# Security Guide for Cisco Unity Connection

Release 8.x
Revised August 2013

**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

Text Part Number:

*Security Guide for Cisco Unity Connection Release 8.x*

# CONTENTS

# Preface

## Audience and Use

The *Security Guide for Cisco Unity Connection* provides information related to aspects of the security of your Cisco Unity Connection system. Within each chapter, you will find descriptions of potential security issues; information on any actions you need to take; recommendations that will help you make decisions; discussion of the ramifications of the decisions you make; and in many cases, best practices.

## Documentation Conventions

***Table 1 Conventions in the Security Guide for Cisco Unity Connection***

| Convention | Description |
|---|---|
| boldfaced text | Boldfaced text is used for:<br>• Key and button names. (Example: Select **OK**.)<br>• Information that you enter. (Example: Enter **Administrator** in the User Name box.) |
| < ><br>(angle brackets) | Angle brackets are used around parameters for which you supply a value. (Example: In your browser, go to **https://<Cisco Unity Connection server IP address>/cuadmin**.) |
| -<br>(hyphen) | Hyphens separate keys that must be pressed simultaneously. (Example: Press **Ctrl-Alt-Delete**.) |
| ><br>(right angle bracket) | A right angle bracket is used to separate selections that you make in the navigation bar of Cisco Unity Connection Administration. (Example: In Cisco Unity Connection Administration, expand **Contacts > System Contacts**.) |

The *Security Guide for Cisco Unity Connection* also uses the following conventions:

**Note** Means reader take note. Notes contain helpful suggestions or references to material not covered in the document.

**Caution** Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

# Cisco Unity Connection Documentation

For descriptions and URLs of Cisco Unity Connection documentation on Cisco.com, see the *Documentation Guide for Cisco Unity Connection Release 8.x*. The document is shipped with Connection, and is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/roadmap/8xcucdg.html.

## Documentation References to Cisco Unified Communications Manager Business Edition

The name of the product known as Cisco Unified Communications Manager Business Edition in versions 8.0 and earlier has been changed to Cisco Unified Communications Manager Business Edition 5000 in versions 8.5 and later.

In the Cisco Unity Connection 8.x documentation set, references to "Cisco Unified Communications Manager Business Edition" and "Cisco Unified CMBE" apply to both Business Edition version 8.0 and to Business Edition 5000 versions 8.5 and later. The references do not apply to Business Edition 6000.

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

# Cisco Product Security Overview

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. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations can be found at http://www.access.gpo.gov/bis/ear/ear_data.html.

CHAPTER 1

# IP Communications Required by Cisco Unity Connection 8.x

See the following sections:



## Cisco Unity Connection 8.x Service Ports

Table 1-1 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 Connection.

*Table 1-1 TCP and UDP Ports That Are Used for Inbound Connections to the Cisco Unity Connection Server*

| Ports and Protocols[1] | Operating System Firewall Setting | Executable/Service or Application | Service Account | Comments |
|---|---|---|---|---|
| TCP: 20500, 20501, 20502, 19003 | Open only between servers in a Connection cluster | CuCsMgr/Connection Conversation Manager | cucsmgr | Servers in a Connection cluster must be able to connect to each other on these ports. |
| TCP: **21000–21512** | Open | CuCsMgr/Connection Conversation Manager | cucsmgr | IP phones must be able to connect to this range of ports on the Connection server for some phone client applications. |
| TCP: **5000** | Open | CuCsMgr/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).<br>Administration workstations connect to this port. |

*Table 1-1 TCP and UDP Ports That Are Used for Inbound Connections to the Cisco Unity Connection Server (continued)*

| Ports and Protocols[1] | Operating System Firewall Setting | Executable/Service or Application | Service Account | Comments |
|---|---|---|---|---|
| TCP and UDP ports allocated by administrator for SIP traffic<br>Possible ports are **5060–5100** | Open | CuCsMgr/Connection Conversation Manager | cucsmgr | Connection SIP Control Traffic handled by conversation manager.<br>SIP devices must be able to connect to these ports. |
| TCP: 20055 | Open only between servers in a Connection cluster | CuLicSvr/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 Connection cluster | unityoninit/Connection DB | root | Servers in a Connection cluster must be able to connect to each other on these database ports.<br>For external access to the database, use CuDBProxy. |
| TCP: **143, 993, 7993, 8143, 8993** | Open | CuImapSvr/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. |
| TCP: **25, 8025** | Open | CuSmtpSvr/Connection SMTP Server | cusmtpsvr | Servers delivering SMTP to 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/Connection Voice Recognizer | openspeech | Restricted to localhost only (no remote connections to this service are needed). |
| UDP: **16384–21511** | Open | CuMixer/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/<br>Speech recognition RTP | cumixer | Restricted to localhost only (no remote connections to this service are needed). |
| TCP: 22000<br>UDP: 22000 | Open only between servers in a Connection cluster | CuSrm/<br>Connection Server Role Manager | cusrm | Cluster SRM RPC.<br>Servers in a Connection cluster must be able to connect to each other on these ports. |

*Table 1-1 TCP and UDP Ports That Are Used for Inbound Connections to the Cisco Unity Connection Server (continued)*

| Ports and Protocols[1] | Operating System Firewall Setting | Executable/Service or Application | Service Account | Comments |
|---|---|---|---|---|
| TCP: 22001<br>UDP: 22001 | Open only between servers in a Connection cluster | CuSrm/ Connection Server Role Manager | cusrm | Cluster SRM heartbeat.<br>Heartbeat event traffic is not encrypted but is MAC secured.<br>Servers in a Connection cluster must be able to connect to each other on these ports. |
| TCP: **20532** | Open | CuDbProxy/ 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.<br>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 Connection cluster.<br>Administrative workstations must be able to connect to a Connection server on this port.<br>Servers in a Connection cluster must be able to connect to each other on this port. |
| UDP: **161** | Open | Snmpd Platform SNMP Service | root | — |
| UDP: **500** | Open | Raccoon ipsec isakmp (key management) service | root | Using ipsec is optional, and off by default.<br>If the service is enabled, servers in a Connection cluster must be able to connect to each other on this port. |
| TCP: **8500**<br>UDP: **8500** | Open | clm/cluster management service | root | The cluster manager service is part of the Voice Operating System.<br>Servers in a Connection cluster must be able to connect to each other on these ports. |

*Table 1-1 TCP and UDP Ports That Are Used for Inbound Connections to the Cisco Unity Connection Server (continued)*

| Ports and Protocols[1] | Operating System Firewall Setting | Executable/Service or Application | Service Account | Comments |
|---|---|---|---|---|
| UDP: **123** | Open | Ntpd Network Time Service | ntp | Network time service is enabled to keep time synchronized between servers in a Connection cluster.<br>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.<br>Servers in a Connection cluster must be able to connect to each other on this port. |
| TCP: 5007 | Open | Tomcat/Cisco Tomcat (SOAP Service) | tomcat | Servers in a Connection cluster must be able to connect to each other on these ports. |
| TCP: 1500, 1501 | Open only between servers in a Connection cluster | cmoninit/Cisco DB | informix | These database instances contain information for LDAP integrated users, and serviceability data.<br>Servers in a Connection cluster must be able to connect to each other on these ports. |
| TCP: 1515 | Open only between servers in a Connection cluster | dblrpm/Cisco DB Replication Service | root | Servers in a Connection cluster must be able to connect to each other on these ports. |
| TCP: 8001 | Open only between servers in a Connection cluster | dbmon/Cisco DB Change Notification Port | database | Servers in a Connection cluster must be able to connect to each other on these ports. |
| TCP: 2555, 2556 | Open only between servers in a Connection cluster | RisDC/Cisco RIS Data Collector | ccmservice | Servers in a Connection cluster must be able to connect to each other on these ports. |
| TCP: 1090, 1099 | Open only between servers in a Connection cluster | Amc/Cisco AMC Service (Alert Manager Collector) | ccmservice | Performs back-end serviceability data exchanges<br>1090: AMC RMI Object Port<br>1099: AMC RMI Registry Port<br>Servers in a Connection cluster must be able to connect to each other on these ports. |

