPRemoteSyslogDeliveryFailed alert.

Configuring Remote Audit Logs

Before configuring remote audit logs for a Unity Connection system running in EnhancedSecurityMode, make sure that:

- You must have already set up your remote syslog server.
- You must also have configured IPSec between each cluster node and the remote syslog server, including the gateways in between.

  For information on setting up IPsec configuration, see the "IPSEC Management" section in the "Security" chapter of the *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 14* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14cucosagx.html .

Step 1 In Cisco Unified Serviceability, select**Tools** > **Audit Log Configuration**.

Step 2 From the Server drop-down menu select any server in the cluster except the publisher node and click **Go**.

Step 3 Check the **Apply to All Nodes** check box.

Step 4 In the **Server Name** field, enter the IP Address or fully qualified domain name of the remote syslog server.

Step 5 Complete the remaining fields in the Audit Log Configuration window. For help with the fields and their descriptions, see the online help.

Step 6 Click **Save**.

Configuring Remote Audit Log Transfer Protocol

Use the following procedure to configure the transfer protocol for remote audit logs. In the **EnhancedSecurityMode**, the default setting is TCP.

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils remotesyslog show protocol** command to confirm the protocol that is configured.

Step 3 If you need to change the protocol, do the following:

To configure TCP, run the **utils remotesyslog set protocol tcp** command.

To configure UDP, run the **utils remotesyslog set protocol udp** command.

Step 4 Restart the node.

Step 5 Repeat this procedure for all Unity Connection cluster nodes.

Configuring Email Server for Alert Notifications

Use the following procedure to set up your email server for alert notifications.

Step 1 In the Real-Time Monitoring Tool's System window, click **Alert Central**.

Step 2 Choose **System** > **Tools** > **Alert** > **Config Email Server**.

Step 3 In the **Mail Server Configuration** popup, enter the details for the mail server.

Step 4 Click **OK**.

Enabling Email Alerts

Use the following procedure to set up an email alert for the TCPRemoteSyslogDeliveryFailed alarm.

Step 1 In the Real-Time Monitoring Tool System area, click **Alert Central**.

Step 2 In the Alert Central window, select **TCPRemoteSyslogDeliveryFailed**.

Step 3 Select **System** > **Tools** > **Alert** > **Config Alert Action**.

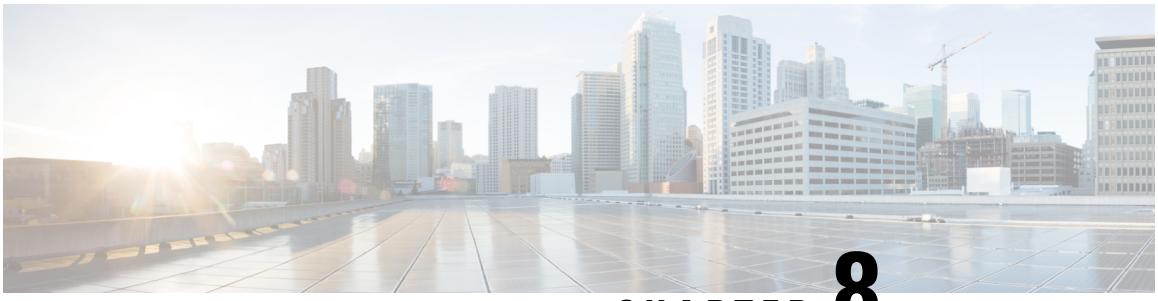
Step 4 In the Alert Action popup, select **Default** and click **Edit**.

Step 5 In the Alert Action popup, **Add a recipient**.

Step 6 In the popup window, enter the address where you want to send email alerts and click **OK**.

Step 7 In the Alert Action popup, make sure that the address appears under **Recipients** and that the **Enable** check box is checked.

Step 8 Click **OK**.



CHAPTER 8

Passwords, PINs, and Authentication Rule Management

In Cisco Unity Connection, authentication rules govern user passwords, PINs, and account lockouts for all user accounts. We recommend that you define Unity Connection authentication rules as follows:

- To require that users change their PINs and passwords often.
- To require that user PINs and passwords be unique and not easy to guess.

Well thought out authentication rules can also thwart unauthorized access to Unity Connection applications, such as Cisco Personal Communication Assistant (Cisco PCA) and Cisco Unity Connection Survivable Remote Site Voicemail, by locking out users who enter invalid PINs or passwords too many times.

In this chapter, you find information on completing the above tasks and on other issues related to PIN and password security. To help you understand the scope of Cisco Unity Connection password management, the first section in this chapter describes the different passwords required to access the Cisco Personal Communications Assistant (PCA), the Unity Connection conversation, Cisco Unity Connection Administration, and other administrative web applications. Each of the sections that follow offer information on actions you need to take; recommendations that help you make decisions; discussion of the ramifications of the decisions you make; and in many cases, best practices.

For information that guides you through the process of securing Unity Connection passwords and defining authentication rules, see the following sections.

• Passwords, PINs, and Authentication Rule Management, on page 47

Passwords, PINs, and Authentication Rule Management

In Cisco Unity Connection, authentication rules govern user passwords, PINs, and account lockouts for all user accounts. We recommend that you define Unity Connection authentication rules as follows:

- To require that users change their PINs and passwords often.
- To require that user PINs and passwords be unique and not easy to guess.

Well thought out authentication rules can also thwart unauthorized access to Unity Connection applications, such as Cisco Personal Communication Assistant (Cisco PCA) and Cisco Unity Connection Survivable Remote Site Voicemail, by locking out users who enter invalid PINs or passwords too many times.

In this chapter, you find information on completing the above tasks and on other issues related to PIN and password security. To help you understand the scope of Cisco Unity Connection password management, the first section in this chapter describes the different passwords required to access the Cisco Personal Communications Assistant (PCA), the Unity Connection conversation, Cisco Unity Connection Administration, and other administrative web applications. Each of the sections that follow offer information on actions you need to take; recommendations that help you make decisions; discussion of the ramifications of the decisions you make; and in many cases, best practices.

For information that guides you through the process of securing Unity Connection passwords and defining authentication rules, see the following sections.

About the PINs and Passwords Users Use to Access Unity Connection Applications

Cisco Unity Connection users use different PINs and passwords to access various Unity Connection applications. Knowing which passwords are required for each application is important in understanding the scope of Unity Connection password management.

Phone PINs

Users use a phone PIN to sign in to the Cisco Unity Connection conversation by phone. Users use the phone keypad to enter a PIN (which consists entirely of digits), or can say the PIN if enabled for voice recognition.

Web Application (Cisco PCA) Passwords

A user who is assigned to an administrative role may also use the web application password to sign in to the following Unity Connection applications:

- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability
- Cisco Unified Serviceability
- Real-Time Monitoring Tool
- Cisco Unity Connection SRSV Administration

Note If you are using Cisco Unified Communications Manager Business Edition (CMBE) or LDAP authentication, users must use their Cisco Unified CMBE or LDAP account passwords to access Unity Connection web applications. Ensuring That Users Are Initially Assigned Unique and Secure PINs and Passwords in Cisco Unity Connection.