*Table 1-1 TCP and UDP Ports That Are Used for Inbound Connections to the Cisco Unity Connection Server (continued)*

| 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.<br>Servers in a Connection cluster must be able to connect to each other on these ports for communications that use HTTP-based interactions like REST. |
| TCP: 5001, 8005 | Blocked; internal use only | tomcat/Cisco Tomcat | tomcat | Internal tomcat service control and axis ports. |
| TCP: **32768–61000**<br>UDP: **32768–61000** | Open | — | — | Ephemeral port ranges, used by anything with a dynamically allocated client port. |
| TCP: 7080 | Open | jetty/Connection Jetty | jetty | *Exchange 2007 and Exchange 2010 only, single inbox only:* EWS notifications of changes to Connection voice messages. |
| UDP: 9291 | Open | CuMbxSync/ Connection Mailbox Sync Service | cumbxsync | *Exchange 2003 only, single inbox only:* WebDAV notifications of changes to Connection voice messages. |

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

# Outbound Connections Made by the Cisco Unity Connection 8.x Server

**Revised December 11, 2010**

Table 1-2 lists the TCP and UDP ports that Cisco Unity Connection uses to connect with other servers in the network.

*Table 1-2 TCP and UDP Ports That Cisco Unity Connection Uses to Connect With Other Servers in the Network*

| Ports and Protocols | Executable | Service Account | Comments |
|---|---|---|---|
| TCP: 2000* (Default SCCP port)<br>Optionally TCP port 2443* if you use SCCP over TLS.<br>* Many devices and applications allow configurable RTP port allocations. | CuCsMgr | cucsmgr | Connection SCCP client connection to Cisco Unified CM when they are integrated by using SCCP. |
| UDP: 16384–32767* (RTP)<br>* Many devices and applications allow configurable RTP port allocations. | CuMixer | cumixer | Connection outbound audio-stream traffic. |

*Table 1-2 TCP and UDP Ports That Cisco Unity Connection Uses to Connect With Other Servers in the Network (continued)*

| Ports and Protocols | Executable | Service Account | Comments |
|---|---|---|---|
| UDP: 69 | CuCsMgr | cucsmgr | When you are configuring encrypted SCCP, encrypted SIP, or encrypted media streams, Connection makes a TFTP client connection to Cisco Unified CM to download security certificates. |
| TCP: 53<br>UDP: 53 | any | any | Used by any process that needs to perform DNS name resolution. |
| TCP: 53, and either 389 or 636 | CuMbxSync<br>CuCsMgr<br>tomcat | cumbxsync<br>cucsmgr<br>tomcat | Used when Connection is configured for unified messaging with Exchange and one or more unified messaging services are configured to search for Exchange servers.<br>Connection uses port 389 when you choose LDAP for the protocol used to communicate with domain controllers.<br>Connection uses port 636 when you choose LDAPS for the protocol used to communicate with domain controllers. |
| TCP: 80, 443 (HTTP and HTTPS) | CuMbxSync<br>CuCsMgr<br>tomcat | cumbxsync<br>cucsmgr<br>tomcat | Connection makes HTTP and HTTPS client connections to other servers for communications for external services (in Connection 8.0) or unified messaging (in 8.5 and later), such as connections to Microsoft Exchange for single inbox and calendar integrations. |
| TCP: 80, 443, 8080, and 8443 (HTTP and HTTPS) | CuCsMgr<br>tomcat | cucsmgr<br>tomcat | Connection makes HTTP and HTTPS client connections to:<br>• Other Connection servers for Digital Networking automatic joins.<br>• Cisco Unified CM for AXL user synchronization. |
| TCP: 143, 993 (IMAP and IMAP over SSL) | CuCsMgr | cucsmgr | Connection makes IMAP connections to Microsoft Exchange servers to perform text-to-speech conversions of email messages in a Connection user's Exchange mailbox. |
| TCP: 25 (SMTP) | CuSmtpSvr | cusmtpsvr | Connection makes client connections to SMTP servers and smart hosts, or to other Connection servers for features such as VPIM networking or Connection Digital Networking. |
| TCP: 21 (FTP) | ftp | root | The installation framework performs FTP connections to download upgrade media when an FTP server is specified. |

*Table 1-2 TCP and UDP Ports That Cisco Unity Connection Uses to Connect With Other Servers in the Network (continued)*

| Ports and Protocols | Executable | Service Account | Comments |
|---|---|---|---|
| TCP: 22 (SSH/SFTP) | CiscoDRFMaster<br>sftp | drf<br>root | The Disaster Recovery Framework performs SFTP connections to network backup servers to perform backups and retrieve backups for restoration.<br>The installation framework will perform SFTP connections to download upgrade media when an SFTP server is specified. |
| UDP: 67 (DHCP/BootP) | dhclient | root | Client connections made for obtaining DHCP addressing.<br>Although DHCP is supported, Cisco highly recommends that you assign static IP addresses to Connection servers. |
| TCP: 123<br>UDP: 123 (NTP) | Ntpd | root | Client connections made for NTP clock synchronization. |

CHAPTER 2

# Preventing Toll Fraud in Cisco Unity Connection 8.x

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

See the following sections:



## Using Restriction Tables to Help Prevent Toll Fraud in Cisco Unity Connection 8.x

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 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 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 will be 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 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 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.

To learn more about how restriction tables work and how to set them up, see the Managing Restriction Tables in Cisco Unity Connection 8.x chapter of the *System Administration Guide for Cisco Unity Connection Release 8.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html.

# 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

# Securing the Connection Between Cisco Unity Connection 8.x, Cisco Unified Communications Manager, and IP Phones

In this chapter, you will 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 will help you make decisions; discussion of the ramifications of the decisions you make; and best practices.

See the following sections:



## Security Issues for Connections Between Cisco Unity Connection 8.x, Cisco Unified Communications Manager, and IP Phones

A potential point of vulnerability for a Cisco Unity Connection system is the connection between 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 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, Connection, and IP phones that are managed by Cisco Unified CM)
- Modification of call signaling between Connection and Cisco Unified CM

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

# Cisco Unified Communications Manager Security Features for Cisco Unity Connection 8.x Voice Messaging Ports

Cisco Unified CM can secure the connection with Connection against the threats listed in the "Security Issues for Connections Between Cisco Unity Connection 8.x, Cisco Unified Communications Manager, and IP Phones" section on page 3-11. The Cisco Unified CM security features that Connection can take advantage of are described in Table 3-1.