To help protect Cisco Unity Connection from unauthorized access and toll fraud, every user should be assigned a unique phone PIN and web application (Cisco PCA) password.

When you add users to Unity Connection, the phone PIN and web application password are determined by the template that is used to create the user account. By default, user templates are assigned randomly generated strings for the phone PIN and web password. All users created from a template are assigned the same PIN and password.

Consider the following options to ensure that each user is assigned a unique and secure PIN and password at the time that you create the account, or immediately thereafter:

- If you are creating a small number of user accounts, after you have used Cisco Unity Connection Administration to create the accounts, change the phone PIN and web password for each user on the Users > Users > Change Password page. Alternatively, instruct users to sign in as soon as possible to change their PINs and passwords (if you choose this option, also ensure that the User Must Change at Next Sign-In check box is checked on the Edit Password page of the template you used to create the accounts).
- If you are creating multiple user accounts, use the Bulk Password Edit tool to assign unique passwords and PINs to Unity Connection end user accounts (users with mailboxes) after they have been created. You use the Bulk Password Edit tool along with a CSV file that contains unique strings for the passwords and PINs to apply the passwords/PINs in bulk.

The Bulk Password Edit tool is a Windows-based tool. Download the tool and view Help at http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html.

Unity Connection SRSV Passwords and Shared Secrets

All the requests initiated from the central Unity Connection server to the Unity Connection SRSV server use administrator credentials of Unity Connection SRSV for communication whereas the requests from Unity Connection SRSV to Unity Connection use secret tokens for authentication.

The central Unity Connection server uses the administrator username and password of Unity Connection SRSV to authenticate access to the server. The username and password of Unity Connection SRSV get stored in the Connection database as you create a new branch on the central Unity Connection server.

During each provisioning cycle with Unity Connection SRSV, the central Unity Connection server generates a secret token and shares the token with Unity Connection SRSV. After the provisioning is completed from the Unity Connection SRSV site, it notifies the central Unity Connection server using the same token. Then this token is removed from both the central Unity Connection and Unity Connection SRSV servers as soon as the provisioning cycle is completed. This concept of runtime token keys is known as shared secrets.

For more information on Unity Connection SRSV, refer to the Complete Reference Guide for Cisco Unity Connection Survivable Remote Site Voicemail (SRSV) Release 14 at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/srsv/guide/b_14cucsrsvx.html.

Changing Web Application Passwords

You can change the web application (Cisco PCA) password for an individual user on the Users > Users > Change Password page in Cisco Unity Connection Administration at any time.

When passwords expire, users and administrators is required to enter a new password when they next attempt to sign in to the Cisco PCA or Connection Administration.

Users can also change their Cisco PCA passwords in the Unity Connection Messaging Assistant.

To change passwords for multiple end user accounts (users with mailboxes), you can use the Bulk Password Edit tool to assign unique new passwords to the accounts. You use the Bulk Password Edit tool along with a CSV file that contains unique strings for the passwords to apply the passwords in bulk. The Bulk Password Edit tool is a Windows-based tool. Download the tool and view Help at X http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html. You can also use the Cisco Unity Connection Bulk Administration Tool (BAT) to change multiple user passwords at one time.

For users who are able to access voice messages in an IMAP client, make sure that they understand that whenever they change their Cisco PCA password in the Messaging Assistant, they also must update the password in their IMAP client. Passwords are not synchronized between IMAP clients and the Cisco PCA.

Best Practice:

Specify a long—eight or more characters—and non-trivial password. Encourage users to follow the same practice whenever they change their passwords, or assign them to an authentication rule that requires them to do so. Cisco PCA passwords should be changed every six months.

Changing Phone PINs

You can change the phone PIN for an individual user on the Users > Users > Change Password page in Cisco Unity Connection Administration at any time.

Users can use the Unity Connection phone conversation or the Unity Connection Messaging Assistant to change their phone PINs.

To change PINs for multiple end user accounts (users with mailboxes), you can use the Bulk Password Edit tool to assign unique new PINs to the accounts. You use the Bulk Password Edit tool along with a CSV file that contains unique strings for the PINs to apply the PINs in bulk. The Bulk Password Edit tool is a Windows-based tool. Download the tool and view Help at http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html. You can also use the Cisco Unity Connection Bulk Administration Tool (BAT) to change multiple user PINs at one time.

When PINs expire, users are required to enter a new PIN when they next attempt to sign in to the Unity Connection conversation.

Because users can use the Messaging Assistant to change their phone PINs, they can help ensure the security of their PINs by taking appropriate measures also to keep their web application (Cisco PCA) passwords secure.

Users need to understand that the phone PIN and Cisco PCA password are not synchronized. While first-time enrollment prompts them to change their initial phone PIN, it does not let them change the password that they use to sign in to the Cisco PCA website.

Best Practice:

Each user should be assigned a unique PIN that is six or more digits long and non-trivial. Encourage users to follow the same practice or assign them to an authentication rule that requires them to do so.

Defining Authentication Rules to Specify Password, PIN, and Lockout Policies

Note Cisco Unity Connection authentication rules are not applicable to managing user passwords in Cisco Unified Communications Manager Business Edition (CMBE), or when LDAP authentication is enabled, because authentication is not handled by Unity Connection in those cases.

Use authentication rules to customize the sign-in, password, and lockout policies that Cisco Unity Connection applies when users access Unity Connection by phone, and how users access Cisco Unity Connection Administration, the Cisco PCA, and other applications such as IMAP clients.

The settings that you specify on the Edit Authentication Rule page in Connection Administration determine:

- The number of failed sign-in attempts to the Unity Connection phone interface, the Cisco PCA, or Connection Administration that are allowed before an account is locked.
- The number of minutes an account remains locked before it is reset.
- Whether a locked account must be unlocked manually by an administrator.
- The minimum length allowed for passwords and PINs.
- The number of days before a password or PIN expires.

Best Practices:

For increased security, we recommend the following best practices when defining authentication rules:

- Require that users change their Unity Connection passwords and PINs at least once every six months.
- Require web application passwords to be eight or more characters and non-trivial.
- Require voicemail PINs to be six or more characters and non-trivial.

For greater security, establish authentication rules that prevent PINs and passwords from being easy to guess and from being used for a long time. At the same time, is also best to avoid requiring PINs and passwords that are so complicated or that must be changed so often that users have to write them down to remember them.

In addition, use the following guidelines as you specify authentication rules in the following fields:

Failed Sign-In __ Attempts:

Use this field to indicate how Unity Connection handles situations when a user repeatedly enters an incorrect PIN or password. We recommend that you set the field to lock user accounts after three failed sign-in attempts.

Reset Failed Sign-In Attempts Every __ Minutes:

Use this field to specify the number of minutes after which Unity Connection clear the count of failed sign-in attempts (unless the failed sign-in limit is already reached and the account is locked). We recommend that you set the field to clear the count of failed sign-in attempts after 30 minutes.

Lockout Duration:

Use this field to specify the length of time that a user who is locked out must wait before attempting to sign in again.

For even tighter security, you can check the Administrator Must Unlock check box, which prevents users from accessing their accounts until an administrator unlocks them on the applicable User > Password Settings page. Check the Administrator Must Unlock check box only if an administrator is readily available to assist users or if the system is prone to unauthorized access and toll fraud.

Credential Expires After __ Days:

As a best practice, do not enable the Never Expires option. Instead, confirm that this field has a value greater than zero so that users are prompted to change their passwords every X days (X is the value specified in the Credential Expires After field).

We recommend that you configure web passwords to expire after 120 days and phone PINs to expire after 180 days.

Minimum Credential Length:

As a best practice, set this field to six or higher.

For authentication rules that are used for web application passwords, we recommend that you require users to use passwords that are eight or more characters in length.

For authentication rules that are used for phone PINs, we recommend that you require users to use PINs that are six or more digits in length.

When you change the minimum credential length, users are required to use the new length the next time that they change their PINs and passwords.

Minimum Number of Character Changes between Successive Credentials:

Use this field to specify the number of characters that a user must change while updating the web application password.(not applicable for PIN)

The value of this field should be less than or equal to the value of Minimum Credential Length.

By default, the value of this field is set to 1, which means that the user must change at least one character between old password and new password.

Stored Number of Previous Credentials:

As a best practice, specify a number in this field. By doing so, you enable Unity Connection to enforce password uniqueness by storing a specified number of previous passwords or PINs for each user. When users change passwords and PINs, Unity Connection compares the new password or PIN with those stored in the credential history. Unity Connection rejects any password or PIN that matches a password or PIN stored in the history.

By default, Unity Connection stores 5 passwords or PINs in credential history.

Check For Trivial Passwords:

As a best practice, confirm that this field is enabled so that users must use non-trivial PINs and passwords.

A non-trivial phone PIN has the following attributes:

- The PIN cannot match the numeric representation of the first or last name of the user.
- The PIN cannot contain the primary extension or alternate extensions of the user.
- The PIN cannot contain the reverse of the primary extension or alternate extensions of the user.
- The PIN cannot contain groups of repeated digits, such as “408408” or “123123.”
- The PIN cannot contain only two different digits, such as “121212.”
- A digit cannot be used more than two times consecutively (for example, “28883”).
- The PIN cannot be an ascending or descending group of digits (for example, “012345” or “987654”).
- The PIN cannot contain a group of numbers that are dialed in a straight line on the keypad when the group of digits equals the minimum credential length that is allowed (for example, if 3 digits is allowed, the user could not use “123,” “456,” or “789” as a PIN).

A non-trivial web application password has the following attributes:

- The password must contain at least three of the following four characters: an uppercase character, a lowercase character, a number, or a symbol.
- The password cannot contain the user alias or its reverse.
- The password cannot contain the primary extension or any alternate extensions.

- A character cannot be used more than three times consecutively (for example, !Cooool).
- The characters cannot all be consecutive, in ascending or descending order (for example, abcdef or fedcba).

Changing the Unity Connection SRSV User PIN

If you want to change the PIN of a Unity Connection SRSV user, you can do it through the Cisco Unity Connection Administration interface. After changing the PIN of the selected user, you need to provision the associated branch to update the user information in the Unity Connection SRSV database.

Note You cannot change the PIN of an SRSV user through Cisco Unity Connection SRSV Administration interface.

Restricting the Concurrent Session Limit

Unity Connection provides enhanced security by allowing the administrator to restrict the concurrent sessions that a user can have on the following interfaces:

- **Telephony Interface**: On telephony interface, if a user attempts a new session beyond the configured maximum limit, the call gets disconnected.
- **Visual Voicemail Interface** *(PIN Based Authentication)*: On visual voicemail interface, if a user attempts a new session beyond the configured maximum limit, the user is not allowed to login to the interface.

  Telephony or visual voicemail sessions includes calling from both primary extension as well as alternate extension. To enable the feature on both the interfaces, login to Cisco Unity Connection Administration, navigate to **System Settings** > **Advanced** > **Conversations** and enter a value for the maximum concurrent sessions in the **Maximum Concurrent Sessions for Telephony Interface (Per User)** field.

- **IMAP Interface**: On IMAP interface, if a user tries to login to an IMAP account beyond the configured limit, the login attempt fails. To enable the feature on IMAP interface, login to Cisco Unity Connection Administration, navigate to **System Settings** > **Advanced** > **Messaging** and enter a value for the maximum concurrent sessions in the **Maximum Concurrent Sessions for IMAP Interface (Per User)** field.

By default, the value of **Maximum Concurrent Sessions for Telephony Interface (Per User)** and **Maximum Concurrent Sessions for IMAP Interface (Per User)** field is set to zero, which means that the feature is disabled.

Note In case of Outlook 2010, the recommended minimum value for the field is 4 and for Outlook 2013, the recommended value is 2.

Configuring Inactivity Timeout

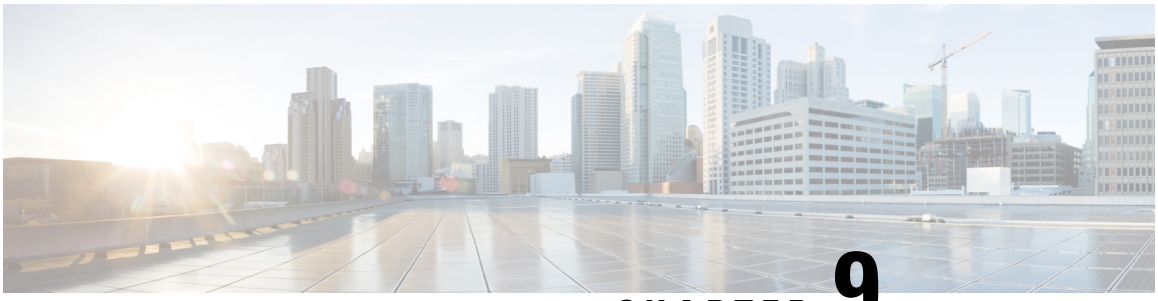
Unity Connection provides a new feature for enhanced security by allowing administrator to configure the number of days for user inactivity timeout. If a user does not login to the voicemail account from any of the Unity Connection interface, such as TUI or Web Inbox for configured numbers of days, the account is disabled and further access is denied.

To enable this feature, login to Cisco Unity Connection Administration, navigate to **System Settings** > **Advanced** > **Connection Administration** and enter a value for the inactivity timeout in the **User Inactivity Timeout (in Days)** field.

Note By default, the value of **User Inactivity Timeout (in Days)** field is set to zero, which means that the feature is disabled.

When the feature is enabled the following settings are applicable to Unity Connection:

- You can search the inactive users by limiting the search criterion to **Inactive Users** at **Users** > **Search Users** page of Cisco Unity Connection Administration.
- You can update the **VoiceMail Application Access** for the user to **Active** or **Inactive** at **Users** > **Edit User Basics** page of Cisco Unity Connection Administration.
- The **Check Inactive Users** sysagent task can be scheduled to run at configured intervals and mark a user inactive if the user has not logged in for more than configured number of days.