*Table 3-1 Cisco Unified CM Security Features That Are 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.<br>This feature protects against:<br>• Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and Connection.<br>• Modification of the call signalling.<br>• Identity theft of the Connection server.<br>• Identity theft of the Cisco Unified CM server. |
| 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 Connection voice messaging ports (for an SCCP integration) or 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.<br>This feature protects against:<br>• Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and Connection.<br>• Modification of the media stream.<br>• Identity theft of the Connection server.<br>• Identity theft of the Cisco Unified CM server. |

*Table 3-1 Cisco Unified CM Security Features That Are Used by Cisco Unity Connection (continued)*

| Security Feature | Description |
|---|---|
| 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 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.<br>This feature protects against:<br>• Man-in-the-middle attacks that observe the information flow between Cisco Unified CM and Connection.<br>• Network traffic sniffing that observes the signaling information flow between Cisco Unified CM and Connection. |
| 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 Connection and the endpoint (for example, a phone or gateway). Support includes audio streams only. Media encryption includes creating a media master key pair for the devices, delivering the keys to Connection and the endpoint, and securing the delivery of the keys while the keys are in transport. Connection and the endpoint use the keys to encrypt and decrypt the media stream.<br>This feature protects against:<br>• Man-in-the-middle attacks that listen to the media stream between Cisco Unified CM and Connection.<br>• Network traffic sniffing that eavesdrops on phone conversations that flow between Cisco Unified CM, 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 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 Connection private secure messaging feature. For details on the Connection secure messaging feature, see the "How Cisco Unity Connection 8.x Handles Messages That Are Marked Private or Secure" section on page 10-62.

# Security Mode Settings for Cisco Unified Communications Manager and Cisco Unity Connection 8.x

Cisco Unified Communications Manager and Cisco Unity Connection have the security mode options shown in Table 3-2 for voice messaging ports (for SCCP integrations) or port groups (for SIP integrations).

**Caution** The Cluster Security Mode setting for 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 will fail.

*Table 3-2 Security Mode Options*

| Setting | Effect |
|---|---|
| Non-secure | The integrity and privacy of call-signaling messages will not be ensured because call-signaling messages will be sent as clear (unencrypted) text and will be connected to Cisco Unified CM through a non-authenticated port rather than an authenticated TLS port.<br><br>In addition, the media stream cannot be encrypted. |
| Authenticated | The integrity of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages will not be ensured because they will be sent as clear (unencrypted) text.<br><br>In addition, the media stream will not be encrypted. |
| Encrypted | The integrity and privacy of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an authenticated TLS port, and the call-signaling messages will be encrypted.<br><br>In addition, the media stream can be encrypted.<br><br>**Caution** 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 will not be encrypted. Also, if an intervening device (such as a transcoder or gateway) is not enabled for encryption, the media stream will not be encrypted. |

# Best Practices for Securing the Connection Between Cisco Unity Connection 8.x, 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 Connection Release 8.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/integration/guide/cucm_sccp/cucintcucmskinny.html.

CHAPTER 4

# Securing Administration and Services Accounts in Cisco Unity Connection 8.x

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

See the following sections:



## Understanding Cisco Unity Connection 8.x Administration Accounts

**Revised September 27, 2012**

A Cisco Unity Connection server has two types of administration accounts. Table 4-1 summarizes the purposes for and the differences between the two types of accounts.

*Table 4-1 Administration Accounts on a Connection Server*

| | Operating System Administration Account | Application Administration Account |
|---|---|---|
| **The account is used to access** | • Cisco Unified Operating System Administration<br>• Disaster Recovery System<br>• Command line interface | • Cisco Unity Connection Administration<br>• Cisco Unified Serviceability<br>• Cisco Unity Connection Serviceability<br>• 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 |

*Table 4-1 Administration Accounts on a Connection Server (continued)*

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

# Best Practices for Accounts That Are Used to Access Cisco Unity Connection Administration in Connection 8.x

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 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 Cisco Unity Connection user account specifically for the purpose of administering Connection, you sign in to Cisco Unity Connection Administration by using the credentials that are associated with the default administrator account. The default administrator account is created during the installation of 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 will generate an error:
  - CCMSysUser
  - WDSysUser
  - CCMQRTSysUser
  - IPMASysUser
  - WDSecureSysUser
  - CCMQRTSecureSysUser
  - IPMASecureSysUser
  - TabSyncSysUser
  - CUCService

To learn more about creating administrative accounts, see the "Adding an Administrator Account (User Without a Voice Mailbox)" section in the "Adding Cisco Unity Connection 8.x Accounts Individually" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 8.x*. The guide is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx.html.

**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 will be assigned to the System Administrator role, which gives administrators full access to all 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.)

To learn more about the predefined roles Cisco Unity Connection offers and the level of privileges included with each role, see the "Roles in Cisco Unity Connection 8.x" section in the "Preparing to Add User Accounts in Cisco Unity Connection 8.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 8.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx.html.

**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 (Cisco Unity Connection 8.5 and Later Only)

**Added November 16, 2010**

When you configure unified messaging for Cisco Unity Connection 8.5 and later, you create one or more Active Directory accounts that 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 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 Connection cannot use it to access Exchange mailboxes.

CHAPTER 5

# FIPS Compliance in Cisco Unity Connection 8.6

Cisco Unity Connection 8.6 supports the FIPS mode that complies with the Federal Information Processing Standards 140-2 (FIPS) requirements.

FIPS mode is not supported in Cisco Unified Communications Manager Business Edition (CUCMBE). Though the **utils fips <option>** Command Line Interface (CLI) command is visible for administrator, but it is not functional.

Recommendations to enable FIPS mode for Connection are:

- If you are performing a fresh installation of Cisco Unity Connection 8.6 and planning to use the FIPS mode, you must enable FIPS before configuring the Connection server and adding a telephony integration.
- If you are performing an upgrade to Cisco Unity Connection 8.6, make sure to follow the steps for regenerating certificates before using any pre-existing telephony integrations. To learn how to regenerate certificates, see the Regenerating Certificates for FIPS section.

See the following sections:

# 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/en/US/products/ps6509/prod_maintenance_guides_list.html.

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

**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.

# Regenerating Certificates for FIPS

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.

Perform the following steps whenever you enable or disable the FIPS mode:

**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.

**Caution** 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 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 Connection Conversation Manager service in the Critical Services section.
    d. When the Status area displays a message that the 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* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/os_administration/guide/8xcucosag060.html#wp1053189.

# 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

See the following sections:

- Configure Networking When Using FIPS Mode, page 5-26
- Configure Unified Messaging When Using FIPS Mode, page 5-26
- Configure IPsec Policies When Using FIPS Mode, page 5-26

- Unsupported Features When Using FIPS Mode, page 5-26

## 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 or Cisco Unified MeetingPlace
- Set the Web-Based Authentication Mode setting to Basic on the Edit Unified Messaging Service page in Connection Administration

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

## Configure IPsec Policies When 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 http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/os_administration/guide/8xcucosagx.html.

For information on setting up IPsec policies for Microsoft Exchange servers, consult the relevant Microsoft IPsec documentation.

## 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)

# Configuring Voicemail PIN For Touchtone Conversation Users To Sign In

Enabling FIPS in Cisco Unity Connection 8.6 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 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 Connection, the PIN is hashed by using an SHA-1 algorithm, which is much harder to decrypt and is FIPS compliant.

In version 8.5 and earlier, when a user calls Connection and enters the ID and PIN, Connection checks the database to determine whether the user's PIN was hashed with MD5 or SHA-1 algorithm. Connection hashes the PIN that the user entered, and compares it with the hashed PIN in the Connection database. If the PINs match, the user is logged in.