CHAPTER 9

Cisco Unity Connection Security Password

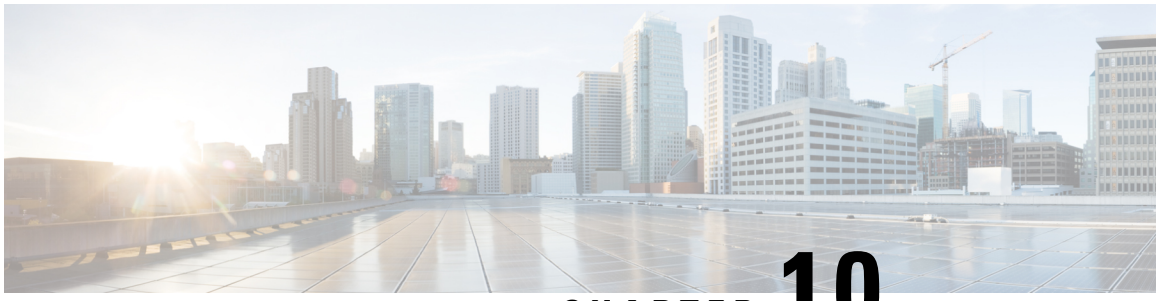
Cisco Unity Connection Security Password

About Security Password

During Unity Connection installation, you specify a security password that is not associated with any user. The password has two purposes:

- When a Unity Connection cluster is configured, the two servers in a cluster use the security password to authenticate with one another before replicating data. If you change the security password on one server in a cluster, you must also change the password on the other server, or the two servers cannnot replicate data or messages.
- Regardless of whether a cluster is configured, the security password is used as the encryption key for the Disaster Recovery System. If you back up a Unity Connection server, change the security password, and then try to restore data from the backup, you must enter the security password that was in effect when you backed up the server. (If the current security password matches the security password with which the backup was made, you do not need to specify the password to restore data.)

To change the security password, use the **set password user** CLI command. For more information, including the sequence in which you change the password on the servers in a cluster, see the applicable version of the Command Line Interface Reference Guide for Cisco Unified Communications Solutions *Release 14* at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html.



CHAPTER 10

Using SSL to Secure Client/Server Connections

Using SSL to Secure Client/Server Connections

Introduction

This chapter contains information on creating a certificate signing request, issuing an SSL certificate (or having it issued by an external certification authority), and installing the certificate on the Cisco Unity Connection server to secure Cisco Personal Communications Assistant (Cisco PCA) and IMAP email client access to Cisco Unity Connection.

The Cisco PCA website provides access to the web tools that users use to manage messages and personal preferences with Unity Connection. Note that IMAP client access to Unity Connection voice messages is a licensed feature.

Related Documentation

This chapter contains several instances where a user needs to create, generate, download and upload the Certificate Signing Request (CSR) using Multi-Server certificates or Single-Server Certificate. For more information see the chapter 'Security' of *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14cucosagx.html.

Deciding the Installation of a SSL Certificate to Secure Cisco PCA, Unity Connection SRSV, and IMAP Email Client Access to Unity Connection

When you install Unity Connection, a local self-signed certificate is automatically created and installed to secure communication between the Cisco PCA and Unity Connection, communication between IMAP email clients and Unity Connection, and communication between Unity Connection SRSV and the central Unity Connection server. This means that all the network traffic (including usernames, passwords, other text data, and voice messages) between the Cisco PCA and Unity Connection is automatically encrypted, the network traffic between IMAP email clients and Unity Connection is automatically encrypted if you enable encryption in the IMAP clients, and the network traffic between Unity Connection SRSV and the central Unity Connection

server is automatically encrypted. However, if you want to reduce the risk of man-in-the-middle attacks, do the procedures in this chapter.

If you decide to install an SSL certificate, we recommend that you also consider adding the trust certificate of the certification authority to the Trusted Root Store on user workstations. Without the addition, the web browser displays security alerts for users who access the Cisco PCA and for users who access Unity Connection voice messages with some IMAP email clients.

For information on managing security alerts, see the "Managing Security Alerts When Using Self-Signed Certificates with SSL Connections" section in "Setting Up Access to the Cisco Personal Communications Assistant" chapter of *User Workstation Setup Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/user_setup/guide/b_14cucuwsx.html.

For more information on self-signed certificate, refer to the "Security in Cisco Unity Connection Survivable Remote Site Voicemail" chapter of *Complete Reference Guide for Cisco Unity Connection Survivable Remote Site Voicemail (SRSV), Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/srsv/guide/b_14cucsrsvx.html.

Securing Connection Administration, Cisco PCA, Unity Connection SRSV, and IMAP Email Client Access to Unity Connection

Do the following tasks to create and install an SSL server certificate to secure Cisco Unity Connection Administration, Cisco Personal Communications Assistant, Unity Connection SRSV, and IMAP email client access to Cisco Unity Connection:

1. If you are using Microsoft Certificate Services to issue certificates, install Microsoft Certificate Services.
2. If you are using another application to issue certificates, install the application. See the manufacturer documentation for installation instructions. Then skip to Task 3.

   If you are using an external certification authority to issue certificates, skip to Task 3.

Note If you already have installed Microsoft Certificate Services or another application that can create certificate signing requests, skip to Task 3.

3. If a Unity Connection cluster is configured, run the `set web-security` CLI command or generate a Multi-server SAN certificate (for SIP integration only) for both Unity Connection servers in the cluster and assign both servers the same alternate name. The alternate name is automatically be included in the certificate signing request and in the certificate. For information on the `set web-security` CLI command, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
4. If a Unity Connection cluster is configured, configure a DNS A record that contains the alternate name that you assigned in Task 3. List the publisher server first. This allows all IMAP email applications, Cisco Personal Communications Assistant, and Unity Connection SRSV to access Unity Connection voice messages using the same Unity Connection server name.
5. Create a certificate signing request. Then download the certificate signing request to the server on which you installed Microsoft Certificate Services or another application that issues certificates, or download the request to a server that you can use to send the certificate signing request to an external CA.

If a Unity Connection cluster is configured with Single-server certificate signing request, do this task for both servers in the Unity Connection cluster.

6. If you are using Microsoft Certificate Services to export the root certificate and to issue the server certificate, see

   If you are using another application to issue the certificate, see the documentation for the application for information on issuing certificates.

   If you are using an external CA to issue the certificate, send the certificate signing request to the external CA. When the external CA returns the certificate, continue with Task 7.

   Only PEM-formatted (also known as Base-64 encoded DER) certificates can be uploaded to Unity Connection. The certificate must have a .pem filename extension. If the certificate is not in this format, you can usually convert what you have to PEM format using freely available utilities like OpenSSL.

   If a Unity Connection cluster is configured with Single-server certificate signing request, do this task for both servers in the Unity Connection cluster

7. Upload the root certificate and the server certificate to the Unity Connection server.

   If a Unity Connection cluster is configured with Single-server certificate signing request, do this task for both servers in the Unity Connection cluster.

8. Restart the Unity Connection IMAP Server service so that Unity Connection and the IMAP email clients use the new SSL certificates. Do the Restarting the Connection IMAP Server Service.

   If a Unity Connection cluster is configured, do this task for both servers in the Unity Connection cluster.

9. To prevent users from seeing a security alert whenever they access Unity Connection using the Connection Administration, Cisco PCA, or an IMAP email client, do the following tasks on all computers from which users access Unity Connection:

   Import the server certificate that you uploaded to the Unity Connection server in Task 7 into the certificate store. The procedure differs based on the browser or IMAP email client. For more information, see the documentation for the browser or IMAP email client.

   Import the server certificate that you uploaded to the Unity Connection server in Task 7 into the Java store. The procedure differs based on the operating system running on the client computer. For more information, see the operating system documentation and the Java Runtime Environment documentation.

Restarting the IMAP Server Service

Step 1 Sign in to Cisco Unity Connection Serviceability.

Step 2 On the Tools menu, select **Service Management**.

Step 3 In the Optional Services section, for the Connection IMAP Server service, select **Stop**.

Step 4 When the Status area displays a message that the Connection IMAP Server service was successfully stopped, select **Start** for the service.

Securing Access to Cisco Unified MeetingPlace

To secure access to MeetingPlace, do the following tasks.

1. Configure SSL for MeetingPlace. For more information, see the "Configuring SSL for the Cisco Unified MeetingPlace Application Server" chapter of the *Administration Documentation for Cisco Unified MeetingPlace Release 8.0* at https://www.cisco.com/c/en/us/support/conferencing/unified-meetingplace/products-maintenance-guides-list.html.
2. Integrate Unity Connection with MeetingPlace. When you configure Unity Connection for the MeetingPlace calendar integration, specify SSL for the security transport.
3. On the Unity Connection server, upload the root certificate of the certification authority from which you got the server certificate that you installed on the MeetingPlace server in Task 1. Note the following:
4. The root certificate is not the same thing as the certificate that was installed on the MeetingPlace server. The root certificate for the certification authority contains a public key that can be used to verify the authenticity of the certificate uploaded to the MeetingPlace server.

- The root certificate is not the same thing as the certificate that was installed on the MeetingPlace server. The root certificate for the certification authority contains a public key that can be used to verify the authenticity of the certificate uploaded to the MeetingPlace server.
- Only PEM-formatted (also known as Base-64 encoded DER) certificates can be uploaded to Unity Connection. The certificate must have a .pem filename extension. If the certificate is not in this format, you can usually convert what you have to PEM format using freely available utilities like OpenSSL.
- The root certificate filename must not contain any spaces.

Securing Communication between Unity Connection and Cisco Unity Gateway Servers

Do the following tasks to create and install an SSL server certificate to secure Connection Administration, Cisco Personal Communications Assistant, and IMAP email client access to Unity Connection when networking is configured on Unity Connection:

1. If you are using Microsoft Certificate Services to issue certificates, install Microsoft Certificate Services. For information on installing Microsoft Certificate Services on a server running a later version of Windows Server, refer to Microsoft documentation.

   If you are using another application to issue certificates, install the application. See the manufacturer documentation for installation instructions. Then skip to Task 2.

   If you are using an external certification authority to issue certificates, skip to Task 2.

Note If you already have installed Microsoft Certificate Services or another application that can create certificate signing requests, skip to Task 2.

2. If a Unity Connection cluster is configured for the Unity Connection gateway server, run the `set web-security` CLI command on both Unity Connection servers in the cluster and assign both servers the same alternate name. The alternate name is automatically included in the certificate signing request and in the certificate. For information on the `set web-security` CLI command, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html.

3. If a Unity Connection cluster is configured for the Unity Connection gateway server, configure a DNS A record that contains the alternate name that you assigned in Task 2. List the publisher server first. This allows Cisco Unity to access Unity Connection voice messages using the same Unity Connection server name.

Note On the Unity Connection gateway server, create a certificate signing request. Then download the certificate signing request to the server on which you installed Microsoft Certificate Services or another application that issues certificates, or download the request to a server that you can use to send the certificate signing request to an external CA. If a Unity Connection cluster is configured, do this task for both servers in the Unity Connection cluster.

Note On the Cisco Unity gateway server, create a certificate signing request. Then download the certificate signing request to the server on which you installed Microsoft Certificate Services or another application that issues certificates, or download the request to a server that you can use to send the certificate signing request to an external CA. If Cisco Unity failover is configured, do this task for the primary and secondary servers.

4. If you are using Microsoft Certificate Services to export the root certificates and to issue the server certificates, do the procedure in the "Exporting the Root Certificate and Issuing the Server Certificate (Microsoft Certificate Services Only)".

   If you are using another application to issue the certificate, see the documentation for the application for information on issuing certificates.

   If you are using an external CA to issue certificates, send the certificate signing request to the external CA. When the external CA returns the certificates, continue with Task 7.

   Only PEM-formatted (also known as Base-64 encoded DER) certificates can be uploaded to Unity Connection. The certificate must have a pem filename extension. If the certificate is not in this format, you can usually convert what you have to PEM format using freely available utilities like OpenSSL.

   Do this task for the Unity Connection server (both servers if a Unity Connection cluster is configured) and for the Cisco Unity server (both servers if failover is configured).

5. Upload the root certificate and the server certificate to the Unity Connection server.

Note If a Unity Connection cluster is configured, do this task for both servers in the Unity Connection cluster.

6. Restart the Unity Connection IMAP Server service so that Unity Connection and the IMAP email clients use the new SSL certificates. Do the "Restarting the IMAP Server Service".

   If a Unity Connection cluster is configured, do this task for both servers in the Unity Connection cluster.

7. Upload the root certificate and the server certificate to the Cisco Unity server.

Note If failover is configured, do this task for the primary and secondary servers.

Creating and Downloading a Certificate Signing Request on a Cisco Unity Gateway Server

Step 1 On the Windows Start menu, select **Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

Step 2 Expand the name of the Cisco Unity server.

Step 3 Expand **Web Sites**.

Step 4 Right-click **Default Web Site**, and select **Properties**.

Step 5 In the Default Web Site Properties dialog box, select the **Directory Security** tab.

Step 6 Under Secure Communications, select **Server Certificate**.

Step 7 In the Web Server Certificate Wizard:

a) Select **Next**.
b) Select **Create a New Certificate**, and select **Next**.
c) Select **Prepare the Request Now, But Send It Later**, and select **Next**.
d) Enter a name and a bit length for the certificate.

We strongly recommend that you choose a bit length of 512. Greater bit lengths may decrease performance.

e) Select **Next**.
f) Enter the organization information, and select **Next**.
g) For the common name of the site, enter either the system name of the Cisco Unity server or the fully qualified domain name.

Caution The name must exactly match the name that the Unity Connection site gateway server uses to construct a URL to access the Cisco Unity server. This name is the value of the Hostname field in Connection Administration on the Networking > Links > Intersite Links page.

h) Select **Next**.
i) Enter the geographical information, and select **Next**.
j) Specify the certificate request filename and location, and write down the filename and location because you need the information in the next procedure.
k) Save the file to a disk or to a directory that the certificate authority (CA) server can access.
l) Select **Next**.
m) Verify the request file information, and select **Next**.
n) Select **Finish** to exit the Web Server Certificate wizard.

Step 8 Select **OK** to close the Default Web Site Properties dialog box.

Step 9 Close the Internet Information Services Manager window.

Restarting the Connection IMAP Server Service

Step 1 Sign in to Cisco Unity Connection Serviceability.

Step 2 On the Tools menu, select **Service Management**.

Step 3 In the Optional Services section, for the Connection IMAP Server service, select **Stop**.