The following sections explains how to configure voicemail PIN in Connection while FIPS is enabled:

- Hashing All Voicemail PIN with SHA-1 Algorithm in Cisco Unity Connection 8.6(1) And Later Versions, page 5-27
- Replacing MD5-hashed Voicemail PIN with SHA-1 Algorithm in Cisco Unity 5.x Or Earlier Versions, page 5-27

# Hashing All Voicemail PIN with SHA-1 Algorithm in Cisco Unity Connection 8.6(1) And Later Versions

In version 8.6 and later, 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. Connection hashes all the voicemail PINs with SHA-1 and compares it with the hashed PIN in the 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.

# Replacing MD5-hashed Voicemail PIN with SHA-1 Algorithm in Cisco Unity 5.x Or Earlier Versions

For Connection user accounts that were originally created in Cisco Unity 5.x or earlier, the voicemail PIN that might have been hashed with MD5 algorithm must be replaced with SHA-1 algorithm. Consider the following points while replacing the MD5-hashed passwords with SHA-1-hashed passwords:

- Use the latest version of the User Data Dump utility to determine how many users still have MD5-hashed PINs. For each user, the Pin_Hash_Type column contains either MD5 or SHA-1. To download the latest version of the utility and to view the Help, see the User Data Dump page on the Cisco Unity Tools website at http://ciscounitytools.com/Applications/CxN/UserDataDump/UserDataDump.html.

**Note** The earlier versions of the User Data Dump utility do not include the Pin_Hash_Type column.

- Check the User Must Change at Next Sign-In check box on the Password Settings page in Connection Administration before you enable FIPS. This encourages users to sign in to Connection and change their voicemail PINs.

- Run the Bulk Password Edit utility if you still have users who have not changed their voicemail PINs. The Bulk Password Edit utility lets you selectively change PINs to random values and exports data on the changes to a .csv file. The export file includes the name, alias, email address, and new PIN for each user who's PIN was changed. You can use the .csv file to send an email to each user with the new PIN. The utility is available on the Cisco Unity Tools website at http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html.

CHAPTER 6

# Passwords, PINs, and Authentication Rule Management in Cisco Unity Connection 8.x

In Cisco Unity Connection, authentication rules govern user passwords, PINs, and account lockouts for all user accounts. We recommend that you define 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 Connection applications by locking out users who enter invalid PINs or passwords too many times.

In this chapter, you will 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 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 will help you make decisions; discussion of the ramifications of the decisions you make; and in many cases, best practices.

For information that will guide you through the process of securing Connection passwords and defining authentication rules, see the following sections:

**Understanding Which PINs and Passwords Users Use**

About the PINs and Passwords That Users Use to Access Cisco Unity Connection 8.x Applications, page 6-30

**Understanding How PINS and Passwords Are Assigned and How to Initially Secure Them**

Ensuring That Users Are Initially Assigned Unique and Secure PINs and Passwords in Cisco Unity Connection 8.x, page 6-31

**How to Change User PINs and Passwords**

Changing Cisco Unity Connection 8.x Web Application Passwords, page 6-31

Changing Cisco Unity Connection 8.x Phone PINs, page 6-32

**How to Define Authentication Rules**

Defining Authentication Rules to Specify Password, PIN, and Lockout Policies in Cisco Unity Connection 8.x, page 6-33

# About the PINs and Passwords That Users Use to Access Cisco Unity Connection 8.x Applications

**Revised November 16, 2010**

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

Users use the web application password to sign in to the Cisco Personal Communications Assistant (Cisco PCA), which provides access to the Messaging Inbox (in Connection 8.0), Messaging Assistant, and Personal Call Transfer Rules web tools.

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

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

**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 Connection web applications.

# Ensuring That Users Are Initially Assigned Unique and Secure PINs and Passwords in Cisco Unity Connection 8.x

**Revised November 16, 2010**

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 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 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.

# Changing Cisco Unity Connection 8.x Web Application Passwords

**Revised November 16, 2010**

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 will be 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 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 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 information on using BAT, see the "Using the Cisco Unity Connection 8.x Bulk Administration Tool" appendix in the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 8.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx.html.

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. If users have trouble receiving voice messages in an IMAP client after having updated their Cisco PCA password in both applications, see the "Troubleshooting IMAP Client Sign-In Problems in Cisco Unity Connection 8.x" section in the "Configuring an Email Account to Access Cisco Unity Connection 8.x Voice Messages" chapter of the *User Workstation Setup Guide for Cisco Unity Connection Release 8.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/user_setup/guide/8xcucuwsx.html.

**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 Cisco Unity Connection 8.x Phone PINs

**Revised November 16, 2010**

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 Connection phone conversation or the 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. For information on using BAT, see the "Using the Cisco Unity Connection 8.x Bulk Administration Tool" appendix in the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 8.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx.html.

When PINs expire, users will be required to enter a new PIN when they next attempt to sign in to the 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 in Cisco Unity Connection 8.x

**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 Connection in those cases.

Use authentication rules to customize the sign-in, password, and lockout policies that Cisco Unity Connection applies when users access 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 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 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
- Reset Failed Sign-In Attempts Every __ Minutes
- Lockout Duration
- Credential Expires After __ Days
- Minimum Credential Length
- Stored Number of Previous Credentials
- Check For Trivial Passwords

### Failed Sign-In __ Attempts

Use this field to indicate how 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 Connection will 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 will be 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 will be 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 will be required to use the new length the next time that they change their PINs and passwords.

**Stored Number of Previous Credentials**

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

By default, 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).

CHAPTER 7

# Single Sign-On in Cisco Unity Connection 8.6 and Later

**Revised August 2, 2011**

Cisco Unity Connection 8.6 and later versions support the single sign-on feature that allows end users to log in once and gain access to use the following Cisco Unity Connection applications without signing on again:

- Cisco Personal Communications Assistant
- Web Inbox
- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability

For more information about the single sign-on feature, see the Cisco white paper, *A complete guide for the installation, configuration and integration of Open Access Manager 9.0 with CUCM 8.5, 8.6 /CUC 8.6 and Active Directory for SSO* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf.

See the following sections:


- Configuration Checklist for Single Sign-On, page 7-37
- System Requirements for Single Sign-On, page 7-38
- Configuring Single Sign-On, page 7-39


## Configuration Checklist for Single Sign-On

This section provides a checklist for configuring the single sign-on feature in the network.

*Table 7-1 Single Sign-On Configuration Checklist*

| Configuration Steps | | Related Topics and Documentation |
|---|---|---|
| **Step 1** | Ensure that your environment meets the requirements described in the System Requirements for Single Sign-On, page 7-38 | — |
| **Step 2** | Provision the OpenAM server in Active Directory, and then generate keytab files.<br>**Note** If your Windows version does not include the ktpass tool for generating keytab files, then you must obtain it separately. | Microsoft Active Directory documentation |
| **Step 3** | Configure the OpenAM server for Cisco Unity Connection. | Configuring OpenAM Server, page 7-39 |
| **Step 4** | Import the OpenAM server certificate into the Cisco Unified Communications Manager tomcat-trust store. | http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf |
| **Step 5** | Configure Windows single sign-on with Active Directory and OpenAM. | http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf |
| **Step 6** | Configure client browsers for single sign-on. | http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf |
| **Step 7** | Enable single sign-on in Cisco Unified Communications Manager. | Running CLI Commands for Single Sign-On, page 7-40 |

# System Requirements for Single Sign-On

The following single sign-on system requirements exist for Cisco Unity Connection:

- Cisco Unity Connection release 8.6(1) or higher on each server in a cluster.