Step 4 When the Status area displays a message that the Connection IMAP Server service was successfully stopped, select **Start** for the service.

Uploading the Root and Server Certificate to the Cisco Unity Server

Step 1 On the Cisco Unity server, install the Certificates MMC for the computer account.

Step 2 Upload the certificates. For more information, refer to Microsoft documentation.

Installing Microsoft Certificate Services (Windows Server 2008)

If you want to use a third-party certificate authority to issue SSL certificates, or if Microsoft Certificate Services is already installed, skip this section.

Step 1 Open Server Manager, click Add Roles, click Next, and click Active Directory Certificate Services. Click Next two times.

Step 2 On the Select Role Services page, click Certification Authority. Click Next.

Step 3 On the Specify Setup Type page, click Standalone or Enterprise. Click Next.

Note You must have a network connection to a domain controller in order to install an enterprise CA.

Step 4 On the Specify CA Type page, click Root CA. Click Next.

Step 5 On the Set Up Private Key page, click Create a new private key. Click Next.

Step 6 On the Configure Cryptography page, select a cryptographic service provider, key length, and hash algorithm. Click Next.

Step 7 On the Configure CA Name page, create a unique name to identify the CA. Click Next.

Step 8 On the Set Validity Period page, specify the number of years or months that the root CA certificate is valid. Click Next.

Step 9 On the Configure Certificate Database page, accept the default locations unless you want to specify a custom location for the certificate database and certificate database log. Click Next.

Step 10 On the Confirm Installation Options page, review all of the configuration settings that you have selected. If you want to accept all of these options, click Install and wait until the setup process has finished.

Step 11 Right click the Active Directory Certificate Authority. Select Add Role Services and select the check box for Certificate Authority Web Enrollment, Online Responder, Network Device Enrollment Service and install these services.

Step 12 Go to Server Manager -> Add Role -> Next-> check the Web Server (IIS) box and install it.

Step 13 Right click the Web Server (IIS). Select Add Role Services and check all the role services and install them.

Exporting the Root Certificate and Issuing the Server Certificate (Microsoft Certificate Services Only)

Step 1 On the server on which you installed Microsoft Certificate Services, sign in to Windows using an account that is a member of the Domain Admins group.

Step 2 On the Windows Start menu, select **Programs** > **Administrative Tools** > **Certification Authority**.

Step 3 In the left pane, expand **Certification Authority (Local)** > **<Certification authority name**, where <Certification authority name> is the name that you gave to the certification authority when you installed Microsoft Certificate Services in the Installing Microsoft Certificate Services (Windows Server 2008).

Step 4 Export the root certificate:

a) Right-click the name of the certification authority, and select **Properties**.
b) On the General tab, select **View Certificate**.
c) Select the **Details** tab.
d) Select **Copy to File**.
e) On the Welcome to the Certificate Export Wizard page, select **Next**.
f) On the Export File Format page, select **Next** to accept the default value of **DER Encoded Binary X.509 (.CER)**.
g) On the File to Export page, enter a path and filename for the .cer file. Select a network location that you can access from the Unity Connection server.

   Write down the path and filename. You need it in a later procedure.

h) Follow the onscreen prompts until the wizard has finished the export.
i) Select **OK** to close the Certificate dialog box, and select **OK** again to close the Properties dialog box.

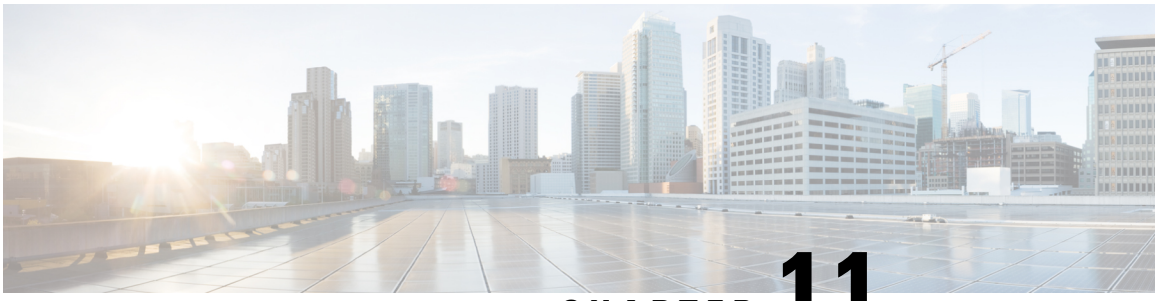
Step 5 Issue the server certificate:

a) Right-click the name of the certification authority, and select **All Tasks > Submit New Request**.
b) Browse to the location of the certificate signing request file that you created in the and double-click the file.
c) In the left pane of Certification Authority, select **Pending Requests**.
d) Right-click the pending request that you submitted in b., and select **All Tasks > Issue**.
e) In the left pane of Certification Authority, select **Issued Certificates**.
f) Right-click the new certificate, and select **All Tasks > Export Binary Data**.
g) In the Export Binary Data dialog box, in the Columns that Contain Binary Data list, select **Binary Certificate**.
h) Select **Save Binary Data to a File**.
i) Select **OK**.
j) In the Save Binary Data dialog box, enter a path and filename. Select a network location that you can access from the Cisco Unity Connection server.

   Write down the path and filename. You need it in a later procedure.

k) Select **OK**.

Step 6 Close Certification Authority.



CHAPTER 11

Securing User Messages

Securing User Messages

Introduction

By setting message sensitivity, users can control who can access a voice message and whether it can be redistributed to others. Cisco Unity Connection also offers ways for you to prevent users from saving voice messages as WAV files to their hard drives or other locations outside the Unity Connection server, enabling you to maintain control of how long messages are retained before they are archived or purged. Unity Connection also offers methods for managing the secure deletion of messages.

Handling Messages Marked Private or Secure

When users send messages by phone in Cisco Unity Connection, the messages can be marked private, secure, or both private and secure. You can also specify whether Unity Connection marks messages that are left by outside callers as private, secure, or both.

Private Messages

- A private message can be forwarded and can be saved locally as a WAV file when accessed from an IMAP client unless you specify otherwise. (See the Message Security Options for IMAP Client Access to learn how to prohibit users from playing and forwarding private messages and from saving private messages as WAV files.)
- When users reply to a private message, the reply is marked private.
- When users send a message, they can choose to mark it private.
- When outside callers leave a message, they can choose to mark it private if the system is configured with message delivery and sensitivity option for private messages
- When users do not explicitly sign in to their mailboxes before leaving messages for other users, they can choose to mark it private (if the system is configured with that option).
- By default, Unity Connection relays private messages (as regular messages with the private flag) for users who have one or more message actions configured to relay messages to an SMTP relay address.

To disable relaying of private messages, uncheck the Allow Relaying of Private Messages check box on the System Settings > Advanced > Messaging page in Cisco Unity Connection Administration.