The feature requires the following third-party applications for configuring the single sign-on feature:

- Microsoft Windows Server 2003 with SP1/SP2 or Microsoft Windows Server 2008 with SP2 for deploying Active Directory
- Microsoft Active Directory server (any version)
- ForgeRock Open Access Manager (OpenAM) version 9.0
- Apache Tomcat 7.0.0

The single sign-on feature uses Active Directory and OpenAM simultaneously to provide single sign-on access to client applications.

The third-party applications required for the single sign-on feature must meet the following configuration requirements:

- Active Directory must be deployed in a Windows domain-based network configuration, not just as an LDAP server.
- The OpenAM server must be accessible by name on the network to Connection server, all client systems, and the Active Directory server.
- The OpenAM server can be installed on Microsoft Windows 2003 server or RedHat Enterprise Linux (RHEL) server.

- The Active Directory (Domain Controller) server, Windows clients, Cisco Unity Connection, and OpenAM must be in the same domain.
- DNS must be enabled in the domain.
- The clocks of all the entities participating in single sign-on must be synchronized.

See the third-party product documentation for more information about those products.

# Configuring Single Sign-On

The complete set of instructions to configure Connection and OpenAM server for single sign-on are given in the Cisco white paper, *A complete guide for the installation, configuration and integration of Open Access Manager 9.0 with CUCM 8.5, 8.6 /CUC 8.6 and Active Directory for SSO* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf. This section outlines the key steps and/or instructions that must be followed for Connection-specific configuration. However, if you are configuring single sign-on for the first time, it is strongly recommended to follow the detailed instructions given in the Cisco white paper.

- Configuring OpenAM Server, page 7-39
- Running CLI Commands for Single Sign-On, page 7-40

## Configuring OpenAM Server

To configure OpenAM server, you must perform the following steps:

Step 1: Configure Policies on OpenAM Server

To configure policies on OpenAM server, you must log in to OpenAM and select the Access Control tab. Click the Top Level Realm option, select the Policies tab, and then create a new policy. Follow the steps as given in the Cisco white paper, http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf, for creating a new policy. While following the instructions given in the white paper, make sure to create policies with the below mentioned Connection-specific information:

- Ensure the following points while adding rules to the policy:
  - Each rule should be of the URL Policy Agent service type
  - Make sure to check the GET and POST checkbox for each rule
  - Create a rule for each of the following resources, where 'fqdn' is the fully qualified domain name of your Connection server:

    https://<fqdn>:8443/*

    https://<fqdn>:8443/*?*

    https://<fqdn>/*

    https://<fqdn>/*?*

    http://<fqdn>/*

    http://<fqdn>/*?*
- Ensure the following points while adding a subject to the policy:
  - Make sure that the Subject Type field is Authenticated Users.
  - Specify a subject name

  - Do not check the Exclusive check box.
- Ensure the following points while adding a condition to the policy:
  - Mention the Condition type as Active Session Time
  - Specify a condition name
  - Configure active session timeout as 120 minutes and select 'No' for the Terminate Session option.

Step 2: Configure a Windows Desktop SSO login module instance

Follow the instructions for configuring Windows Desktop as given in the Cisco white paper, https://supportforums.cisco.com/docs/DOC-14462.

Step 3: Configure a J2EE Agent Profile for Policy Agent 3.0

Follow the instructions to create a new J2EE agent as given in the Cisco white paper, https://supportforums.cisco.com/docs/DOC-14462 with the below mentioned Connection-specific settings:

- The name mentioned as agent profile name is the name that you need to enter when enabling SSO on the Connection server, when it prompts as "Enter the name of the profile configured for this policy agent".
- The agent password entered here is the password that is entered on the Connection server when it prompts as "Enter the password of the profile name".
- Make sure to add the following URIs to the Login Form URI section on the Application tab:
  - /cuadmin/WEB-INF/pages/logon.jsp
  - /cuservice/WEB-INF/pages/logon.jsp
  - /ciscopca/WEB-INF/pages/logon.jsp
  - /inbox/WEB-INF/pages/logon.jsp
  - /ccmservice/WEB-INF/pages/logon.jsp
- Under the Application tab, add the following URI in the Not Enforced URI Processing session:
  - /inbox/gadgets/msg/msg-gadget.xml

In addition to above Connection-specific configuration, ensure the following points:

- Import users from LDAP to Connection. Users must be configured with the appropriate roles to log in to Cisco Unity Connection Administration, or Cisco Unity Connection Serviceability.
- Upload the OpenAM certificate into Connection as described in the Configuring SSO on Cisco Unified Communications Manager 8.6 section of the Cisco white paper, http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf.

# Running CLI Commands for Single Sign-On

The following sections describe the CLI commands that configure single sign-on:

- utils sso enable
- utils sso disable
- utils sso status

For more information, see the Cisco white paper, .

- **utils sso enable**

The utils sso command enables and configures SSO-based authentication. Make sure to run the command on every node in the cluster.

**Caution** When you enable or disable single sign-on the Cisco Unity Connection, web server (Tomcat) restarts.

**Command syntax**

**utils sso enable**

**Parameters**

enable -Enables SSO-based authentication. This command starts the single sign-on configuration wizard.

- **utils sso disable**

This command disables SSO-based authentication. This command lists the web applications for which SSO is enabled. Enter Yes when prompted to disable single sign-on for the specified application. You must run this command on all nodes in a cluster.

**Command syntax**

**utils sso disable**

- **utils sso status**

This command displays the status and configuration parameters of single sign-on.

**Command Syntax**

**utils sso status**

CHAPTER 8

# The Cisco Unity Connection 8.x Security Password

**Added November 16, 2010**

## About the Cisco Unity Connection 8.x Security Password

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

- When a 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 will not be able to 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 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 8.x* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

CHAPTER 9

# Using SSL to Secure Client/Server Connections in Cisco Unity Connection 8.x

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 Connection. Note that IMAP client access to Connection voice messages is a licensed feature.

See the following sections:

# Deciding Whether to Install an SSL Certificate to Secure Cisco PCA and IMAP Email Client Access to Cisco Unity Connection 8.x

When you install Cisco Unity Connection, a local certificate is automatically created and installed to secure communication between the Cisco PCA and Connection, and between IMAP email clients and Connection. This means that all network traffic (including usernames, passwords, other text data, and voice messages) between the Cisco PCA and Connection is automatically encrypted, and network traffic between IMAP email clients and Connection is automatically encrypted if you enable encryption in the IMAP clients. 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 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 the "Setting Up Access to the Cisco Personal Communications Assistant" chapter of the *User Workstation Setup Guide for Cisco Unity Connection Release 8.x*. For information on configuring supported IMAP email clients, see the "Configuring an Email Account to Access Cisco Unity Connection Voice Messages" chapter of the same guide. The guide is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/user_setup/guide/8xcucuwsx.html.)

# Securing Connection Administration, Cisco PCA, and IMAP Email Client Access to Cisco Unity Connection 8.x

**Revised August 8, 2013**

Do the following tasks to create and install an SSL server certificate to secure Cisco Unity Connection Administration, Cisco Personal Communications Assistant, and IMAP email client access to Cisco 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 Windows Server 2003, see the "Installing Microsoft Certificate Services (Windows Server 2003 Only)" section on page 9-58. 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 Connection cluster is configured, run the `set web-security` CLI command on both Connection servers in the cluster and assign both servers the same alternate name. The alternate name will 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 http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

3. If a Connection cluster is configured, configure a DNS A record that contains the alternate name that you assigned in Task 2. List the publisher server first. This allows all IMAP email applications and the Cisco Personal Communications Assistant to access Connection voice messages by using the same Connection server name.
4. 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. Do the "To Create and Download a Certificate Signing Request" procedure on page 9-48.

   If a Connection cluster is configured, do this task for both servers in the Connection cluster.
5. If you are using Microsoft Certificate Services to export the root certificate and to issue the server certificate, do the procedure in the "Exporting the Root Certificate and Issuing the Server Certificate (Microsoft Certificate Services Only)" section on page 9-59.

   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 6.

   Only PEM-formatted (also known as Base-64 encoded DER) certificates can be uploaded to 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 by using freely available utilities like OpenSSL.

   If a Connection cluster is configured, do this task for both servers in the Connection cluster.
6. Upload the root certificate and the server certificate to the Connection server. Do the "To Upload the Root and Server Certificates to the Cisco Unity Connection Server" procedure on page 9-49.

   If a Connection cluster is configured, do this task for both servers in the Connection cluster.
7. Restart the Connection IMAP Server service so that Connection and the IMAP email clients use the new SSL certificates. Do the "To Restart the Connection IMAP Server Service" procedure on page 9-50.

   If a Connection cluster is configured, do this task for both servers in the Connection cluster.
8. To prevent users from seeing a security alert whenever they access Connection by using the Connection Administration, Cisco PCA, or an IMAP email client, do the following tasks on all computers from which users will access Connection:
   - Import the server certificate that you uploaded to the Connection server in Task 6. 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 Connection server in Task 6. 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.

### To Create and Download a Certificate Signing Request

**Step 1** On the Cisco Unity Connection server, sign in to Cisco Unified Operating System Administration.

**Step 2** On the Security menu, select **Certificate Management**.

**Step 3** On the Certificate List page, select **Generate CSR**.

**Step 4** On the Generate Certificate Signing Request page, in the **Certificate Name** list, select **tomcat**.

**Step 5** Select **Generate CSR**.

**Step 6** When the Status area displays a message that the CSR was successfully generated, select **Close**.

**Step 7** On the Certificate List page, select **Download CSR**.

**Step 8** On the Download Certificate Signing Request page, in the **Certificate Name** list, select **tomcat**.

**Step 9** Select **Download CSR**.

**Step 10** In the File Download dialog box, select **Save**.

**Step 11** In the Save As dialog box, in the **Save As Type** list, select **All Files**.

**Step 12** Save the file **tomcat.csr** to a location on the server on which you installed Microsoft Certificate Services or on a server that you can use to send the CSR to an external certification authority.

**Step 13** On the Download Certificate Signing Request page, select **Close**.

### To Upload the Root and Server Certificates to the Cisco Unity Connection Server

**Step 1** On the Cisco Unity Connection server on which you created the certificate signing request, sign in to Cisco Unified Operating System Administration.

**Step 2** On the Security menu, select **Certificate Management**.

**Note** If you select **Find** and display a list of the certificates currently installed on the server, you will see an existing, automatically generated, self-signed certificate for Tomcat. That certificate is unrelated to the Tomcat certificates that you upload in this procedure.

**Step 3** Upload the root certificate:

**a.** On the Certificate List page, select **Upload Certificate**.

**b.** On the Upload Certificate page, in the Certificate Name list, select **tomcat-trust**.

**c.** Select **Browse**, and browse to the location of the root CA certificate.

If you used Microsoft Certificate Services to issue the certificate, this is the location of the root certificate that you exported in the "To Export the Root Certificate and to Issue the Server Certificate" procedure on page 9-59.

If you used an external certification authority to issue the certificate, this is the location of the root CA certificate that you received from the external certification authority.

**d.** Select the name of the file.

**e.** Select **Open**.

**f.** On the Upload Certificate page, select **Upload File**.

**g.** When the Status area reports that the upload succeeded, select **Close**.

**Step 4** Upload the server certificate:

**a.** On the Certificate List page, select **Upload Certificate**.

**b.** On the Upload Certificate page, in the Certificate Name list, select **tomcat**.

**c.** Select **Browse**, and browse to the location of the server certificate.

If you used Microsoft Certificate Services to issue the certificate, this is the location of the server certificate that you issued in the "To Export the Root Certificate and to Issue the Server Certificate" procedure on page 9-59.

If you used an external certification authority to issue the certificate, this is the location of the server certificate that you received from the external certification authority.

**d.** Select the name of the file.

**e.** Select **Open**.

**f.** On the Upload Certificate page, select **Upload File**.

**g.** When the Status area reports that the upload succeeded, select **Close**.

**Step 5** Restart the Tomcat service (the service cannot be restarted from Cisco Unified Serviceability):

**a.** Sign in to the Connection server by using an SSH application.

**b.** Run the following CLI command to restart the Tomcat service:

```
utils service restart Cisco Tomcat
```

**To Restart 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.

# Securing Access to Exchange Calendars, Contacts, and Emails

**Revised November 16, 2010**

For information on securing access to Exchange calendars, contacts, and emails, see the applicable documentation:

- *(Cisco Unity Connection 8.5 and later)* The "Configuring Cisco Unity Connection 8.5 and Later and Microsoft Exchange for Unified Messaging" chapter of the *Unified Messaging Guide for Cisco Unity Connection Release 8.5 and Later*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/unified_messaging/guide/85xcucumgx.html.
- *(Cisco Unity Connection 8.0)* The "Configuring Text-to-Speech Access to Exchange Emails in Cisco Unity Connection 8.0" chapter and/or the "Creating Calendar and Contact Integrations in Cisco Unity Connection 8.0" chapter of the *System Administration Guide for Cisco Unity Connection Release 8.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html.

# Securing Access to Cisco Unified MeetingPlace

**Revised November 16, 2010**

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 http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_maintenance_guides_list.html.
2. Integrate Connection with MeetingPlace. When you configure Connection for the MeetingPlace calendar integration, specify SSL for the security transport.

   For more information, see the applicable documentation:

   - *(Connection 8.5 and later)* The "Configuring Cisco Unity Connection 8.5 and Later and Cisco Unified MeetingPlace for Unified Messaging" chapter of the *Unified Messaging Guide for Cisco Unity Connection Release 8.5 and Later*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/unified_messaging/guide/85xcucumgx.html.
   - *(Connection 8.0)* The "Creating a Calendar and Contact Integration with Cisco Unified MeetingPlace" section in the "Creating Calendar and Contact Integrations in Cisco Unity Connection 8.0" chapter of the *System Administration Guide for Cisco Unity Connection Release 8.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html.
3. On the 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:
   - 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 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 by using freely available utilities like OpenSSL.
   - The root certificate filename must not contain any spaces.

**To Upload the Root Certificate to the Connection Server**

**Step 1** Sign in to Cisco Unified Operating System Administration by using the administrator account and password.

The administrator account, which you created during Connection installation, is different from the accounts and passwords that you use to sign in to Connection Administration.

**Step 2** On the Security menu, select **Certificate Management**.

**Step 3** Select **Upload Certificate**.

**Step 4** In the Certificate Name list, select **Connection-trust**.

**Step 5** Select **Browse**, and find the file that contains the root certificate for the certification authority that issued the certificate for MeetingPlace.

**Step 6** Select **Upload File**.

# Securing Access to Cisco Unified MeetingPlace Express (Cisco Unity Connection 8.0 Only)

**Note** Integrations with Cisco Unified MeetingPlace Express are not supported in Cisco Unity Connection 8.5 and later.

To secure access to MeetingPlace Express, do the following tasks.