Secure Messages

- Secure messages are stored only on the Unity Connection server, allowing you to control how long messages are retained before they are archived or permanently deleted. For secure messages, the Save Recording As option is automatically disabled on the Media Player in Cisco Unity Connection ViewMail for Microsoft Outlook, and Cisco Unity Connection ViewMail for IBM Lotus Notes.
- Secure messages can be useful for enforcing your message retention policy. You can configure Unity Connection to automatically delete secure messages that are older than a specified number of days, regardless of whether users have listened to or touched the messages in any way.
- Secure messages can be played using the following interfaces:
  - Unity Connection phone interface
  - Web Inbox
  - Cisco ViewMail for Microsoft Outlook (version 8.5 and later)
  - Cisco Unity Connection ViewMail for IBM Lotus Notes
  - Cisco Unified Mobile Communicator and Cisco Mobile
  - Cisco Unified Messaging with IBM Lotus Sametime version 7.1.1 and later. (For requirements for playing secure messages using Cisco Unified Messaging with Lotus Sametime, see the applicable Release Notes for Cisco Unified Messaging with IBM Lotus Sametime at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html)
- Secure messages can be forwarded using the following interfaces:
  - Unity Connection phone interface
  - Web Inbox
  - Cisco Unity Connection ViewMail for Microsoft Outlook 8.5
- Secure messages cannot be accessed using the following interfaces:
  - IMAP clients (unless ViewMail for Outlook or ViewMail for Notes is installed)
  - RSS readers
- By default, only Unity Connection users who are homed on the local networking site can receive a secure message. VPIM contacts or users homed on a remote networking site may also be able to receive the message, but only when the VPIM location or intersite link is configured to allow secure message delivery. Message security cannot be guaranteed once a message leaves the Unity Connection site or is sent to a VPIM location.
- Replies to secure messages are also marked secure.
- A secure message can be forwarded to other Unity Connection users and to the Unity Connection users in a distribution list. The forwarded message is also marked secure. Users cannot change the sensitivity of forwarded messages and replies.

- When users sign in to Unity Connection and send a message, class of service settings determine whether the message is marked secure. By default, Unity Connection automatically marks a message secure when the user marks it private.
- If you want Unity Connection to announce to users that a message is marked secure, check the Announce Secure Status in Message Header check box on the System Settings > Advanced Settings > Conversation Configuration page. When the check box is checked, Unity Connection plays a prompt to the user before playing the secure message, announcing that it is a "...secure message...."
- When callers are routed to a user or call handler greeting and then leave a message, the Mark Secure check box on the Edit > Message Settings page for a user or call handler account determines whether Unity Connection marks the message secure.
- By default, Unity Connection does not relay secure messages for users who have one or more message actions configured to relay messages to an SMTP relay address. If a secure message is received for a user who is configured for relay, Unity Connection sends a non-delivery receipt to the sender. To have Unity Connection relay secure messages, check the Allow Relaying of Secure Messages check box on the System Settings > Advanced > Messaging page in Cisco Unity Connection Administration. Note that when the check box is checked, secure messages are relayed with a secure flag; however, most email clients treat the messages as regular messages.
- Fax messages from the fax server are never marked secure.

ViewMail Limitations Regarding Secure Messages

- Secure messages cannot be forwarded using Cisco Unity Connection ViewMail for Microsoft Outlook 8.0 or ViewMail for IBM Lotus Notes.
- ViewMail for Outlook 8.0 and ViewMail for Notes support only playing secure messages.
- Messages that are composed or replied to using ViewMail for Outlook 8.0 or ViewMail for Notes are not sent as secure, even when users are assigned to a class of service for which the Require Secure Messaging field is set to Always or to Ask.

Configuring Unity Connection to Mark All Messages Secure

Use the following Task List to configure Unity Connection to mark all messages secure:

1. Configure all classes of service to always mark messages secure. See the Enabling Message Security for Class of Service (COS) Members. (When users sign in to Unity Connection and send a message, class of service settings determine whether the message is marked secure.)
2. Configure user mailboxes to mark all outside caller messages secure. See the Configuring Users and User Templates to Mark Messages Left by Outside Callers Secure.
3. Configure call handlers to mark all outside caller messages secure. See the Configuring Users and User Templates to Mark Messages Left by Outside Callers Secure.
4. If you do not want Unity Connection to announce to users that a message is marked secure, uncheck the Announce Secure Status in Message Header check box on the System Settings > Advanced Settings > Conversation Configuration page.

Enabling Message Security for Class of Service (COS) Members

Step 1 In Cisco Unity Connection Administration, find the COS that you want to change, or create a new one.

Step 2 On the Edit Class of Service page, under Message Options, in **Require Secure Messaging** list, select Always.

Step 3 Select **Save**.

Step 4 Repeat Step 1 to Step 3 for each class of service. Alternatively, you can edit multiple classes of services at once using the Bulk Edit option.

Configuring Users and User Templates to Mark Messages Left by Outside Callers Secure

Step 1 In Cisco Unity Connection Administration, find the user account or template that you want to edit.

If you want to edit multiple users at the same time, on the Search Users page, check the applicable user check boxes, and select **Bulk Edit**

Step 2 On the Edit menu, select **Message Settings**.

Step 3 On the Edit Message Settings page, under Message Security, select the Mark Secure option.

If you are in Bulk Edit mode, you must first check the check box to the left of the Mark Secure field to indicate that you want to make a change to the field for the selected users or templates.

Step 4 Select Save.

Configuring Call Handlers and Call Handler Templates to Mark Messages Left by Outside Callers Secure

Step 1 In Cisco Unity Connection Administration, find the call handler or call handler template that you want to edit.

If you want to edit multiple call handlers at the same time, on the Search Call Handlers page, check the applicable call handler check boxes, and select **Bulk Edit**.

Step 2 On the Edit menu, select **Message Settings**.

Step 3 On the Edit Message Settings page, under Message Security check the Mark Secure check box.

If you are in Bulk Edit mode, you must first check the check box to the left of the Mark Secure field to indicate that you want to make a change to the field for the selected users.

Step 4 Select Save.

Shredding Message Files for Secure Delete

Some organizations require additional security in the deletion of messages, beyond having users simply delete them. The Message File Shredding Level setting on the Advanced Settings > Messaging Configuration page in Cisco Unity Connection Administration is a systemwide setting that ensures that the copy of the message being deleted by the user is securely deleted, by causing the message to be shredded the specified number of times when it is deleted. To enable the feature, you enter a setting other than 0 (zero). The setting that you enter in the field (a number from 1 through 10) indicates the number of times that the deleted message files are shredded. The shredding is done by way of a standard Linux shred tool: the actual bits that make up the message are overwritten with random bits of data the specified number of times.

By default, the shredding process occurs every 30 minutes when the Clean Deleted Messages sysagent task runs. Clean Deleted Messages is a read-only task; the configuration settings for the task cannot be changed. (Information about the task can be found in Cisco Unity Connection Administration under Tools > Task Management).

There are some circumstances in which copies of messages or files that are associated with messages are not shredded:

- During the normal process of sending messages, temporary audio files are created. These temporary audio files are deleted when the message has been sent, but are not shredded. Any reference to the message is removed, but the actual data stays on the hard drive until the operating system has a reason to reuse the space and overwrites the data. In addition to these temporary audio files, there are other temporary files that are used during the delivery of a message that are deleted and shredded, if you have enabled shredding. Note that temporary files that are shredded are shredded immediately when the message they are associated with is deleted; unlike the message itself, the temporary files do not wait for the Clean Deleted Messages sysagent task to run.
- When a user attempts to play a message in the Web Inbox that is in a format that cannot be played, the message is transcoded into a temporary audio file. This temporary audio file is deleted when the user deletes the message, but it is not shredded.
- Shredding can occur only on messages that reside on the Unity Connection server. To ensure that messages are not recoverable from other servers, you should not use the following features: message relay, IMAP, ViewMail for Outlook, ViewMail for Notes, Web Inbox, single inbox, the SameTime Lotus plug-in, Cisco Unified Personal Communicator, Cisco Mobile, or SMTP Smart hosts in between networked servers. If you want to use these features, you should also use the secure messaging feature. When you use secure messaging, there are no local copies of the secure messages, and users are not allowed to save local copies; therefore, all copies of messages remain on the Unity Connection server, and can thus be shredded when deleted.

Note For additional information about secure messaging, see the Handling Messages Marked Private or Secure.

- Messages that are sent between locations in a Unity Connection network are written to a temporary location before they are sent. The temporary copies of the messages are deleted, but not shredded.

If you have enabled shredding in a Unity Connection cluster, messages are shredded on both the primary and secondary server when they are deleted.

We strongly recommend that you set the shredding level no higher than 3, due to performance issues.

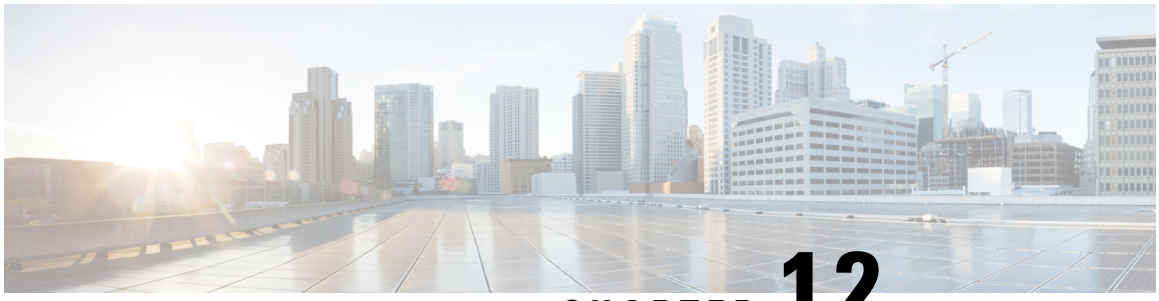
Note that messages are shredded only when they have been hard deleted.

Message Security Options for IMAP Client Access

When users access voice messages that are marked with normal or private sensitivity from an IMAP client, the IMAP client may allow users to save messages as WAV files to their hard disks, and may allow users to forward the messages. To prevent users from saving and/or forwarding voice messages from their IMAP client, consider specifying one of the following class of service options:

- Users can access only message headers in an IMAP client—regardless of message sensitivity.

- Users can access message bodies for all messages except those that are marked private. (Secure messages cannot be accessed in an IMAP client, unless the client is Microsoft Outlook and ViewMail for Outlook is installed or the client is Lotus Notes and ViewMail for Notes is installed).



CHAPTER 12

Next Generation Security

Overview

Cisco Unity Connection supports Next Generation Security that provides confidentiality, integrity, and authentication through Suite B cryptographic algorithm. Suite B algorithm includes various components, such as AES encryption and ECDSA ciphers to meet security and scalability requirements of an organization.

Next Generation Security	Supported Version
Authentication Signature Algorithm	RSA (1024/2048/3092/4096) ECDSA (256/384/512)
Message Integrity	SHA-256 SHA-384 SHA-512
Encryption	AES-GCM (128/256) mode
Key Agreement	ECDH (256/384)

Note

- Unity Connection supports TLS 1.2 for Next Generation Security.
- Next Generation Security does not support RSA 1024 key when FIPS is enabled.

Unity Connection supports Next Generation Security over the following interfaces:

- HTTPS
- SIP
- SRTP

Note In addition to the above interfaces, Unity Connection supports Next Generation Security over SMTP interface as well with default cipher settings.

Next Generation Security Over HTTPS Interface

Next Generation Security over HTTPS Interface restricts web applications deployed over tomcat or jetty to use Suite B ciphers for inbound connections with Unity Connection. User must enable SSL to activate Next generation Security over Jetty or Web interface. For more information on enabling SSL over Connection Jetty, see the applicable *Command Line Interface Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Configuring Next Generation Security Over HTTPS Interface

To configure Next Generation Security over HTTPS interface:

Step 1 Sign in to Cisco Unity Connection Administration page, expand **System Settings** > **General Configurations** and select **HTTPS Ciphers**.

Step 2 Select any one of the following:

- **All Supported EC and RSA Ciphers**: When this option is selected, Unity Connection server negotiates with both EC based and RSA based ciphers.
- **RSA Ciphers Only**: When this option is selected, Unity Connection server negotiates with RSA based ciphers only.

Below table lists the HTTPS Cipher options in priority order of RSA or ECDSA ciphers:

Table 7: HTTPS Cipher options with Priority order

HTTPS Cipher Options	HTTPS Ciphers in Priority Order
All Supported EC and RSA Ciphers	• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA • SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

HTTPS Cipher Options	HTTPS Ciphers in Priority Order
RSA Ciphers Only	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA • SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

Step 3 Select **Save** to apply the changes.

Note After modifying the HTTPS cipher, make sure to restart tomcat service for the changes to take effect. In addition, you must also disable and enable jetty over SSL using the utils cuc jetty ssl {disable/enable} command, if jetty SSL is enabled.

Next Generation Security Over SIP Interface

Next Generation Security over SIP interface restricts SIP interface to use Suite B ciphers based on TLS 1.2, SHA-2 and AES256 protocols. It allows the various combinations of ciphers based on the priority order of RSA or ECDSA ciphers.

To specify the ciphers that should be used to enable Next Generation Security over SIP interface, navigate to **System Settings** > **General Configuration** and select the cipher from the **TLS Ciphers** drop-down list.

Note Next Generation Security over SIP interface uses only Encryption security mode.

For more information on configuring ciphers and third party certificates over SIP interface, see "Enabling Next Generation Security over SIP Integration" section of "Setting Up a Cisco Unified Communications Manager SIP Trunk Integration" chapter of *Cisco Unified Communications Manager Cisco Unified Communication Manager SIP Integration Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/integration/cucm_sip/b_14cucintcucmsip.html.

Next Generation Security Over SRTP Interface

Next Generation Security over SRTP interface restricts SRTP interface to use Suite B ciphers based on SHA-2 and AES256 protocols.

To specify the ciphers that should be used to enable Next Generation Security over SRTP interface, navigate to **System Settings** > **General Configuration** and select the cipher from the **SRTP Ciphers** drop-down list.

For more information on configuring ciphers and third party certificates over SRTP interface, see "Enabling Next Generation Security over SIP Integration" section of "Setting Up a Cisco Unified Communications Manager SIP Trunk Integration" chapter of *Cisco Unified Communications Manager Cisco Unified*

Communication Manager SIP Integration Guide for Cisco Unity Connection Release 14 available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/integration/cucm_sip/b_14cucintcucmsip.html.