1. Configure SSL for MeetingPlace Express. For more information:
   a. Go to the "Cisco Unified MeetingPlace Express, Release 2.x" doc wiki at http://docwiki.cisco.com/wiki/Cisco_Unified_MeetingPlace_Express%2C_Release_2.x.
   b. Under "Configuration and Maintenance Tasks," select "Configuring SSL and Managing Certificates for Cisco Unified MeetingPlace Express."
2. Integrate Cisco Unity Connection with MeetingPlace Express. When you configure Connection for the MeetingPlace Express calendar integration, specify SSL for the security transport. For more information, see the "Creating a Calendar and Contact Integration with Cisco Unified MeetingPlace Express" section in the "Creating Calendar and Contact Integrations in Cisco Unity Connection 8.0" chapter of the *System Administration Guide for Cisco Unity Connection Release 8.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html.
3. On the Connection server, upload the root certificate of the certification authority from which you got the server certificate that you installed on the MeetingPlace Express server in Task 1. Note the following:
   – The root certificate is not the same thing as the certificate that was installed on the MeetingPlace Express 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 Express server.
   – Only PEM-formatted (also known as Base-64 encoded DER) certificates can be uploaded to 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 by using freely available utilities like OpenSSL.
   – The root certificate filename must not contain any spaces.

**To Upload the Root Certificate to the Connection Server**

**Step 1** Sign in to Cisco Unified Operating System Administration by using the administrator account and password.

The administrator account, which you created during Connection installation, is different from the accounts and passwords that you use to sign in to Connection Administration.

**Step 2** On the Security menu, select **Certificate Management**.

**Step 3** Select **Upload Certificate**.

**Step 4** In the Certificate Name list, select **Connection-trust**.

**Step 5** Select **Browse**, and find the file that contains the root certificate for the certification authority that issued the certificate for MeetingPlace.

**Step 6** Select **Upload File**.

# Securing Access to an LDAP Directory

For information on securing data that is transmitted between LDAP servers and Cisco Unity Connection, see the "Uploading SSL Certificates on the Cisco Unity Connection Server" section in the "Integrating Cisco Unity Connection 8.x with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection* Release 8.x at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html.

# Securing Communication Between Connection and Cisco Unity Gateway Servers When Connection Networking Is Configured

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 Cisco 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 Windows Server 2003, see the "Installing Microsoft Certificate Services (Windows Server 2003 Only)" section on page 9-58. 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 Connection cluster is configured for the Connection gateway server, run the `set web-security` CLI command on both Connection servers in the cluster and assign both servers the same alternate name. The alternate name will 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 http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
3. If a Connection cluster is configured for the 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 Connection voice messages by using the same Connection server name.

4. On the 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. Do the "To Create and Download a Certificate Signing Request on a Connection Gateway Server" procedure on page 9-55.

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

5. 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. Do the "To Create and Download a Certificate Signing Request on a Cisco Unity Gateway Server" procedure on page 9-55.

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

6. 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)" section on page 9-59.

   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 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 by using freely available utilities like OpenSSL.

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

7. Upload the root certificate and the server certificate to the Connection server. Do the "To Upload the Root and Server Certificates to the Cisco Unity Connection Server" procedure on page 9-49.

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

8. Restart the Connection IMAP Server service so that Connection and the IMAP email clients use the new SSL certificates. Do the "To Restart the Connection IMAP Server Service" procedure on page 9-50.

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

9. Upload the root certificate and the server certificate to the Cisco Unity server. Do the "To Upload the Root and Server Certificates to the Cisco Unity Server" procedure on page 9-57.

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

### To Create and Download a Certificate Signing Request on a Connection Gateway Server

**Step 1** On the Cisco Unity Connection server, sign in to Cisco Unified Operating System Administration.

**Step 2** On the Security menu, select **Certificate Management**.

**Step 3** On the Certificate List page, select **Generate CSR**.

**Step 4** On the Generate Certificate Signing Request page, in the **Certificate Name** list, select **tomcat**.

**Step 5** Select **Generate CSR**.

**Step 6** When the Status area displays a message that the CSR was successfully generated, select **Close**.

**Step 7** On the Certificate List page, select **Download CSR**.

**Step 8** On the Download Certificate Signing Request page, in the **Certificate Name** list, select **tomcat**.

**Step 9** Select **Download CSR**.

**Step 10** In the File Download dialog box, select **Save**.

**Step 11** In the Save As dialog box, in the **Save As Type** list, select **All Files**.

**Step 12** Save the file **tomcat.csr** to a location on the server on which you installed Microsoft Certificate Services or on a server that you can use to send the CSR to an external certification authority.

**Step 13** On the Download Certificate Signing Request page, select **Close**.

---

**To Create and Download 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 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 will 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.

---

**To Upload the Root and Server Certificates to the Cisco Unity Connection Server**

---

**Step 1** On the Cisco Unity Connection server on which you created the certificate signing request, sign in to Cisco Unified Operating System Administration.

**Step 2** On the Security menu, select **Certificate Management**.

**Note** If you select **Find** and display a list of the certificates currently installed on the server, you will see an existing, automatically generated, self-signed certificate for Tomcat. That certificate is unrelated to the Tomcat certificates that you upload in this procedure.

**Step 3** Upload the root certificate:

a. On the Certificate List page, select **Upload Certificate**.

b. On the Upload Certificate page, in the Certificate Name list, select **tomcat-trust**.

c. Leave the Root Certificate field blank.

d. Select **Browse**, and browse to the location of the root CA certificate.

If you used Microsoft Certificate Services to issue the certificate, this is the location of the root certificate that you exported in the "To Export the Root Certificate and to Issue the Server Certificate" procedure on page 9-59.

If you used an external certification authority to issue the certificate, this is the location of the root CA certificate that you received from the external certification authority.

e. Select the name of the file.

f. Select **Open**.

g. On the Upload Certificate page, select **Upload File**.

h. When the Status area reports that the upload succeeded, select **Close**.

**Step 4** Upload the server certificate:

a. On the Certificate List page, select **Upload Certificate**.

b. On the Upload Certificate page, in the Certificate Name list, select **tomcat**.

c. In the Root Certificate field, enter the filename of the root certificate that you uploaded in Step 3.

d. Select **Browse**, and browse to the location of the server certificate.

If you used Microsoft Certificate Services to issue the certificate, this is the location of the server certificate that you issued in the "To Export the Root Certificate and to Issue the Server Certificate" procedure on page 9-59.

If you used an external certification authority to issue the certificate, this is the location of the server certificate that you received from the external certification authority.

e. Select the name of the file.

f. Select **Open**.

g. On the Upload Certificate page, select **Upload File**.

h. When the Status area reports that the upload succeeded, select **Close**.

**Step 5** Restart the Tomcat service (the service cannot be restarted from Cisco Unified Serviceability):

a. Sign in to the Connection server by using an SSH application.

b. Run the following CLI command to restart the Tomcat service:

```
utils service restart Cisco Tomcat
```

**To Restart 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.

**To Upload the Root and Server Certificates 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 2003 Only)

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.

Do the procedure in this section if you want to use Microsoft Certificate Services to issue your own certificate and if you want to install the application on a server running Windows Server 2003.

If you want to install a root certification authority (the generic term for Microsoft Certificate Services) on a Windows Server 2008 server, refer to the Windows Server 2008 online help.

**To Install the Microsoft Certificate Services Component**

**Step 1** On any server whose DNS name (FQDN) or IP address can be resolved by all client computers that will use the Cisco PCA or that will use an IMAP client to access Cisco Unity Connection voice messages, sign in to Windows by using an account that is a member of the local Administrators group.

**Step 2** On the Windows Start menu, select **Settings > Control Panel > Add or Remove Programs**.

**Step 3** In the left pane of the Add or Remove Programs control panel, select **Add/Remove Windows Components**.

**Step 4** In the Windows Components dialog box, check the **Certificate Services** check box. Do not change any other items.

**Step 5** When the warning appears about not being able to rename the computer or to change domain membership, select **Yes**.

**Step 6** Select **Next**.

**Step 7** On the CA Type page, select **Stand-alone Root CA**, and select **Next**. (A stand-alone certification authority (CA) is a CA that does not require Active Directory.)

**Step 8** On the CA Identifying Information page, in the Common Name for This CA field, enter a name for the certification authority.

**Step 9** Accept the default value in the Distinguished Name Suffix field.

**Step 10** For Validity Period, accept the default value of **5 Years**.

**Step 11** Select **Next**.

**Step 12** On the Certificate Database Settings page, select **Next** to accept the default values.

If a message appears indicating that Internet Information Services is running on the computer and must be stopped before proceeding, select **Yes** to stop the services.

**Step 13** If you are prompted to insert the Windows Server 2003 disc into the drive, do so.

**Step 14** In the Completing the Windows Components Wizard dialog box, select **Finish**.

**Step 15** Close the Add or Remove Programs dialog box.

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

Do the following procedure only when you are using Microsoft Certificate Services to issue the certificate.

**To Export the Root Certificate and to Issue the Server Certificate**

**Step 1** On the server on which you installed Microsoft Certificate Services, sign in to Windows by 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 "To Install the Microsoft Certificate Services Component" procedure on page 9-58.

**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 Connection server.

Write down the path and filename. You will 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 "To Create and Download a Certificate Signing Request" procedure on page 9-48, 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 will need it in a later procedure.

k. Select **OK**.

**Step 6** Close Certification Authority.

CHAPTER 10

# Securing User Messages in Cisco Unity Connection 8.x

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 Connection server, enabling you to maintain control of how long messages are retained before they are archived or purged. Connection also offers methods for managing the secure deletion of messages.

See the following sections:



## How Cisco Unity Connection 8.x Handles Messages That Are Marked Private or Secure

**Revised TBD**

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 Connection marks messages that are left by outside callers as private, secure, or both.

**Private Messages**

- Any recipient can receive a private message—including non-Connection users. Recipients can listen to private messages by using the phone, the Connection Messaging Inbox (in Connection 8.0) or Connection Web Inbox (8.5 and later), ViewMail for Outlook, ViewMail for Notes, Cisco Unified Personal Communicator, Cisco Unified Messaging with IBM Lotus Sametime, or an IMAP client.
- A private message cannot be forwarded by phone, from the Messaging Inbox (in Connection 8.0) or Web Inbox (8.5 and later), or from ViewMail for Outlook or ViewMail for Notes.

- 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 in Cisco Unity Connection 8.x" section on page 10-69 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. (available in Connection 8.6 and later only).
- 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, 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 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 Options menu on the Media Master in the Connection Messaging Inbox (in Connection 8.0), Cisco Unity Connection ViewMail for Microsoft Outlook (version 8.0), and Cisco Unity Connection ViewMail for IBM Lotus Notes.
- Secure messages can be useful for enforcing your message retention policy. You can configure 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. For more information, see the "Managing Message Aging Policies in Cisco Unity Connection 8.x" section in the "Controlling the Size of Mailboxes in Cisco Unity Connection 8.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 8.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html.
- Secure messages can be played by using the following interfaces:
  - Connection phone interface
  - Cisco Unity Connection Messaging Inbox (in Connection 8.0)
  - Cisco Unity Connection Web Inbox (Connection 8.5 and later)
  - Cisco Unity Connection ViewMail for Microsoft Outlook (version 8.0)
  - Cisco ViewMail for Microsoft Outlook (version 8.5 and later)
  - Cisco Unity Connection ViewMail for IBM Lotus Notes
  - Cisco Unified Personal Communicator version 7.0 and later
  - 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 by 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/en/US/products/ps9830/prod_release_notes_list.html.)
- Secure messages can be forwarded by using the following interfaces:
  - Connection phone interface

  - Cisco Unity Connection Connection Web Inbox (in Connection 8.5 and later)
  - Cisco Unity Connection Messaging Inbox (in Connection 8.0)
  - Cisco Unity Connection ViewMail for Microsoft Outlook 8.5
- Secure messages cannot be accessed by using the following interfaces:
  - IMAP clients (unless ViewMail for Outlook or ViewMail for Notes is installed)
  - RSS readers
- By default, only 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 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 Connection users and to the 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 Connection and send a message, class of service settings determine whether the message is marked secure. By default, Connection automatically marks a message secure when the user marks it private.
- *(Cisco Unity Connection 8.0(2) and later)* If you want 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, 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 Connection marks the message secure.
- By default, 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, Connection sends a non-delivery receipt to the sender. To have 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 will 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 by 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 by 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 Cisco Unity Connection to Mark All Messages Secure

**Added November 16, 2010**

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

1. Configure all classes of service to always mark messages secure. See the "To Enable Message Security for COS Members" procedure on page 10-66. (When users sign in to 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 "To Configure Users and User Templates to Mark Messages Left By Outside Callers Secure" procedure on page 10-66.
3. Configure call handlers to mark all outside caller messages secure. See the "To Configure Call Handlers and Call Handler Templates to Mark Messages Left By Outside Callers Secure" procedure on page 10-66.
4. *(Cisco Unity Connection 8.0(2) and later)* If you do not want 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.

### To Enable Message Security for 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.

### To Configure 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**.

### To Configure 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**.

# Disabling the "Save Recording As" Option in the Cisco Unity Connection 8.0 Messaging Inbox for All Voice Messages

**Revised November 16, 2010**

By default, except for messages that are marked private, secure, or private and secure, users can save their messages as WAV files to their hard disks by using the Save Recording As option, available on the Media Master Options menu in the Cisco Unity Connection 8.0 Messaging Inbox. You can prevent users from saving any voice message—regardless of its sensitivity—by disabling the Save Recording As option on the Options menu of the Media Master in the Messaging Inbox.

Note the following as you consider this security option:

- When you prevent users from by saving messages to their hard disks, they may choose to retain them in their Inboxes and Deleted Items folders longer as a way of archiving them.
- Disabling the Save Recording As option affects all users who are associated with the Connection server; you cannot disable it only for individual users.
- Users can continue to use the Media Master to save greetings or recorded names as WAV files.

**To Disable the Save Recording As Option in the Media Master in the Cisco Unity Connection 8.0 Messaging Inbox**

**Step 1** In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then select **PCA**.

**Step 2** On the PCA Configuration page, check the **Unity Inbox: Disable Save Recording As Option in Media Master** check box.

**Step 3** Select **Save**.

# Shredding Message Files for Secure Delete (Cisco Unity Connection 8.5 and Later Only)

**Added November 16, 2010**

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 Messaging Inbox or 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 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, the Messaging Inbox or 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 Connection server, and can thus be shredded when deleted.

  **Note** For additional information about secure messaging, see the "Secure Messages" section on page 10-63.

- Messages that are sent between locations in a 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 Cisco 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. For information on the methods that users can use to delete messages, and a definition of soft and hard deletes, see the "Deleting Messages in Cisco Unity Connection 8.x" section in the "Messaging in Cisco Unity Connection 8.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 8.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html.

# Message Security Options for IMAP Client Access in Cisco Unity Connection 8.x

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.)

# INDEX

## Q



## R



## S



## T



## U



## V